



DAMAGE CONTROL

**CYBER INSURANCE
AND COMPLIANCE**

JOSEPH E. BRUNSMAN, MSL // DANIEL W. HUDSON, CPCU // KENNETH J. REINERS, CISSP

Damage Control

Cyber Insurance & Compliance

Joseph E. Brunsman, MSL

Capt. (Ret) Daniel W. Hudson, CPCU

Kenneth J. Reiners, CISSP

Damage Control

Publishing History

Paperback Edition 1 / March 2020
ISBN: 978-0-578-66416-3

Copyright © 2020 by Chesapeake Professional Liability Brokers, Inc.
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the authors

Damage Control

Disclaimer

This book was designed for general insurance guidance and considerations only.

Limit of liability/disclaimer of warranty: The publisher and the authors make no representations or warranties with regard to:

The completeness or accuracy of the contents of this work and specifically disclaim and exclude all warranties, express or implied, including without limitation, warranties of fitness for a particular purpose or usage of trade. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher and authors are not engaged in rendering legal, accounting, or other professional services. If professional assistance is required or needed, the services of a competent professional should be sought. Neither the publisher nor the authors shall be liable for damages resulting herefrom. The fact that this work refers to an organization or website as a citation and/or a potential source of further information does not mean that the publisher or the authors endorse the information, the organization, the website, or the recommendations each may provide. Readers should be aware that Internet websites and website addresses listed may have changed or been deleted since this work was written. This limitation/disclaimer also specifically excludes any third-party beneficiaries.

Damage Control

Dedications

Here I sit again writing with great thanks to my loving wife for keeping the world together as I work on yet another book. One of these days – I promise – I'll be asleep before 2 A.M. To my two young sons, I know you won't read this until much later in life. By then I'll be your lame old Dad. Nevertheless, when I wrote this, I was young and cool. Science will tell you if you can – Philosophy will tell you if you should. Read great and difficult books – this will allow you to form your own opinions. Understand statistics and probabilities – this will help you weigh the opinions of others. I won't much care what grades you earn in school so long as you maintain a sense of wonder and curiosity about the world. Succeed with humility, fail with grace, and help anyone willing to help themselves. No matter how hard life will become, remember that every hero's journey begins with a tragedy. Make good mistakes. When you can't work any smarter, work your ass off. Leave the world a little better than when you joined it. Be grateful. Have some fun along the way. Do the hard work. Half the battle is showing up.

~ Joseph E. Brunsman.

I dedicate this book to my U.S. Naval Academy shipmates, to those who have served, to those that continue to serve, and to my wonderful family. Thank you all for your generous support throughout the years.

~ Daniel W. Hudson

I would like to dedicate this book to my wonderful and loving wife, who has supported me every step of the way, and to my amazing little daughter, who has brought me so much joy, and reminded me about the importance of living in the present.

~ Kenneth J. Reiners

Damage Control

About the Authors

Joseph E. Brunzman

Joe is an avid truth seeker, sought-after keynote speaker, and a best-selling author. He began his life by skipping school and hanging out in the library where he read every technology and science book available. This inevitably led him to military school where he served the remainder of his sentence dodging alien hunters at New Mexico Military Institute (NMMI) in Roswell, New Mexico. Upon graduation, he enlisted in the Navy, serving three years as an Information Systems Technician (IT) where he focused on database management, network security, radio communications, and satellite communications.

Upon receiving an appointment to the United States Naval Academy, he majored in Systems Engineering (Robotics). He won the senior design award for creating a semi-autonomous, beer-launching fridge. That fridge is still used today to lure unsuspecting freshman into taking 20 credit hours a semester for the next three years. As a naval officer, he served as a Surface Warfare Officer where he held positions ranging from Electronic Warfare Officer to Anti-Terrorism Force Protection Officer.

After visiting over 30 countries, he left the service for the greener pastures of insurance life. Within the first eight months on his new job, he became a best-selling author by co-authoring the first book ever published on the topic of insurance for accounting firms. This has been followed up by numerous publications in various magazines around the country.

In 2019, he completed his Master of Science in Law in Cybersecurity Law from the Francis King Carey School of Law. He is the Vice-President and Chief Content Officer of Chesapeake Professional Liability Brokers in Annapolis, MD.

When not being humored by his infinitely patient wife or playing with his two young sons, he can be found furiously researching his latest technology article or doing his best to learn Brazilian Jiu-Jitsu.

Daniel W. Hudson

A United States Naval Academy graduate with an MBA from the University of North Florida, Dan has specialized in insurance solutions for various businesses for over 25 years. He holds both a Chartered Property Casualty Underwriter (CPCU) and an Associate in Risk Management (ARM) designations.

He is the co-author of two best-selling books on insurance as well as numerous articles in various magazines. In 1995 he founded Chesapeake Professional Liability Brokers, Inc.

Dan served as a naval flight officer, flying more than 550 missions in the navy submarine hunter, P-3C Orion. He conducted worldwide, anti-submarine, littoral warfare and counter-narcotics operations. He served as the Commanding Officer of Patrol Squadron Six-Four (VP-64), earning the prestigious Battle "E." On his final tour of duty, he served as Deputy Commander of Reserve Patrol Wing, retiring as a captain.

Kenneth J. Reiners

After graduating from Mankato State University with a bachelors in Exercise Science, Kenneth heard the calling to serve his country, and joined the Navy shortly after in 2013. Kenneth did two tours in the Navy as a Cryptologist Technician of Networks (CTN), which helped form the foundation of his cybersecurity career. His first tour was with a National Mission Team under the Cyber National Mission Forces, where he conducted SIGINT analysis and reporting. His second tour was with the newly formed Cyber Protection Teams, where he leveraged security tools for threat hunting and incident response regarding attacks carried out by nation state actors and advanced persistent threats.

While in the Navy, Kenneth completed a masters in Cybersecurity Technology and completed several industry recognized certifications to include SEC+, CEH, and CISSP. Kenneth currently works as a Solutions Architect in Annapolis, MD. He focuses on consulting and provides pre-sales engineering support to a wide variety of customers within the U.S. Intelligence Community, Fortune 1000 companies, and higher education.

Outside of work, Kenneth loves learning about the latest biohacking, fitness, and nutrition research as well as blockchain and distributed ledger technologies. He also enjoys working out, anything outdoors, and spending time with his beautiful wife and daughter.

Damage Control

Why We Wrote this Book and Why You Should Read It

For the foreseeable future, educated choices regarding cyber insurance will remain mainly with the consumer. This is because, among other reasons, the average insurance agent in the United States is 59 years old.¹ Learning this non-standardized, evolving, and complex line of insurance while in the twilight years of their careers is decidedly unpalatable. Unsurprisingly, a joint survey from the Griffith Insurance Education Foundation and The Institutes found that younger employees consider insurance, “boring,” and thus young agents with the requisite technical knowledge are unlikely to be available.

While the promise of large premiums could lure current insurance agents into developing the expertise necessary to knowledgeably advise clients, there too lies another problem. Although cyber insurance is the hot new product on the market, the premiums are comparatively minor. Globally, the cyber insurance market in 2017 was estimated to be at \$4.52 billion and is expected to reach \$17 billion by the year 2023.² By comparison, the entire United States Insurance market wrote a total of \$1.2 trillion in premiums in 2017 alone.³

Even if the premiums available for cyber insurance rise as forecasted, the driver behind most insurance agents will continue to remain the commission payable for each policy written. Here too, the numbers will not give rise to experts in cyber insurance. Take, for example, a recent case where the restaurant chain P.F. Chang’s cyber insurance policy limits were made public. Although a multi-billion-dollar-per-year business with significant exposure across untold numbers of computers and terminals, their cyber insurance policy premium was approximately \$134,000.⁴ The average commissions for agents working at an insurance brokerage is often as low as 3%. In the example above, this would result in a payable commission of as little as \$4,020; before taxes.

While not a trivial figure, remember that there are only so many multi-billion-dollar-grossing companies requiring cyber insurance insights. Businesses of that size will most assuredly have in-house general counsel to advise them on their policy choices. Most likely, it will be small- to medium-sized businesses that will lean heavily on their insurance agents to “get it right.” For an insurance agent to write a cyber policy for a one-million-dollar-grossing business, the commission can come out to between \$40 and \$100 per policy.⁵ This is not exactly a panacea of potential revenue that would spur the average insurance agent to specialize in cyber insurance. When compared to the hundreds of thousands, or millions, of dollars that a business is legally obligated to pay out following a data breach, there is a decided asymmetric barrier to the importance given to cyber insurance.

Breaches may be increasing in both frequency and severity, but the insurance market has so far responded in a novel way. Foremost, the cyber insurance market is currently “soft.” This is insurance industry parlance for a highly competitive market where numerous insurers are all vying to write new policies. This often results in premiums far lower than the limited actuarial data would support. In turn, this can lower the commission an insurance agent is paid even further.

Further exacerbating the downward pressure on cyber insurance premiums is the “actuary’s paradox.” In all other surveyed lines of insurance, claims reported by the insured generally result in higher premiums when the policy is renewed. In cyber insurance, certain insurers rationalize that following a breach, a business will take the threat more seriously. Thus, they can be classified as a better risk in the future. As a result, a business’s premium can be lower after a breach than before.⁶ It would be hard to conceive of a sustainable auto insurer who lowered rates after a crash.

The final issue is that the law continues to evolve at a rapid pace. Any hard-won knowledge learned by an insurance broker is easily rendered irrelevant by the swiftly changing legal landscape. For example, in 2018 alone, 37 different states and territories introduced over 256 new bills or resolutions that would affect data security or cybersecurity.⁷ Consider that roughly 89% of those who join the insurance industry will quit within 36 months; there is simply not enough time for the average broker to gain any level of competence in this field.⁸

As breach frequency and severity continues to rise, consumers will increasingly demand knowledgeable brokers who are able to assist them in navigating the bewildering world that is cyber insurance. Yet, the general rule within insurance law is that “absent special circumstances that might give rise to a broader duty, the default rule is that agents and brokers have no duty to advise insureds about the adequacy or appropriateness of the insurance coverage they purchase or about optional coverage that might be available.”⁹

To add to the ambiguity, in most jurisdictions, the insurance company has no obligation to explain the policy to the business. As the Supreme Court of California once paradoxically noted, “[w]hen a court is reviewing claims under an insurance policy, it must hold the insured bound by clear and conspicuous provisions in the policy even if evidence suggests that the insured did not read or understand them.”¹⁰ Consequently, it’s on you to get it right, or risk professional damage to your business potential financial ruin.

Businesses want to maximize their chances of the correct coverage options while avoiding the most common reasons for a declination of coverage. To do so, they must be armed with the appropriate knowledge before making any decisions.

Damage Control

How to Use this Book

Big problems happen when cybersecurity is the responsibility of only one person in an organization. In the modern age, every member of a company has a responsibility toward cybersecurity.

Staff needs to know what rules they're supposed to follow, and why. HR needs to inform the IT department who needs access to what and when. The IT department needs to coordinate with management and explain why certain projects require funding and how to prioritize those requests. The CIO/CISO needs to have buy-in with other stakeholders when approaching the CFO for budget requests. The CEO needs to understand the big picture and balance competing interests. Of course, the partner in charge of purchasing cyber insurance can benefit from this book.

Read the book from front to back. You will be surprised to learn what regulations you may fall under and how cyber insurance will – or will not – respond. Give it to your business partners and other responsible parties. Give it to your friends. Tell them all to read it front to back. Help them avoid preventable and costly mistakes.

All this may seem heretical in the modern age where we are torn from one meeting to the next, and information comes in 30-second segments. When your business is facing a breach or inquiries from regulators, all those other distractions will seem trivial. Make sure that you are armed with as much knowledge as possible so you can make the best decisions possible.

Best case scenario: You're armed with knowledge you will thankfully never use.

Worst case scenario: You're facing the storm – a very expensive and difficult storm – without a compass.

On a less terrifying note, many terms in this book will be used interchangeably – unless otherwise noted – due to the wide audience of the readership. Interchangeable terms could include: Business/firm/practice/company, customer/client, and hacker/malicious-actor/unauthorized-third party. Finally, the cases and circumstances referenced in this book contain the allegations of second and third parties. While we have done our best to separate conjecture from fact, readers are encouraged to reference the entirety of each case and circumstance before casting judgment on the named parties.

Damage Control

Table of Contents

Disclaimer	i
Dedications	iii
About the Authors.....	v
Why We Wrote this Book and Why You Should Read It	vii
Table of Cases.....	xv
Section 1: Fundamental Knowledge	1
Learn from Others’ Mistakes	3
Business Adversaries	7
Attack Vectors	9
Forms of Malware.....	11
Types of Defense (Controls).....	15
What is “Reasonable” Cybersecurity?	19
Will I lose clients after a breach?.....	35
Ransomware and the Potential of Breach Notification.....	41
The Crucial Role of Employee Training in Cybersecurity	47
Data Retention is a Cybersecurity Issue	53
The Limits of Cyber Insurance	57
Section 2: State-Level Requirements.....	59
State Breach Notification Laws	61
Protected Information	65
Exempted Information	69
The Definition of a Breach	71
Exceptions.....	73
Data Encryption Safe Harbors	75
Service Provider Requirements	77
Notice Requirements.....	81
How Notice Is Given Including Content Requirements	85

State-level Enforcement Actions and Penalties	87
Client Claims Following a Breach	91
Section 3: Notable State-Specific Privacy Laws	93
California Consumer Privacy Act (CCPA)	95
Massachusetts' 201 CMR 17	99
New York's 23 NYCRR 500	103
New York SHIELD Act	109
Illinois' Biometric Information Privacy Act (BIPA)	113
Section 4: Cybersecurity and Privacy Requirements	121
FTC Cybersecurity Oversight	123
Gramm Leach Bliley Act and the Safeguards Rule	127
Securities and Exchange Commission (SEC) Regulation S-P	131
SEC Custody Rule	135
Red Flag Rule(s) – SEC & FTC	137
EU-US & Swiss-US Privacy Shield frameworks	141
AICPA/IRS Requirements	149
American Bar Association Requirements	153
Financial Industry Regulatory Authority (FINRA)	159
Government Contractors: Cybersecurity Maturity Model Certification Model (CMMC)	161
Healthcare: HIPAA/HITECH	175
Notable OCR Enforcement Action Examples	185
HIPAA Audit Program	191
Educational Institutions: The Family Educational Rights and Privacy Act (FERPA)	193
TCPA – Telephone Consumer Protection Act	203
CAN-SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act	205
Americans with Disabilities Act (ADA)	207
The Consumer Financial Protection Bureau	209
Public Companies & Cybersecurity	213
GDPR – EU General Data Protection Regulation	219

APEC - Asia-Pacific Economic Cooperation	223
Other Foreign “Cyber” Laws	227
 Section 5: Potential Coverage in Non-Cyber Insurance Policies	229
Commercial Insurance Policies	231
Commercial Crime Policies	235
Professional Liability Policies	239
Professional Liability Policy Cyber Endorsements	245
Employment Practices Liability Insurance Policies	251
Director and Officers Liability Insurance (D&O) Policies.....	253
Tech E&O Policies	257
 Section 6: Dedicated Cyber Insurance Policies	259
Cyber Insurance Applications.....	261
Concerning Admitted vs. Non-Admitted Policies	267
Large Losses May Lead to Novel Policy Interpretations by Insurers.....	269
Self-Insurance for Cyber Losses.....	273
Understanding “Named Insured”	275
Defense Arrangements.....	277
Tail Policy Coverage	279
Understanding the Difference Between 1 st - And 3 rd - Party Cyber Insurance Coverage	281
Deductible/Retention Options.....	285
Overlapping Coverage, Other Insurance Clauses, and Multiple Deductibles	287
Sublimits, Policy Structure, and Appropriate Limits.....	291
Choice of Law Provisions.....	295
Selecting Limits	297
Common Coverage Options.....	301
Common Coverage Exclusions.....	311
Simplifying Coverage Assessments with Wargaming.....	315
The Insurability of Fines and Penalties.....	321
Excess Insurance Considerations.....	327
General Guidelines on Purchasing Cyber Insurance	331

Section 7: After the Policy is Bound..... 333

 Policy Benefits 335

 Potential Claim Reporting..... 337

 Claim Reporting..... 341

 Giving Notice to the Insurer 343

 Material Changes 345

Section 8: Interesting Extras 347

 Examples of Real Business Breaches 349

 Tips on Passwords from NIST 353

 Warning Signs..... 355

 What is an Incident Response Plan? 357

 What is a Cybersecurity Framework?..... 361

 Assessing the Security of Cloud Providers 369

 What are Written Information Security Programs & Policies? 375

 The Golden Rules of Cyber 379

 Attorneys and Cybersecurity..... 381

 The Interesting Role of CPAs in Cybersecurity 385

Section 9: Other Useful Publications from the Authors . 395

 Tips on Minimizing Wire Fraud 397

 Russian Hackers Specifically Targeting Accounting Firms 401

 Cyber-Related Claims Without a Breach ... They're Coming 405

 Use of Driver's License Numbers Raises Security Concerns..... 409

 Should CPA Firms Be Worried About Data-Breach Claims? 413

Section 10: Staying Current..... 419

 Author's Contact Information..... 421

References..... 423

Damage Control

Table of Cases

A

American Tooling Center v. Travelers Casualty & Surety Co., 387
Ameriforge Group Inc., d/b/a AFGlobal Corp. v. Federal Insurance Co., 402
Apache Corp. v. Great American Insurance Co., 235
Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co., 237

B

Beck v. McDonald, 306
Boardman Molded Products v. Involta, LLC, 77
Bryan Brothers, Inc. V. Continental Casualty Company, 241
Bullock v. Maryland Casualty Company, 325

C

CAMICO Mutual Insurance Company v. Heffler Radetich & Saitta, LLP., 241
Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., 284
Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), 185
Columbia Casualty Co. v. Cottage Health System, 263
Commonwealth of Massachusetts v. Equifax, Inc., 100
Creative Hospitality Ventures, Inc. v. United States Liability Company, 233
Curry v. Schletter, Inc., 50

D

Drexel Burnham Lambert Group., Inc. v. Vigilant Insurance Company, 325

F

F.T.C. v. Wyndham Worldwide Corp., 124
Fairfield Insurance Company v. Stephens Martin Paving, 325
Flores v. ACE American Insurance Company, 203
Friends of the Earth Inc. v. Laidlaw Environmental Services, Inc., 420
FTC. v. LifeLock, Inc., 146

H

Hope Lee-Thomas v. Labcorp, 188
Howard v. Citrix Systems, 371

I

- In re Anthem, Inc.*, 187
In re Equifax Inc., Customer Data Security Breach Litigation, 337
In re Facebook Biometric Info Privacy Litigation, 118
In the Matter of Accretive Health Inc., 22
In the Matter of BJ's Wholesale Club, Inc., 22
In the Matter of CardSystems Solutions, Inc., 30
In the Matter of Credit Karma, Inc., 28
In the Matter of CVS Caremark Corporation, C-2459 (2009), 71
In the Matter of Dave and Buster's, Inc., 29
In the Matter of DSW Inc., 29
In the Matter of Dwolla, Inc., 209
In the Matter of Eli Lilly and Company, 20
In the Matter of Fandango, LLC, 25
In the Matter of Franklin's Budget Car Sales, Inc., also d/b/a Franklin Toyota/Scion, 27
In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekanth Srivastava, individually and as officers of GMR Transcription Services, Inc., 30
In the Matter of Goal Financial, LLC, 24
In the Matter of Gregory Navone, 26
In the Matter of GW & Wade, LLC, 135
In the Matter of InfoTrax Systems, L.C and Mark Rawlins, 27
In the Matter of Lookout Services, Inc., 24
In the Matter of Morgan Stanley Smith Barney, 132
In the Matter of Petco Animal Supplies, Inc., 22
In the Matter of Premier Capital Lending, Inc., and Debra Stiles, 20
In the Matter of Reed Elsevier, Inc. and Seisint, Inc., 23
In the Matter of Rite Aid, 23
In the Matter of RockYou, 21
In the Matter of SecurTest, Inc., 142
In the Matter of Superior Mortgage Corp., 24
In the Matter of TaxSlayer, 128
In the Matter of ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc., 26
In the Matter of Very Incognito Technologies, Inc., a corporation d/b/a Vipvape, 224
In the Matter of Voya Financial Advisors, Inc., 138
In the Matter of The TJX Companies, 26

K

- Krottner v. Starbucks Corp.*, 418

L

- Liu v. Four Seasons Hotel Ltd*, 119

M

Michelle Espinosa v. RevMD Partners, LLC, 117
Mondalez International, Inc. v. Zurich American Insurance Company, 271

N

Netcracker Technology Corporation (NTC), 169
New Hotel Monteleone, LLC. v. Certain Underwriters at Lloyd's of London and Eustis Insurance, Inc., 293

O

of Gonzaga University v. Doe, 195
Oregon Health & Science University (OHSU), 186

P

P.F. Chang's China Bistro, Inc. v. Federal Insurance Co., 146
P.F. Chang's China Bistro, Inc. v. Federal Insurance Co., 271
Patco Construction v. People's United Bank., 33

R

Reilly v. Ceridian Corp., 418
Remijas v. Neiman Marcus Group, LLC, 305
Resnick v. AvMed Inc., 419
Roberts v. Maricopa County Community College District, 197
Rosenbach v. Six Flags Entm't Corp., 117

S

Shore v. Johnson & Bell, Case No. 16-cv-4363 (N.D. Ill. 2016), 409
Spec's Family Partners, Ltd. v. Hanover Insurance Company, 253
State of Washington v. Uber Technologies, Inc., 88
States v. Aerojet Rocketdyne Holdings, Inc., 172

T

The Center for Children's Digestive Health, 185
Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC, 232

U

United States of America v. Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, 42
United States v. Miami University, 196

W

Warth v. Seldin, 422 U.S. 490 (1975), 417

Wilson v. Chem-Solv, Inc., 325

Z

Zurich American Insurance Co. v. Sony Corp., 232

Damage Control

Damage Control

Joseph E. Brunsman, MSL

Capt. (Ret) Daniel W. Hudson, CPCU

Kenneth J. Reiners, CISSP

Damage Control

Section 1: Fundamental Knowledge

Before a business contemplates cyber insurance, it is helpful to understand their common adversaries, attack vectors, types of malware, and other fundamental knowledge. Beyond merely demonstrating that every business is at risk, this knowledge will later prove valuable when purchasing the most suitable cyber insurance coverage.

Damage Control

Learn from Others' Mistakes

In early February of 2019, a multi-channel direct marketing company appeared to be on the upswing. The company, along with the local chamber of commerce, was celebrating the grand re-opening of their remodeled call center. With almost 5,000 square feet of new floor space and 77 new workstations, the company planned to add 50 new positions over the next six months with yet another 50 new hires in the future.¹¹ All considered, this looked like a profitable company, providing jobs to honest and hardworking people.

Before the end of the year, disaster struck, and their operations ended.

Nearly 300 employees received the statement letter below. It was obtained by a local news source and released roughly two days before Christmas, 2019.

"Dear Employees of The [REDACTED] Company,

I know that you are all angry, confused, and hurt by the recent turn of events. Please know that I am just as devastated as you all are, especially that we had to do this at this particular time of year.

Please know that we would have NEVER gone to this extreme if we were not forced to. Now is the time to be honest and open about what is REALLY happening so that all of you know the truth, directly from me, especially since some of you have incorrect information and the spreading of untruths thru social media is damaging us further.

Unfortunately, approximately two months ago our [REDACTED] servers were attacked by malicious software that basically "held us hostage for ransom" and we were forced to pay the crooks to get the "key" just to get our systems back up and running. Since then, IT has been doing everything they can to bring all our systems back up, but they still have quite a long way to go. Also, since then, I have been doing my utmost best to keep our doors open, even going as far as paying your wages from my own money to keep us going until we could recoup what we lost due to the cyber attack.

I know how confusing this must be, especially after we just gave away 7 cruises just this week, but again, that was money that I spent out of my

own personal money to give you the best Christmas gift I possibly could, but that was before our systems were hacked. Afterwards I didn't want to disappoint everyone by taking them back. We started the Prizes and Bingo the first of November when again I was being told the systems would be fixed that week.

What we hope is just a temporary setback is an opportunity for IT to continue their work to bring our systems back and for leadership to restructure different areas in the company in an attempt to recoup our losses which have been hundreds of thousands of dollars.

It is extremely important right now that we all keep the faith and hope alive that The ██████████ Company can and will come back from this setback. It is also important that we all keep to the facts and keep calm. And so, I ask that you please share this with the employees who may not be on this page or may not have Facebook. To share this out of the group, you will need to copy the text of this post and share it as your own status.

Please know that when I made my speech at the "Future is Bright" luncheons, everything was sincere and heartfelt. We had no way of predicting that our systems would be hacked at that time. Once we were hit with this terrible virus we were told time and time again that things would be better each week, and then the next week, and the week after that. Accounting was down and we had no way of processing funds. The mail center was down as we had no way of sending statements out, which meant that no funds could come in.

Had we known at the time that this would have hurt the company this badly, we would have made a statement to the employees long ago to warn everyone what this might mean. The ONLY option we had at this time was to close the doors completely or suspend our services until we can regroup and reorganize and get our systems running again. Of course, we chose to suspend operations as Heritage is a company that doesn't like to give up.

I also want to apologize for the way many of you found out we were closing our doors. When we left the meeting yesterday afternoon, everyone had a plan for what was to happen, but we never considered that the word would spread so fast and far to each of you before your managers could speak to the employees who had already gone home for

the day. No one is sorrier than I about you finding out from other sources who did not necessarily have the correct information.

So here it is: The [redacted] Company is temporarily suspending our services. On January 2nd, there will be a message left on the weather line. That message will give you updated information on the restructuring of the company and whether or not we've made progress on our system.

In the meantime, I urge each and every one of you to please keep faith with us. We know how extremely hard you all work for each of the wonderful charities we all represent. We want you all back where you belong in two weeks' time. We are a family, and my hope is that we will stay a family for a long time, despite this setback.

My mother started this company 61 years ago, and I am committed to keeping [redacted] open if it is in my power to do so.

Sincerely,

*[redacted]
Owner and CEO,
[redacted]"12*

It is unknown if the company had adequate cyber insurance or any cyber insurance for that matter. However, a few notable lessons can be used as teaching points for all businesses:

1. Hackers are criminals of opportunity. They are indiscriminate of the business's location, motivations, goodwill, or financial circumstance.
2. Any business leader reading this book could send out a similar letter without proper precautions.
3. The primary and secondary costs associated with ransomware can be devastating. Simply paying the ransom will not guarantee that a business is free to continue normal operations. Cyber insurance can assist with many of these costs.
4. Internal IT staff, while well-meaning and hardworking, may not have the knowledge or resources necessary to help a business recover from a ransomware event in a reasonable amount of time to allow a business to

avoid catastrophe. Cyber insurance can provide for the necessary third-party experts to help a business resume operation.

5. Ransomware can result in continued and prolonged business revenue losses. Cyber insurance can assist with the costs of business interruption.
6. This is not the first, nor the last, company to shut down following a breach of their systems. Adequate cyber insurance should be considered a necessary business expense that could help avoid catastrophe, not just a luxury.
7. Now is the time to act with foresight. This likely includes seeking assistance from legal counsel familiar with cybersecurity and privacy law, a knowledgeable insurance broker well-versed in cyber insurance policies, and competent cybersecurity consultants.
8. Whether or not a business contains PII/PHI/PCI is irrelevant. Criminals will take advantage of any target unlucky enough to fall victim to their ploys.

Damage Control

Business Adversaries

Cyber-criminals

These actors may have no personal vendetta against a business. Their payoff comes from having ransomware injected in your business or stealing your client's personal information, often to file fraudulent returns. It's not personal; it's a criminal enterprise. According to a recent report by *Krebs on Security*, stolen W-2 tax forms are going for between \$4 and \$20 per record depending on the total wages of the affected person. Consider that even small accounting firms could have upwards of a thousand W-2's on file. Likewise, a bank would naturally have large volumes of financial account information, and access to fund transfers. These opportunities represent a payday that may eclipse what a hacker would earn in years of legitimate work in their home country – all in one day.¹³

Employees

This is the most difficult threat to counter as they already have access to your company. Often, employees can damage your network or release information by accident. Occasionally, they will abscond with sensitive information for blackmail purposes or purposefully cripple your network for revenge. In one case, a staff member publicly posted a high-profile client's tax information to the Internet for political purposes. That firm was acquired within a week.

Foreign States

This may seem a strange addition in that your company is unlikely to be directly targeted by a foreign state. But, as was shown with the NotPetya virus, collateral damage is certainly a possibility. The virus was allegedly created by the Russian government to cripple Ukrainian networks. However, the virus quickly spread beyond the boundaries of Ukraine and caused an estimated \$10 Billion in damages worldwide. A British manufacturer, a French construction company, and Danish shipping company were the most high-profile victims of its collateral damage.¹⁴

Random Attackers

This category can include random adolescents and bored adults just looking for a kick. Their motivation to specifically target your business is questionable. These groups often unleash malicious code purely for wreaking widespread havoc. Never

underestimate the power of a low-skilled, but highly, motivated person to cause a disproportionate amount of damage.

Hacktivists

This classification of hacker has an ax to grind. Their motivations can be political, personal, religious, purely for spite, and more. Their methods of attack can range from malware to physical intrusions. Hacktivist groups can prove to be a particularly challenging adversary due to their structure. Anonymous, a particularly well-known hacktivist group, has no structure, no governing body, and no formal membership.¹⁵ Their targets have included the Church of Scientology, the Epilepsy Foundation of America, and Sarah Palin's personal email address.¹⁶

Corporate Espionage & Competitive Intelligence

In a hypercompetitive marketplace, never underestimate unscrupulous competitors. The activities of competitors can range from the entirely legal open source intelligence gathering to decidedly illegal activities. While

Damage Control

Attack Vectors

There is no end to the cryptically named threats facing businesses across the country. It is important to understand how those threats are generally deployed. By understanding the most common threat vectors, a business can consciously do their best to oversee the defenses against them.

Advanced Persistent Threat

This is perhaps the most dangerous threat your business could face. A hacker is specifically targeting your business, and they will stop at nothing. While this type of attack is often perpetrated by large groups or foreign states due to the time requirement, smaller groups and individuals can also be included. Due to the constant threat and varied techniques employed within these attacks, a business is likely to fail in its defense at some point.

Phishing Attacks

Depending on the type, these attacks can also be referred to as “deceptive phishing,” “spear phishing,” and “whaling.” Regardless of the name, they all boil down to a common element of social engineering. The essence of social engineering is that a hacker will attempt to deceive a person into believing that they are someone else – typically, a senior member in the business or a client. The objective is either to steal credentials or have funds transferred to the criminal’s fraudulent bank account.

Brute Force Attacks

These attacks lack sophistication and subtlety. It is all about raw computing power. Often, these attacks attempt to guess every possible permutation of a password until the hacker gains access to your system. Depending on the length and sophistication of your password requirements, this type of attack could be impossible or relatively easy. According to *BetterBuys*, a seven-character password such as, “abcdefg” would take roughly 0.29 milliseconds to crack with a brute force attack. By comparison, a 12-character password would take approximately 200 years.¹⁷

Cryptojacking

While a relatively new type of attack, its effects should not be understated. Cryptojacking occurs when a business has had their computer systems or website accessed by a third party to mine for digital currency. This can not only result in

additional utility costs but may also create unstable computer systems due to the large diversion of their computer resources to assist in perpetrating the crime, further hindering workers from accomplishing their daily tasks.

Businesses should be aware that the prevalence of these intrusions fluctuates in tandem with the costs of various cryptocurrencies. In addition, large businesses are much more likely to be targeted for such schemes because of their concentrated computing power.¹⁸

Man-in-the-Middle Attacks

These types of attacks can come in two forms. The first involves being physically close to the target. In this type of attack, the hackers gain access via an improperly secured router. Once inside the victim's network, they can deploy numerous types of tools to act as an in-between for transmitted information such as banking information and log-in credentials.¹⁹

The second type of man-in-the-middle attack involves the use of malicious code inserted into a business' computer system via infected webpages or email attachments. Utilizing malware such as a keylogger, the hacker can then have log-in credentials and other sensitive data sent back to them at regular intervals.²⁰

Push Payment Fraud Schemes

This particularly insidious fraud attempts to manipulate customers of the business into making payments to fraudsters by impersonating the business. Often, this is done with real-time payment methods, or by setting up fake websites that purport to be made by the business.

Zero-Day Exploits

As the name suggests, these are vulnerabilities that are unknown to the security world until they are used on a broad scale. The ultimate danger of these attacks is that security experts have not yet created a defense to counter the threat. In other words, neither your IT professional nor any other IT professionals in the world is likely to stop this type of threat. Your best defense is your incident response plan.

It should be noted by businesses that many of these threats rely on mass scanning of IP addresses. Attacks against a business can be indiscriminate and originate anywhere across the globe with little to no recourse from law enforcement or legal entities. For any business with a connection to the Internet, there can be no belief in absolute security. A globally connected world equates to globally connected risks.

Damage Control

Forms of Malware

Businesses will often see the following types of malware being discussed but rarely defined. As businesses attempt to make a reasonable effort towards their cybersecurity, they should have a passing understanding of the most common types of malware and how they propagate themselves.

Viruses

Earning this moniker for their ability to infect other computers, viruses require human input to be spread. Their presence can often be unknown by the user. Common avenues of transmission include infected email files and USB drives.

Worms

Unlike viruses, worms do not require human input to be transmitted. Once a worm infects a computer, they use the host computer's resources to spread to other computers across the network or even the Internet. What makes this malware so dangerous is its ability to replicate without user intervention.

Famously the "Iloveyou" worm attacked and infected millions of computers across the world in a single day. After opening the email attachment, the worm would overwrite random file types and then send a copy of itself to every contact in the user's Microsoft Outlook file. This resulted in an estimated one out of every ten computers in the world being infected and resulted in upwards of \$15 billion in damages.²¹

Trojans

In reference to Greek history, trojans mislead users of their actual intent. Often this is accomplished with an email attachment such as a spreadsheet or by clicking on fake advertisements. Once executed, a trojan can be used by the cybercriminal to access the user's personal information such as passwords, banking credentials, and personal information.

Ransomware

Ransomware is a sub-category of trojan that has crippled hospitals, businesses, and, most famously, the government of the city of Atlanta, Georgia in 2018.²² It operates by encrypting files and then demanding a ransom, often in bitcoin. Initially this type of malware contained flaws that would allow specialists to find methods to break the

process and recover files. As the economic windfall has beset the ransomware programmers, their incentive to create ever more effective software has increased. While traditionally the ransomware would begin immediately infecting files, reports now suggest that the ransomware is infecting backups and using higher levels of encryption to force a payment by the infected business.

Often the most successful response to a ransomware event involves the utilization of unencrypted backups. This is one reason that businesses should take a serious look at the periodicity, security, and breadth of their backup information.

Fileless

This especially pernicious form of malware does not actually contain any malicious code that requires installation on a business's computer. All it takes is the username and password of one computer for a hacker to effectively infect the entire network. The methods used by fileless attacks utilize pre-existing operating system tools, which, in turn, pits the computer against itself. This means that detection is incredibly difficult if not impossible for even the most skilled cybersecurity personnel and most security programs. Currently, the best counter to this type of threat is a behavioral detection system.

Common avenues for such an attack can utilize PowerShell and Windows Management Instrumentation (WMI). These tools are already installed on every Windows OS computer and are frequently, and legitimately used by the business's IT professionals for daily tasks. Though a business could outright ban the use of PowerShell and WMI, this would render the network effectively useless as Microsoft has made these tools essential to the use of many of its products.²³

Spyware

Though not as immediately damaging as the other forms of malware, spyware earned its name due to the ability for one person to spy on another. Some businesses are now legitimately using spyware to monitor the engagement of their employees while on the clock.

One form of spyware particularly damaging to a business is known as a "keylogger." Keyloggers function by logging every keystroke and often take screenshots whenever a new program is opened. In turn, this information is routinely sent back to the hacker for inspection. In such a case, an unassuming employee would be providing every username and password to a malicious third party.

Bots

Legitimate bots are used to automatically execute specific operations. A legal example would be starting up your Internet browser every time you open your computer. Hackers naturally value this type of power and can use a bot to execute commands with no direct knowledge by the user. These bots can be used to steal sensitive data, spy on the user, or create a veritable army of computers that can be used to attack other networks via a distributed denial of service (DDoS) attack.

Rootkits

A rootkit is a program which allows remote access of a computer by a third party. Legal rootkits are frequently used by IT professionals to remotely access staff computers to assess problems or install updates. Naturally, this same remote access is prized by cybercriminals who can use this access either directly steal data or install various other forms of malware.

Bricking

Bricking occurs when a piece of hardware is rendered unusable by re-writing or overwriting the firmware of the device. In effect, this makes the device inaccessible at the most fundamental levels as the malware survives a wipe of the system and a reboot.

This term was coined with the idea that it turns the hardware into nothing more than a “brick” because it is no longer useful for any other purpose. This may be done to cover the tracks of the hacker from forensics experts.

Recently, this attack was seen in late 2018 when malware known as “VPNFilter” infected numerous routers. Not only did the malware spy on the traffic being sent through the router, but it could “brick” the device in question with a remote signal from the hacker.²⁴ If a business were to be subject to such an attack, it could not only compromise data including usernames, passwords, and personal information, but it could effectively destroy the device by rendering it totally inoperable.

Action Items:

- ☐ Become familiar with the adversaries, attack vectors, and methods that could be used to infiltrate your business’s computer system;
- ☐ Discuss with your IT professionals, and other stakeholders, how they are countering such threats and if additional investment is needed;

Damage Control

Types of Defense (Controls)

For those who oversee cybersecurity at their business, or for those determining the budget, it is crucial that they have a basic understanding of the most common cybersecurity defenses available. These defenses are generally referred to as “controls” and can be divided or combined into numerous product offerings.

Whether a business requires any, all, or more than those listed below will depend on the cybersecurity framework of the business and various regulatory requirements. In addition, each control listed below can further be segmented into different types. For the sake of brevity, and reader sanity, they will be described in a general fashion.

Employee Training: While not particularly high-tech, employee training can come in many different forms. These range from informal talks at company-wide meetings to tracked computer-based training and fake phishing emails. This control is *crucial* as humans are often the weakest link in any security plan. It is also likely a requirement to meet “reasonable” cybersecurity requirements listed in different laws found throughout this book. An entire chapter is later dedicated to this topic.

Anti-virus and anti-malware software: This type of software is what will most commonly be installed on every business’s computer. In short, it attempts to detect and remove offending software. As threats have increased, these types of software have evolved to protect from viruses, worms, rootkits, keyloggers, trojans, adware, and other common exploits.²⁵

Backups: These take the information you have on your system and create a redundant copy in another location. There are various methods that can be used to accomplish this task including full, incremental, differential, and mirrored backups. No matter what method is used, every business should also be aware of the periodicity, i.e. the frequency, at which backups are being performed. Anything less than daily backups is likely insufficient.

User Permission Segmentation: This limits the access that any one person has to those functions required by their job. Usually, this is accomplished after a successful user-entitlement audit. This can assist in

compliance with various regulatory requirements as well as potentially limit how far a malicious virus can immediately spread within a system.

Data Loss Prevention (DLP) software: DLPs are used to detect potential breaches by monitoring covered data. It can then flag unauthorized use of that data or unauthorized traffic which contains that data. This is particularly important for entities which hold personally identifiable information/personal health information/payment card information (PII/PHI/PCI) as a DLP can be configured to identify this information.

Firewalls: Broadly speaking, firewalls protect the business's internal network from the Internet at large. This is generally done by inspecting information coming from or going to the business's network using a defined set of security rules. Firewalls can be software, hardware, or both.

Intrusion Detection Systems (IDSs): The primary goal of an IDS is to provide an automated inspection of logs and events for intrusions or system failures. In turn, the IDS alerts personnel that an event may be occurring so a timely response can begin.²⁶

Intrusion Prevention Systems (IPSS): An ISP is much like the aforementioned IDS but attempts to proactively prevent or halt intrusions. Due to their similarity, ISPs and IDSs will often be combined and referred to as an Intrusion Detection and Prevention System (IDPS).²⁷

Security Information and Event Management Systems (SIEMS): SIEMS are software that combine Security Information Management (SIM) and Security Event Management (SEM). The goal of this control is to provide real-time analysis of events currently happening on a system. They will contain alarms that are triggered either automatically or through configured inputs.²⁸

Multi-Factor Authentication (MFA): This type of control attempts to utilize multiple factors to authenticate a user. To be useful, they must generally include something a user knows with something the user has. For example, a user knows a username and password and has their cellphone to authenticate the login request. If a user is required to input a username, password, and PIN, this all constitutes what a user knows and

does not include what a user has. Therefore, this last example would not be considered MFA.²⁹

Encryption: The purpose of this control is to secure electronic data by rendering it unusable/unreadable to an unauthorized third party. Businesses can elect to perform encryption at various architectural levels of their system and use different types of encryption.

Vulnerability Scanning: By automatically scanning and probing networks, systems, and applications, third parties attempt to find flaws in security.³⁰

Penetration Testing: This is typically a much more involved process than vulnerability scanning as it attempts to exploit the system being assessed.³¹

Physical Penetration Testing: One of the most overlooked security features; this control attempts limit the access that an unauthorized third party would have to data. This can include a vendor attempting to overcome common security features such as locks, biometrics, card readers, and physical barriers.

Application Whitelisting: This control creates a list of applications and components that are officially authorized to be active. Unlike controls such as an antivirus program which attempt to block bad content while authorizing the rest, whitelisting technologies are meant to permit good activity and block everything else.³²

From the above, it should be understood that there is no one control that will guarantee a breach-free business. Ideally, a business will employ a “defense-in-depth” strategy that encompasses multiple controls that complement and overlap each other. In turn, layers of defense should be employed so that if one control fails, ideally, the next control layer would identify the threat and respond accordingly. Depending on the insurer, the implementation of these controls should lower the business’s cyber insurance premium. In some cases, such controls may be required before insurers offer terms for cyber insurance.

Action Items:

- ☐ Read NIST SP 800-12, Rev. 1, *An Introduction to Information Security*. It can be found for free at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>;
- ☐ Discuss with your IT professionals what controls they have implemented, and if those controls are sufficient for the security the business requires;
- ☐ Determine if additional investment is needed;
- ☐ Determine if there are any preventable holes in your business's defense-in-depth strategy. Compare to the business's cybersecurity framework;
- ☐ Utilize this information when constructing/reviewing your business's incident response plan.

What is “Reasonable” Cybersecurity?

Littered throughout this book are references to various laws that require a business to enact “reasonable” cybersecurity measures. As more jurisdictions, federal regulators, and professional governing bodies mandate that covered entities enact “reasonable” cybersecurity measures, there arises a greater chance that a business could face legal problems for acting negligently.

Most business owners do not want to treat their clients or customers in a negligent fashion. Quite to the contrary, they value their clients and wish to treat them with the utmost care. However, they do not have unlimited resources to devote to cybersecurity, nor should the average business owner be content that “someone else” is handling the sensitive information of their business and clients.

For these reasons, a deeper dive into what is generally regarded as “reasonable” is in order.

Foremost, the legal standard of what a “reasonable” person would have done under the circumstances is not synonymous with what the “average” person would have done. As the American judge and judicial philosopher, Learned Hand, once stated in regard to reasonability, “Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.”³³

Opining on the issue of reasonableness, the FTC has stated, “As the nation’s consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. ... FTC has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one’s security program and defenses. For that reason, the touchstone of the FTC’s approach to data security has been reasonableness – that is, a company’s data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company’s operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC’s cases focus on whether the company has undertaken a reasonable process to secure data.”³⁴

Ultimately, it is true that each business will be judged on a different understanding of “reasonable” cybersecurity controls. However, businesses can look to the various FTC complaints and orders listed below as a starting point to understand how they can best attack the problem.

In the Matter of Eli Lilly and Company: **One employee's mistake can bring an FTC action.**

Eli Lilly is the manufacturer of Prozac, a well-known antidepressant. They had marketed an email service known as "Medi-messenger," which would send various reminders to subscribers concerning their medication and various other highly sensitive matters. After subscribing to the email list, Eli Lilly would disseminate a privacy policy with various – now relatively standard – privacy statements.

A few months after launch, Eli Lilly decided to terminate the email service. Unfortunately for Eli Lilly, one employee allegedly created a computer program to send all the subscribers a simultaneous email. This disclosed the email address of all 669 members enrolled in the "Medi-messenger" program.

The FTC noted that Eli Lilly had allegedly, "failed to provide appropriate training for its employees regarding consumer privacy and information security; failed to provide appropriate oversight and assistance for the employee who sent out the email, who had no prior experience in creating, testing, or implementing the computer program used; and failed to implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email."³⁵

In the Matter of Premier Capital Lending, Inc., and Debra Stiles, individually and as an officer of the corporation: **Businesses that enable remote computer access to their network should assess for appropriate endpoint security.**

Premier Capital Lending (PCL) is a mortgage lender. Through the normal course of business, PCL obtains credit histories or consumer reports for their customers. The FTC alleged that PCL activated and issued a remote login account for a business client to obtain consumer reports usually obtained through PCL. It is further alleged that PCL never visited the business client's workspace, audited the client's computer network to determine if vulnerabilities existed, or assessed their ability to handle, store, or properly dispose of consumer information.

The FTC alleges that later, an unauthorized party hacked into the business client's computer and obtained the login information provided by PCL. This allowed the third-party to allegedly gain access to

approximately 83 consumer reports including names, addresses, and social security numbers.

According to the FTC, PCL's security practices were deficient in the following areas for failing to, "assess the risks of allowing a third party to access consumer reports through PCL's account; implement reasonable steps to address these risks by, for example, evaluating the security of the third party's computer network and taking steps to ensure that appropriate data security measures were present; conduct reasonable reviews of consumer report requests made on PCL's account, using readily available information (such as management reports or invoices) for signs of unauthorized activity, such as spikes in the number of requests made on the account or made by particular PCL users or blatant irregularities in the information used to make the requests; and assess the full scope of consumer report information stored and accessible through PCL's account and, thus, compromised by the hacker."

In the Matter of RockYou: Collect only the information you require for legitimate businesses purposes. Do not store usernames and passwords in plain text.

In this case, it was alleged that RockYou collected email usernames and the usernames for that email. Furthermore, RockYou was alleged to have stored email addresses and passwords in cleartext. This significantly increased the risk of unauthorized access to a user's email address that RockYou had no legitimate need for to perform its business functions.³⁶

Limit administrative access to the minimum number of people. Use appropriate passwords.

In this case, it was alleged that Twitter had granted almost the entirety of its employees' administrative access over the Twitter system. This included the ability for nearly any employee to "reset a user's account password, view a user's nonpublic tweets and other nonpublic user information, and send tweets on behalf of a user." Furthermore, it was alleged that Twitter failed to create and enforce a policy to make administrative passwords difficult to guess. The FTC detailed that Twitter should have enacted password policies that, "(1) prohibit the use of common dictionary words as administrative passwords; and (2) require that such passwords be unique – i.e., different from any password that the

employee uses to access third-party programs, websites, and networks[.]”³⁷

In the Matter of BJ’s Wholesale Club, Inc.: **Keep data only so long as there is a legitimate need.**

BJ’s was a wholesale club where consumers signed up to become members. In return for purchasing a membership, consumers would then often pay for various goods with credit cards and debit cards. Following a purchase, it was alleged that BJ’s would store unencrypted payment card information for up to 30 days after a purchase, though there was no business need for this practice, and it was against bank rules.³⁸

In the Matter of Petco Animal Supplies, Inc.: **Payment card data should be encrypted.**

Petco, a popular animal supply retailer, had consumers who often purchased various items online with payment cards. When a consumer attempted to complete their purchase, they would include their name, address, credit card, and expiration number. It was alleged that Petco would store this information in a database that was connected to the website. As early as 2001, it was alleged that Petco’s website and applications were vulnerable to SQL-Injection Attacks that would allow an unauthorized user the ability to read the plain text of the database which stored other consumer’s credit card information.³⁹

In the Matter of Accretive Health Inc.: **Only use personal information when absolutely necessary, and remove when it is no longer necessary. Sensitive information in transit should be secured properly.**

Accretive Health is a business that assists hospital systems in their revenue operations. This would include services such as billing, collection of past due accounts, and transcription. Due to these services, Accretive allegedly had access to the names, dates of birth, Social Security numbers, and billing information of hospital clients. Among other failures, the FTC alleged that Accretive failed to employ reasonable security measures by, “[u]sing personal information in training sessions with employees and failing to ensure that the information was removed from employees’ computers following the training,” and, “[t]ransporting laptops containing

information in a manner that made them vulnerable to theft or other misappropriation[.]”⁴⁰

In the Matter of Reed Elsevier, Inc. and Seisint, Inc.: **Store passwords in a secure manner. Suspend or disable accounts after a number of unsuccessful login attempts. Two-factor authentication, regular security audits, and penetration testing may be required.**

Seisint was purchased by Reed Elsevier prior to this matter. Among other allegations, the FTC stated that the companies, “allowed customers to store their user credentials in a vulnerable format in cookies on their computers,” and “failed to suspend user credentials after a certain number of unsuccessful log-in attempts.” For these and other alleged fundamental security oversights, malicious actors supposedly exploited the Seisint ID and password provisions. This allowed the actors to steal the sensitive information of several hundred thousand consumers, which led to fraudulent credit cards being issued with subsequent fraudulent charges being made on those cards.⁴¹ In reference to this case, the FTC noted elsewhere that two-factor authentication might have prevented such a breach.⁴²

In the Matter of Rite Aid: **Physical documents containing personal information must be disposed of properly.**

Rite Aid, among other activities, operates a number of pharmacies across the United States. New reports had noted that Rite Aid was disposing of consumers’ personal information, to include pharmacy labels and job applications, in open dumpsters. These dumpsters were accessible by the general public and could have led to identity theft.⁴³ According to the FTC, Rite Aid failed to, “(1) implement policies and procedures to dispose securely of such information, including, but not limited to, policies and procedures to render the information unreadable in the course of disposal; (2) adequately train employees to dispose securely of such information; (3) use reasonable measures to assess compliance with its established policies and procedures for the disposal of such information; and (4) employ a reasonable process for discovering and remedying risks to such information.”⁴⁴

In the Matter of Lookout Services, Inc.: **Implement appropriate authentication policies and procedures.**

Lookout Services is a company that helps employers comply with federal immigration laws. In the course of business, Lookout Services stored information such as addresses, names, Social Security numbers, and dates of birth. Among other alleged failures, the FTC noted that access to sensitive information could be obtained by entering a simple URL into a web browser. Using this method, no username or password was required. In one event, an employee from a Lookout customer allegedly used the word “test” for both a username and a password to gain access to the sensitive information of more than 11,000 consumers. The FTC noted that because Lookout implemented an intrusion detection system and monitored system logs to close out the alleged events, it was unknown if other breaches occurred.

In the Matter of Goal Financial, LLC: **Companies must restrict access to sensitive physical and electronic information.**

Goal Financial is a company that operates in the student loan industry. In the course of their business, Goal Financial collected sensitive information such as addresses, driver’s license numbers, Social Security numbers, and employment information. The FTC alleged that certain employees were able to remove more than 7,000 consumer files and transfer them to third parties. Later, another employee sold hard drives that had not removed the personal information of more than 34,000 consumers. The following selected alleged shortcomings were noted by the FTC: Goal Financial “failed to assess adequately risks to the information it collected and stored in its paper files and on its computer network, failed to restrict adequately access to personal information stored in its paper files and on its computer network to authorized employee,... and failed to provide adequate training to employees about handling and protecting personal information and responding to security incidents....”⁴⁵

In the Matter of Superior Mortgage Corp.: **Sensitive information must remain secure throughout its lifecycle. Businesses must ensure that their service providers secure customer information and address known security risks.**

Superior Mortgage is a company that specializes in residential mortgage loans. Through the course of its business, Superior Mortgage collected sensitive personal information such as Social Security numbers, credit

histories, and payment card numbers. Among other allegations, the FTC noted that the company failed to, “encrypt or otherwise protect sensitive customer information emailed by respondent and its service providers using networks outside of respondent’s computer network,” and, also, “failed to take reasonable steps to ensure that its service providers were providing appropriate security for customer information and addressing known security risks in a timely fashion.”⁴⁶

In the Matter of Fandango, LLC: **Have a process to receive and address security warnings. Security Audits should be thorough.**

Fandango runs an operation that allows consumers to purchase movie tickets through various applications, both mobile- and PC-based. For mobile application security, a typical online service would use Secure Socket Layers (SSL) to establish an authentic encrypted connection with consumers. In the event that an application fails this process, a hacker could prosecute a man-in-the-middle attack. This would allow the third-party to decrypt, monitor, and change the communications between the user and the online service.

The FTC alleged numerous security failures committed by Fandango. Foremost, the FTC alleged that Fandango’s application on iOS failed to validate SSL certificates for roughly four years. Although Fandango had undergone security audits, they were allegedly not broad enough to discover this issue. Furthermore, Fandango allegedly did not have a clear method for receiving security reports from outside parties. Instead, they relied on their general customer service system. Even when a security researcher allegedly informed them of the security issue, the customer service system auto-replied with a stock message on how to reset passwords and marked the matter as resolved. It was not until the FTC staff contacted Fandango that the security matter as allegedly resolved.

The FTC alleged that Fandango engaged in a number of security failures including, “Failing to maintain an adequate process for receiving and addressing security vulnerability reports from third parties[.]” and, “Failing to appropriately test, audit, assess, or review its applications, including failing to ensure that the transmission of sensitive personal information was secure[.]”⁴⁷

In the Matter of ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc.: **Encrypt sensitive data to industry standards.**

Both Hi-Speed Media and E-Babylon are wholly owned subsidiaries of ValueClick. Through the course of their business, the businesses were said to have stored consumer names, billing addresses, phone numbers, email addresses, passwords, credit card numbers with expiration dates, and other personal information. According to the FTC, the companies simultaneously stored such consumer information in a database with no encryption, and in a database with nonstandard forms of encryption. The nonstandard encryption method was said to have used a “simple alphabetic substitution system that was subject to significant vulnerabilities.”⁴⁸

In the Matter off The TJX Companies: **Companies must update and patch their systems appropriately.**

The TJX Companies is a corporation that owned over 2,500 various apparel and fashion stores across the world. Through the course of their business, the companies routinely collected account information, identification card numbers, names, addresses, Social Security numbers, and payment card information. Following a breach of their payment card systems millions of consumers were affected. The FTC alleged that, among other security failures, The TJX Companies, “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts.”⁴⁹

The FTC has noted elsewhere that network and software complexity may lead some companies to require prioritizing patches according to their severity. Nonetheless, a company should have a process in place to ensure that these patches are accomplished properly and within a reasonable amount of time.⁵⁰

In the Matter of Gregory Navone: **Physical security matters. Even if defunct and small, the FTC will enforce actions.**

Gregory Navone was an individual that had owned or directed numerous businesses that appeared to be mainly mortgage brokerage companies. By the time of the FTC action, it was noted that most of Navone’s companies were either no longer operational or were being operated by someone else. During the course of his business, Navone allegedly collected sensitive consumer data; such as names, addresses, dates of birth, Social Security numbers, payment card information, tax returns, and bank statements. The

FTC alleged that Navone kept sensitive consumer information in boxes located in his garage. It was further alleged that forty boxes of intact documents were found in a publicly accessible dumpster outside an office which houses a company owned and operated by Navone.⁵¹

In the Matter of Franklin's Budget Car Sales, Inc., also d/b/a Franklin Toyota/Scion: **Employees should receive regular information security training. Companies should have an incident response plan.**

Franklin's is a franchise automotive dealership. In the course of business, Franklin's collects sensitive consumer information such as names, Social Security numbers, dates of birth, and drivers' license numbers. Among other alleged violations, the FTC stated that Franklin's did not, "adopt policies, such as an incident response plan, to prevent, or limit the extent of, unauthorized disclosure of personal information[.]" and, did not, "[a]dequately train employees about information security to prevent unauthorized disclosures of personal information[.]"⁵²

In the Matter of InfoTrax Systems, L.C and Mark Rawlins.: **Inventory and manage sensitive data. Utilize intrusion prevention and detection systems, penetration testing, file integrity monitoring tools, data loss prevention tools, and input validation. B2B Service Providers will be held accountable.**

InfoTrax is a company whose primary client base consisted of multi-level marketers. These clients used InfoTrax's services to manage many aspects of their business operations. When distributors registered and placed orders, InfoTrax allegedly collected large amounts of sensitive consumer information such as names, dates of birth, addresses, phone numbers, Social Security numbers, and payment card information. According to the FTC, InfoTrax stored the personal data of approximately 11.8 million consumers.

Mark Rawlins was the CEO of InfoTrax. The FTC noted that Rawlins had spent eighteen years at a software company and had studied computer science in college. Allegedly, Rawlins approved InfoTrax's security policies, spoke with clients regularly about data security, and was involved with his company's data security strategy.

The FTC alleged that for nearly two years, a hacker had gained access to InfoTrax's server seventeen times. One of the databases accessed was allegedly legacy data that had not been inventoried, and thus InfoTrax did not know it existed. According to the FTC's timeline, InfoTrax was not

aware of the breach until a server alert indicated maximum capacity because a disk had run out of space due to the intruder's data archive file. Even after InfoTrax discovered the breach, it is alleged that the intruder was able to re-access the system and steal further consumer information.

The FTC noted that InfoTrax allegedly failed to, “detect malicious file uploads by implementing protections such as adequate input validation[,]” and failed to, “implement an intrusion prevention or detection system to alert [the company] of potentially unauthorized queries and/or access to InfoTrax's network; use file integrity monitoring tools to determine whether any files on InfoTrax's network had been altered; and use data loss prevention tools to regularly monitor for unauthorized attempts to exfiltrate consumers' personal information outside InfoTrax's network boundaries[.]” Furthermore, the FTC noted that InfoTrax, “could have addressed each of the failures described... by implementing readily available and relatively low-cost security measures.”⁵³

In the Matter of Credit Karma, Inc.: **Businesses must adhere to their promises about encryption.**

Credit Karma is a business that allows consumers to reference their credit score through a website and online application. During the development of their iOS application, Credit Karma had allegedly authorized its application development firm to use code that disabled SSL certificate validation for testing purposes. Credit Karma allegedly failed to ensure that the production version of their software – which was released to the public – reinstituted the SSL certificate validation. The FTC alleged that these same violations also occurred with Credit Karma's Android mobile applications. By allegedly failing to verify the SSL certificate validation, this would have negated the ability for encrypted and authenticated connections. In turn, this would allow for potential man-in-the-middle attacks that could place consumers at risk. As was stated by iOS documentation, a failure to validate SSL certificates, “eliminates any benefit you might otherwise have gotten from using a secure connection. The resulting connection is no safer than sending the request via unencrypted HTTP because it provides no protection from spoofing by a fake server.”⁵⁴

In the Matter of DSW Inc.: **Network segmentation is a prudent security measure.**

DSW is a footwear retailer with nearly 200 stores across the United States. In the regular course of business, customers purchase items at DSW using payment cards and personal checks. When a purchase was made at a cash register, the information was allegedly transmitted wirelessly to a computer network in the store. This information was then validated and allegedly transmitted back to the register via the same network.⁵⁵

Ultimately, DSW suffered a breach that, according to the FTC, compromised nearly 1.5 million payment cards and roughly 96,000 checking accounts and driver's license numbers.⁵⁶

The FTC noted that this alleged practice, "did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks."⁵⁷

In the Matter of Dave and Buster's, Inc.: **Networks should be monitored for suspicious activity. Restrict third-party access to networks.**

Dave and Buster's is a restaurant/entertainment business with stores across the country. Through the normal course of business, Dave and Buster's collected payment card information. The FTC alleged that Dave and Buster's, "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by employing an intrusion detection system and monitoring system logs; failed to adequately restrict third-party access to its networks, such as by restricting connections to specified IP addresses or granting temporary, limited access; failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization; and failed to use readily available security measures to limit access between in-store networks, such as by employing firewalls or isolating the payment card system from the rest of the corporate network[.]"⁵⁸

For these oversights, the FTC noted that for nearly four months, a malicious actor was alleged to have exploited these vulnerabilities. This resulted in a breach of approximately 130,000 payment cards.⁵⁹

In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava, individually and as officers of GMR Transcription Services, Inc.: **Businesses will be held responsible for the data security of vendors who receive sensitive information.**

Through the normal course of business, GMR would facilitate the transcription of audio files. These audio and transcript files could include sensitive information such as names, social security numbers, dates of birth, tax information, medical histories, examination notes, and driver's license numbers. This service was allegedly completed by assigning non-medical audio files to independent typists in North American. Medical audio files were allegedly sent to a company based in India called Fedtrans.⁶⁰

Notably, the FTC alleged reasonable security measures were not in place because GMR failed to, "require typists to adopt and implement security measures, such as installing antivirus applications, or confirm that they had done so; adequately verify that their service provider, Fedtrans, implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists."⁶¹

In the Matter of CardSystems Solutions, Inc.: **Payment card data should be disposed of as soon as practical. Business are expected to use common, low-cost, defensive measures.**

CardSystems was a payment card processing company that provided merchants with various products and services to facilitate purchases. Through the course of its business, CardSystems would allegedly store millions of daily authorization requests for up to 30 days within its databases.⁶²

Ultimately, a hacker allegedly exploited vulnerabilities in CardSystems' web application and website with a SQL-injection attack. The FTC noted that the hacker was able to abscond with tens of millions of payment card's information.⁶³

The FTC noted numerous alleged failures by CardSystems. Specifically, they had allegedly, "created unnecessary risks to the

information by storing it in a vulnerable format for up to 30 days,” and, “did not implement simple, low-cost, and readily available defenses to such attacks” and, “failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.”⁶⁴

FTC Case Order Outcomes

Due to the length and technicality of the decision and order documents of each case, they will only be generally discussed here. Many of the decisions and orders contain at least five pages of the minimum additional physical, technical, and administrative safeguards that businesses must follow. Generally, these orders last for twenty years and may include bi-annual security assessments conducted by a third party, yearly penetration testing, and quarterly vulnerability testing. Failure to follow these orders could result in additional sanctions by the FTC.⁶⁵ Negative publicity notwithstanding, businesses should consider that it is typically less painful to diligently ensure reasonable cybersecurity practices and avoid regulatory oversight than it would be to fight the case in court. Indeed, one small business that attempted to fight back against the FTC was bankrupted in the process.⁶⁶

The previously detailed actions should give businesses an additional avenue of inquiry into what the FTC considers reasonable cybersecurity practices, and they are encouraged to work with outside experts. Regardless, businesses should understand that there is size or class of business outside the reach of the FTC. LabMD generated roughly \$4 million per year,⁶⁷ and Gregory Navone’s businesses were stated to have been no longer operational or were being operated by someone else.⁶⁸

For any business to assume that they are too small, too distant, or could claim ignorance of the law, a word of warning. In a 2016 panel discussion, FTC Commissioner McSweeney was incredulous that a business could state that “reasonable security” was an ambiguous term. As the Commissioner stated, the guidelines necessary to implement reasonable cybersecurity is, “all over our website.” She continued, stating, “Companies not making any attempts at reasonable security measures are doing so at their own risk.”⁶⁹

Finally, the FTC will likely enforce other cybersecurity controls to be implemented in the future. This could include simulated phishing attacks, simulated ransomware trials, and other increasingly common and relatively low-cost defensive measures. Therefore, businesses should constantly work with the necessary professionals to reassess how reasonable their measures are considering

technological progress. Relying on the notion that the FTC has not explicitly stated a particular cybersecurity control is required is a dangerous game to play.

State Requirements

In addition to the previously detailed FTC necessity for reasonable cybersecurity measures to be enacted at businesses, various states are now adopting similar requirements. Below are a few selected states' mandates:

Florida states within their breach notification law, “**(2) Requirements for data security.**--Each covered entity, governmental entity, or third-party agent **shall take reasonable measures** to protect and secure data in electronic form containing personal information.”⁷⁰

Alabama states, “(a) Each covered entity and third-party agent shall implement and maintain **reasonable security measures** to protect sensitive personally identifying information against a breach of security.”⁷¹

Nevada has included the following language: “A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain **reasonable security measures** to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.”⁷²

Oregon states the following, “A covered entity and a vendor shall develop, implement and maintain **reasonable safeguards** to protect the security, confidentiality and integrity of personal information, including safeguards that protect the personal information when the covered entity or vendor disposes of the personal information.”⁷³

These are but a selection of state laws with reasonable cybersecurity requirements. Businesses should be advised that, generally, the cybersecurity law that applies to the client is based upon the residency status of the client, not the physical location of the business.⁷⁴ Therefore, businesses with multi-state clients, and certainly those with a national presence, likely already fall under some state's reasonable cybersecurity requirement.

Possible Additional “Reasonable” Requirements

What is considered “reasonable” may also include factors such as common industry practices and the knowledge of the business. Consider the case of *Patco Construction v. People’s United Bank*.

Patco is a small contracting and property development business who had been a client of People’s United Bank – under various names – since 1985. Over the course of seven days, there were six allegedly fraudulent withdrawals from Patco’s account when a malicious third party had accurately supplied answers to Patco’s security questions. The bank had allegedly marked each of these transactions as “high risk” because they did not meet the usual parameters historically seen in Patco’s payment orders.⁷⁵

Ultimately, the bank was able to recover, or block, approximately \$243,000 transactions. This resulted in Patco still suffering a loss of approximately \$345,000.⁷⁶

Previously, the bank had utilized an outside vendor to provide its online banking platform. Following the publication of Federal Financial Institutions Examination Council (FFIEC) Guidance on online banking fraud, the bank worked with its vendor to conduct a risk assessment and institute an integrated multifactor authentication system. Through this assessment, the bank had noted that its online banking product was “high risk” and required additional security.⁷⁷

The Appellate Court’s opinion on why the bank did not exact reasonable measures is both multifaceted and complex. The main thrust of the argument was that the bank had ultimately failed to monitor and immediately notify customers of abnormal transactions that were flagged by the bank’s security system. Thus, they did not act in a way that was commercially reasonable, given their industry and knowledge of threats.⁷⁸

Also, businesses should also consider if they would fall under any explicit or implicit professional standards of care that could be used against them in court.

For example, attorneys need to abide by various ethical rules that govern their conduct. One such potential rule is Model Rule 1.6, which states, “A lawyer shall make **reasonable** efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”⁷⁹

Comment [18] of Model Rule 1.6, among others, discusses how reasonableness will be determined for lawyer:

“Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards

adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules."⁸⁰

Other professionals may also fall under heightened duties of care that would require diligence above a reasonable-person standard. Professionals should consult legal counsel and their governing bodies to determine any additional requirements.

Regardless of industry, business size, or sophistication, demonstrating reasonable cybersecurity is no easy task. Frankly, many business owners have neither the time nor the expertise to make an educated determination on the ongoing reasonability of their cybersecurity policies, practices, and procedures. For these reasons, it is highly advisable for businesses to seek continuing outside assistance to meet their unique requirements. This can come from compliance experts, legal assistance, training resources, and the like.

Action Items:

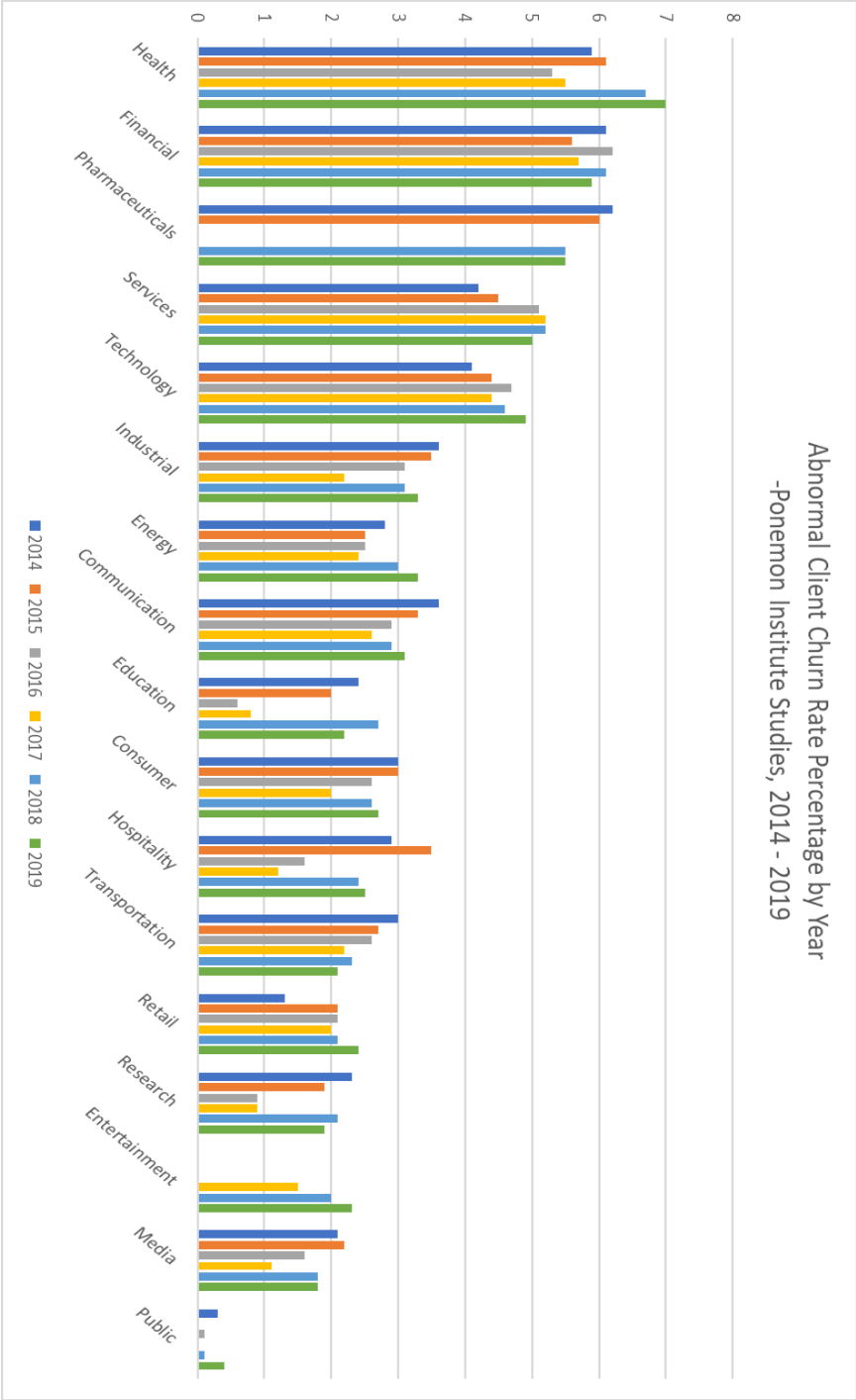
- ☐ Work with legal counsel to determine if your business has enacted reasonable cybersecurity requirements;
- ☐ Work with cybersecurity and compliance specialists to assist in assessing your business's current cybersecurity posture;
- ☐ Determine if any additional investment is needed to meet your unique reasonable requirements;
- ☐ Communicate this information to other stakeholders and IT staff.

Will I lose clients after a breach?

Businesses are rightly concerned that clients will leave following a breach. After all, many professional services organizations such as accountants, doctors, lawyers, architects, information services professionals, and engineers, all depend heavily on their client's trust. For most retailers, customer relations keep the doors open when the Internet or competitors can offer the same products at a lower price.

The initial question is whether the fear of clients leaving is justified, and, if so, to what degree? On the next page is a chart that details abnormal client churn, by industry, across a six-year span.⁸¹

From this chart, a couple of trends can be extrapolated:



- For most industries, there was a lull in abnormal churn in the middle of the data set. The number of clients leaving post-breach generally appears to be *increasing*.
- Healthcare, financial services, pharmaceuticals, service industry, and technology industries will have the greatest difficulty in retaining clients following a breach. Public sector industries typically have minimal turnover as customer alternatives may be non-existent.
- These metrics deal with the percentage loss of customers, not the loss of revenue.⁸² This is an important distinction. If any business were to lose the top 4% of clients by revenue, that could lead to disastrous financial results.

Certain cyber insurance policies may indemnify a business for a loss of client revenue. However, this coverage feature may not be available to certain classes of business, or it may be exceedingly difficult to evidence such losses to an insurer. Broadly, reputation loss coverage is demonstrated by comparing past revenue with projected, future revenue. Because this coverage feature has only been available during economic growth, it is unknown how an economic downturn would affect reimbursement calculations. Furthermore, the timeframe that an insurer will pay for losses is quite limited when compared to the lifespan of a business attempting to regain customers or attract new ones.

Businesses should also be aware that breaches not only lose current customers but can diminish the rate of new customer acquisitions. For customers who remain with the business, there is a definite but unmeasurable element of goodwill that has been lost.⁸³

Non-material errors committed by the business while providing services to clients is a fact of life. Yet, when these errors are combined with one or more breaches in close proximity, it is likely only a matter of time until the client starts looking for an alternative. Those clients will have to go somewhere, and it would be all too easy for a competitor to use data-security as a selling point.

Future Trends

As stated previously, the number of clients leaving following a breach is generally on the upswing. However, as the threats to clients evolve, so too will the percentage of clients that walk out the door never to return. Consider the following letter recently posted by a doctor's office:

“Dear Current or Former Patients of [REDACTED]:

I am dismayed to report that in early November of 2019, The Center [REDACTED] located in [REDACTED], was the victim of a criminal cyberattack. On November 8, 2019, I received an anonymous communication from cyber criminals stating that my “clinic’s server (was) breached.” The hackers claimed to have “the complete patient’s data” for [REDACTED] that “can be publicly exposed or traded to third parties.” They demanded a ransom negotiation, and as of November 29, 2019, about **15-20 patients have since contacted [REDACTED] to report individual ransom demands from the attackers threatening the public release of their photos and personal information unless unspecified ransom demands are negotiated and met.**

On November 12, 2019, I filed a formal complaint with the FBI Cyber Crimes Center, and two days later met with the FBI where they recorded detailed information regarding the cyberattack and ransom demands. The investigation is currently ongoing. The FBI requests that patients receiving ransom demands file an independent cybercrime complaint online at www.ic3.gov. For my part, I have installed new hard drives, firewalls, and viral/malware detection software in hopes of reducing exposure to future cyberattacks, but no system is foolproof, and even the United States government with all its resources has been victimized repeatedly. While upgrading my defenses clearly won’t help those individuals whose data has already been stolen, there is reason to suspect that the theft of patient photographs may be limited to only a very small number of individuals – mostly those patients who used email to send or receive their photographs – so the upgrades may prove useful. However, personally identifiable information (PII) may have been stolen for up to 3,500 former or current patients of [REDACTED]. Because we store PII as the scan of the patient’s intake demographic questionnaire, and not in an electronic demographic database, obtaining contact information in order to individually notify all 3,500 patients has been painstakingly slow and labor intensive, and access to the data has been hindered by ongoing IT service disruptions. Consequently, as an interim notification measure, I have posted this advisory on my website pending individual notifications. Also, kindly disseminate this information to anyone else that you know is a patient of record at [REDACTED].

I deeply regret that individuals currently or formally under my care have been victimized by this criminal act, and I urge you to monitor your financial information closely. A photocopy of your driver's license (or passport for foreign nationals), home address, email address, telephone number(s), and insurance policy numbers (when applicable) were routinely kept on file for most patients, as well as credit card payment receipts (which typically reveal only the last 4 digits).

Please contact [REDACTED] at [REDACTED] or at [REDACTED] for any questions regarding this unfortunate matter. I am sickened by this unlawful and self-serving intrusion, and I am truly very sorry for your involvement in this senseless and malicious act.

Sincerely,

[REDACTED] 84

While the prior cybersecurity practices of the business could be critiqued, that is immaterial to this discussion. What is pertinent is whether any former or future client reading that letter will now have second thoughts about conducting business with this doctor's office. The resounding logical answer would be yes!

For the above reasons, businesses must consider cyber insurance indemnification for a loss in revenue due to abnormal client turnover. However, they should keep in mind that certain long-term losses, such as difficulties attracting new clients and a loss of goodwill, may prove costly. Reasonable cybersecurity practices, policies, and procedures that may avoid a breach altogether may prove more expensive in the short-term but could certainly prove cost-effective in the long run.

Action items

- ☐ Work with a cyber insurance specialist and/or legal counsel to check for reputation loss coverage;
- ☐ Understand how your business must demonstrate a loss to your various insurers;
- ☐ Communicate this data to relevant stakeholders and IT staff;
- ☐ Update your incident response plan as necessary.

Ransomware and the Potential of Breach Notification

Ransomware is a serious issue that can readily cripple the operations of a business. While the issue of whether to pay the ransom is a contentious one, it is beyond the scope of this book.⁸⁵ What is within the scope of this book is how a ransomware event could require notification. Many businesses assume that they can restore their system to the latest backups and go about their day leaving others none the wiser. Often, these same businesses will balk at the suggestion of legal counsel to spend additional funds by retaining computer forensic experts to further investigate the breach.

While the average professional may assume that ransomware couldn't require breach notification, and thus negating the need for additional expenditures, this is not always the case.

Ransomware - Evolved

As stated by the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) ransomware is, "Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website."⁸⁶ Ransomware most commonly encrypts files and then demands a ransom via cryptocurrencies.

Like all forms of malware, ransomware has evolved significantly since its inception. Businesses need to understand that ransomware can be used not only as a standalone attack but also in conjunction with other attacks.

As early as 2016, a new attack vector was discovered that combined the elements of both data theft and ransomware.

Known as "Betabot," this malware was previously known to steal passwords and banking information. When end users enabled macros from an email attachment, the malware was activated. Once the theft was complete, there was no longer any use for the Betabot malware.

In 2016, the malware authors began to include a ransomware payload in conjunction with the data theft. Once the theft was complete, the Cerber ransomware payload was activated to extract additional potential revenue for the hackers.⁸⁷

As time progressed, this approach has also been utilized by hackers to further obscure their efforts. When a business experiences a ransomware attack, their first step is to often restore from their backups. If the ransomware was being used to obscure previous data theft, otherwise well-meaning IT personnel may have

inadvertently destroyed many of the forensic clues that could have demonstrated the theft. Because the business appears to have resumed normal operations, little thought is put towards spending additional funds on what is apparently a needless forensic investigation. This increases the shelf-life of any stolen information and makes the job of law enforcement nearly impossible.⁸⁸

Even if a business experiences a more traditional ransomware attack, they should not simply assume that the presence of backups, even off-site and in the cloud, will be enough to avoid trouble.

For example, take allegations found in the case of *United States of America v. Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri*.

Starting in late 2015, Savandi and Mansouri allegedly began to encrypt computers using a form of ransomware called “SamSam.” While their attack vectors allegedly varied, they ultimately hacked, encrypted, and demanded a ransom from more than 200 victims. As a result, the hackers pocketed more than \$6 million in ransom payments while their victims incurred losses exceeding \$30 million.⁸⁹

While most ransomware attacks rely on automated attack mechanisms that take advantage of anyone unfortunate enough to be infected, the perpetrators of SamSam were much more discerning. As alleged in the case, Savandi and Mansouri conducted “reconnaissance and research” to select their victims, often for weeks at a time. Once inside the victim’s network, they would conduct scans to identify computers for encryption. Once finished, they would install their ransomware on as many computers as possible before simultaneous activation, often outside of working hours. To inflict as much damage as possible, and to further encourage a ransom payment, Savandi and Mansouri **would often encrypt the backups**.⁹⁰

More than 200 victims, including Kansas Heart Hospital, The City of Atlanta, The City of Newark, Medstar Health, Hollywood Presbyterian Medical Center, The Mercer County Business, The University of Calgary, and the Port of San Diego fell victim to their targeted schemes. As noted within the indictment, “Without use of their data, most Victims were unable to function normally; many had to shut down or drastically curtail their operations. These devastating attacks often caused substantial losses to the Victims.”⁹¹

Following the indictment of Savandi and Mansouri, ransomware attacks have continued to become more menacing. A simple evolution has been seen in the “Ryuk” ransomware. Initially, it attempts to stop any anti-malware software on the system. It can also install different versions of itself based upon the architecture of the network. From there, the ransomware also uses “anti-forensic recovery techniques,” which make recovering from backups more difficult. In addition, the malware also includes the theft of credentials and remote monitoring of the workstations. Outside of the

ransomware attack, the credentials can be sold to other nefarious actors for additional attacks or exploitations.⁹²

Another evolved method of ransomware attack is referred to as an “attack loop.” This type of ransomware infects a computer system but lies dormant. While the business continues to utilize backups, it could inadvertently also be backing up the ransomware. When the ransomware does eventually activate, it could take down weeks, and possibly months, of backups.⁹³ Naturally, this could force a business to pay the ransom as it has rendered its backups effectively useless. Should a business attempt to restore from backups that are unknowingly infected with a dormant ransomware package, they are only setting themselves up for another attack, and additional downtime.

Mobile Ransomware

The threat does not end with business computers attached to their parent network. As the Bring Your Own Device (BYOD) movement becomes ever more ubiquitous and necessary for businesses to operate, it has only given malicious actors yet another attack vector. For cybersecurity and IT professionals, BYOD is often jokingly referred to as “Bring Your Own Disaster.”⁹⁴ More than half of people do not password-protect their mobile devices.⁹⁵ Over one-third have no anti-theft or anti-virus protection installed in their mobile device.⁹⁶ Regardless of the operating system used, the majority of users were using outdated operating systems with inferior security features. Security professionals have little to no oversight on the applications downloaded by users, but 25% of mobile applications have a minimum of one high-risk security vulnerability.⁹⁷ Nonetheless, users continue to access personal information such as bank accounts and business emails, which may contain PII/PHI or sensitive client information.

Mobile ransomware is not a new threat, but it has been forecasted that 2020 will see the first focused attacks on mobile devices.⁹⁸ As these devices continue to gain more prominence in daily business activities, it is increasingly likely that businesses will need to respond to ransomware events on devices owned by third parties. According to a recent study, roughly 80% of companies were confident that they would detect a mobile event. However, 63% of the cases were initiated by notification from customers, partners, or law enforcement. This is not surprising as the study identified that only one-third of respondents had implemented even one basic mobile security measure.⁹⁹

Businesses should proactively work with legal counsel to understand what potential legal obligations they may encounter following a mobile ransomware event.

In turn, businesses should also work with competent vendors and consultants to assess their mobile device security practices and controls.

HIPAA

Due to the increasing threat of ransomware attacks against healthcare entities, the US Department of Health and Human Services (HHS) issued explicit guidance to both covered entities (CEs) and business associates (BAs) on their view of ransomware attacks. Setting the stage for later guidance, HHS noted that malicious third parties may “deploy ransomware that also destroys or exfiltrates data, or ransomware in conjunction with other malware that does so.”¹⁰⁰

Under HIPAA, a breach is defined as “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of PHI.”¹⁰¹ HHS takes the presumptive position that any ransomware attack which affects ePHI qualifies as a breach. This is because the encrypted ePHI was “acquired,” and the “disclosure” is forbidden under the HIPAA Privacy Rule.¹⁰² Consequently, the mere encryption of data appears to qualify as an unauthorized “acquisition” under HIPAA; potentially requiring notification.

For a business to demonstrate a low probability that the PHI was compromised, and thus avoid notification requirements, *at least* four risk factors must be accounted for in a risk assessment.

- “(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
- (iii) Whether the protected health information was actually acquired or viewed; and
- (iv) The extent to which the risk to the protected health information has been mitigated.”¹⁰³

HHS ‘encourages’ additional factors to be considered, such as if there is a “high risk of unavailability of the data or high risk to the integrity of the data. If so, these additional factors may indicate a “compromise” and could require notification to affected individuals.

State Breach Notification Laws

While every state’s breach notification is different and can change without notice, they are generally concerned with an unauthorized third-party accessing and acquiring covered data. Furthermore, many of these laws also include notification

exemptions if the event does not pose reasonable harm to the client. This is often accomplished with an explicit or implied risk of harm analysis.

As of publication, the authors could find no instance where any of the various state authorities have officially dictated whether the mere presence of traditional ransomware may require notification. Logically, a traditional ransomware event only encrypts data but does not view or steal it.

In a minority of states, a lower standard exists that may prompt notification following a ransomware event. For example, residents of Connecticut,¹⁰⁴ New Jersey,¹⁰⁵ and Puerto Rico¹⁰⁶ may require notification if there was merely unauthorized access to covered information. Note that there is not necessarily a requirement for a hacker to have access to covered data. When taking these lower notification thresholds into consideration, it is best to seek further guidance from legal counsel.

Contractual Requirements/SEC

Businesses are increasingly consenting to various contractual clauses that may require notification to clients should their information fall victim to a ransomware attack. Whether those contracts require notification in the event of “access,” or if the information must also be “acquired” will depend upon the exact language of the contract. Due to the ambiguity in this area, it is advisable that businesses work with legal counsel before signing any contracts and seek clarification on this topic.

Businesses working with publicly traded entities, or publicly traded entities proper who must adhere to SEC oversight, could be more likely to face such requirements. This is due to increasing scrutiny from the SEC regarding how publicly traded companies are *de facto* required to disclose cybersecurity incidents. From the SEC’s February 2018 statement: “Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion[.]”¹⁰⁷

Final Thoughts

The heart of the problem is that few businesses or their IT staff can make a forensic determination on whether there is credible evidence that information was acquired or not. From an unbiased third-party view, it is just as reasonable to assume information *was* stolen as to assume it wasn’t. If information requiring notification was stolen, but there are no defensible documents supported by a forensics expert that negated the reasonable need for notification, it is possible that regulatory bodies and litigators would take a keen interest in this development. The additional cost to conduct the

forensic investigation – and potentially provide notification to those affected – may very well be dwarfed by the additional costs imposed by defending claims alleging a failure to notify. Should the opposing party win the claim, it is feasible that the affected business would be required to conduct the forensic examination and notification anyways.

Regardless, every business should consider consulting appropriate legal counsel to determine how the various cybersecurity and privacy laws could mandate disclosure following a ransomware event. Due to the ever-evolving nature of ransomware and its potential to steal and abscond with information, act as a ruse to cover data theft, or lie dormant in backups to strike again at a later date, it is advisable that businesses understand that it is generally within their best interest to retain computer-forensics experts to avoid additional trouble and costs. In general, in-house or contracted IT staff will not have the capacity to make a legal determination regarding the motives and methods of the ransomware attack to the satisfaction of regulatory bodies or law enforcement. Nor will they necessarily have the ability to ensure no information was stolen or that any additional malware is not lurking dormant in other files, waiting to strike again.

Action Items

- ☐ Review: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. Found for free at: <https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect;>
- ☐ Review: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. Found for free at: <https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond;>
- ☐ Work with legal counsel to determine your breach notification requirements *before* a breach;
- ☐ Communicate this information to relevant stakeholders and IT staff as necessary;
- ☐ Determine if your business could enact additional cybersecurity measures – such as encryption – to lessen the probability of breach notification to requirements;
- ☐ Update your business's incident response plan as necessary.

The Crucial Role of Employee Training in Cybersecurity

Cybersecurity should not and cannot be regarded solely as a technical problem for the IT department to solve. When an employee receives a fabricated request to wire funds, or they contemplate opening a strange attachment sent unwittingly by a breached vendor, employee training will often be the deciding factor between business as usual or disaster. As the incidents of ransomware, cybercrime, and social engineering increase, cybersecurity is more than ever a human problem that requires constant training and vigilance. Legal requirements notwithstanding, every business should look at employee training if for no other reason than self-preservation.

Below are business insights that management should consider when deliberating on the topic of employee training:

- Businesses cannot assume that those making the software will inherently include background security features. One study of computer science students writing code showed that *not one* student stored passwords securely without being explicitly told to perform this function.¹⁰⁸
- A study published in the *Journal of Management Policy and Practice* showed that only roughly one out of five users learned information security best practices on their own accord.¹⁰⁹ Thus, without management intervention, it is unlikely that the workforce at large will learn the proper cyber-hygiene practices necessary to keep a business safe.
- Employees focus on what management emphasizes and measures. If management gives lackluster, infrequent, and generic employee security awareness training, employees can rightly assume that it is not a business priority. When management enforces consistent, useful, and detailed training with stern reminders for non-compliance, cybersecurity awareness will become a priority for employees.¹¹⁰ In other words, a business gets what it measures.
- When a breach inevitably occurs, The Ponemon Institute consistently ranks employee training as one of the most effective factors in decreasing the cost of a breach.¹¹¹ This is likely due to employees being confident in identifying and reporting suspicious activity before the severity of the breach could escalate further. Indeed, the 2019 report from the Ponemon Institute listed employee training as contributing more to the decrease in breach costs than

having an artificial intelligence platform, board-level involvement, or having a Chief Information Security Officer (CISO) appointed to a business.¹¹²

- As the personal use of business devices increases¹¹³ and personal devices are increasingly used for business purposes,¹¹⁴ the ability for a company's team to enact exacting cybersecurity measures will continue to erode. Thus, end-user training will become even more crucial.
- One study found that 50% of people received *at least* one phishing email per day, but 97% could not identify it as so. With awareness training, the susceptibility of an employee to fall for a phishing scam fell by a reported 75%.¹¹⁵
- According to one study, **human error or human behavior accounted for a shocking 90% of all cyber claims.**¹¹⁶ Naturally, addressing this metric with appropriate training is a worthwhile investment.
- As stated elsewhere in this book, a key component to every business is client retention. Existing clients will increasingly leave following a breach, and new clients will be harder to attract due to the negative publicity.¹¹⁷ The failure to enact consistent employee training could result in future financial difficulties for the business. Employee training should be considered an investment in the current stability, and future viability, of every business.

Legal Considerations

Increasingly, businesses also understand that employee training is likely a *legal requirement*. Recall from previous chapters that the FTC –“the nation's consumer protection agency”¹¹⁸ – has enforced actions against companies ranging from small car dealerships to blood testers, and mortgage companies to software providers. Seemingly, no size or type of business is immune from their reach. As stated by FTC Commissioner McSweeney, reasonable cybersecurity includes “having a process, appointing responsible people for implementing the process, **providing training**, and so on ... Companies not making any attempts at reasonable security measures are doing so at their own risk.”¹¹⁹

Certain states may also explicitly require employee training to demonstrate reasonable cybersecurity. Businesses should be reminded that generally, the cybersecurity law that applies to the client is based upon the residency status of the client, not the physical location of the business.¹²⁰ Failure to follow the mandates of these requirements can lead to severe legal and financial difficulties, potentially by one or more states.

For example, Oregon requires that “[a] covered entity and a vendor shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information, including safeguards that protect the personal information when the covered entity or vendor disposes of the personal information.” Later in the statute, Oregon advises that a covered entity will be deemed to be in compliance if it “[i]mplements an information security program that includes: ... Training and managing employees in security program practices and procedures with reasonable regularity[.]”¹²¹

Effective March 1st, 2020, New York’s SHIELD Act will require covered entities to implement reasonable safeguards. Among these safeguards is the mandates that a covered business “trains and manages employees in the security program practices and procedures[.]”¹²²

Under the California Consumer Privacy Act (CCPA), and California law in general, businesses can face harsh penalties for non-compliance. Unfortunately, it does not appear that CCPA or any applicable California law definitively states what reasonable security entails and whether employee training is required.

However, a 2016 California Attorney General Breach Report includes recommendations that could point to a source for interpretation. As stated within the report, “The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”¹²³

The relevant employee training portion of The Center for Internet Security’s Critical Security Controls (CIS CSC) will be covered shortly in greater detail. Suffice to say, CIS CSC includes employee training as a critical control.¹²⁴ Consequently, employee training is likely a *de facto* requirement in California.

Failure to have documentation of employee training – a potentially easy-win victory for California regulators – could result in serious penalties. The attorney general can seek civil penalties up to either \$2,500 per violation or up to \$7,500 per intentional violation.¹²⁵ While the law is currently unclear, as written, it is conceivable that the Attorney General could levy these fines *per employee* for failure to implement a cybersecurity awareness training program.

As businesses begin to take employee security awareness training seriously, the question of training frequency commonly arises. Yet, it does not appear that the FTC, any state, or any governing body requiring employee training, has ever opined on the minimum mandatory training frequency. To gain a more complete understanding of

employee training frequency, businesses should look toward the NIST Cybersecurity Framework (NIST CSF).

In regards to NIST CSF, the FTC has stated “...the Framework and the FTC’s approach are fully consistent: The types of things the Framework calls for organizations to evaluate are the types of things the FTC has been evaluating for years in its Section 5 enforcement to determine whether a company’s data security and its processes are reasonable.”¹²⁶ Anecdotally, of the states which do have these requirements and list mandatory minimum cybersecurity safeguards, they likewise appear to be heavily influenced by NIST CSF.

As stated by the FTC, “[m]any FTC cases highlight companies’ alleged failures to implement reasonable data security practices that the Framework emphasizes under the Protect function.”¹²⁷ For clarity, employee training is an element found within the Protect function.

Within the Protect function, NIST CSF PF.AT-1 states, “All users are informed and trained.”¹²⁸ Digging further into the informative references section of that subcategory, CIS CSC 17.3 states that employers should “Create a security awareness program for all workforce members to complete on **a regular basis** to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization’s security awareness program should be communicated in a **continuous and engaging manner**.”¹²⁹

So, when the FTC, or the various states, speak about employee training, they are likely referring to engaging content that is conducted on a regular basis.

It is unlikely that most businesses have the expertise or resources to create organic, in-house video content that meets legal requirements. According to one study, the most common approaches to user awareness training were emailed or printed lists. Only roughly one-third of companies are currently using the most effective employee training style, regularly scheduled interactive videos.¹³⁰

Employee Claim Considerations

With all the external requirements regarding employee training, businesses should not ignore the fact that they are likely holding the PII of employees for tax purposes. Thus, a breach of data could very well lead to a claim against an employer by their own employees. Consider the allegations in the case of *Curry v. Schletter, Inc.*

Curry and other class plaintiffs were then-current or former employees of Schletter, Inc. Schletter, Inc. was a part of Schletter Group, a worldwide manufacturer and distributor of solar panels.¹³¹

As a condition of employment, Schletter required employees to submit personal information for tax purposes. This included name, address, date of birth, and social

security numbers. The plaintiffs alleged that they relied upon Schletter to keep this information secure.¹³²

On approximately April 19, 2016, Schletter sent a letter to all current and former U.S. employees that their previous year's W-2 tax form had been sent to an unauthorized third party. This allegedly occurred due to an email phishing scam.¹³³

The plaintiffs alleged that their employer, Schletter, should have understood these types of scams existed. In their claim, they include mention of an FBI report warning of these scams, a publication from prominent cybersecurity journalist Brian Krebs detailing the danger of these activities, and an IRS warning issued to all payroll and human resources professionals to be on the alert.¹³⁴

Of particular interest to this discussion, the current and former employees alleged, among other claims, the following misdeed by their employer: "[T]he Defendant provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure. Specifically, the Defendant failed to adequately train its employees on even the most basic of cybersecurity protocols, including: (a) how to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate; (b) effective password management and encryption protocols for internal and external emails; (c) avoidance of responding to emails that are suspicious or from unknown sources; (d) locking, encrypting and limiting access to computers and files containing sensitive information; (e) implementing guidelines for maintaining and communicating sensitive data...."¹³⁵

Businesses rightfully concerned with even one of the issues and benefits listed above should implement an appropriate employee security awareness training program. Because most businesses will not have the capacity or expertise to consistently create in-house content, this will likely be accomplished by partnering with a qualified vendor to ensure maximum effectiveness and compliance.

Action Items

- ☐ Assess your company's current employee training frequency, depth, and expertise;
- ☐ Work with legal counsel to determine your unique security training requirements;
- ☐ Readers of this book can visit www.HailBytes.com and use coupon code CPLBROKERS for a discount on each employee's monthly training cost.

Data Retention is a Cybersecurity Issue

In 1981, it cost roughly \$500,000 for a gigabyte of storage. As of 2017, the cost had fallen to an astounding three cents per gigabyte.¹³⁶ With that exponential decrease in price came a seemingly exponential increase in the amount of information that businesses held indefinitely. Whether this was a conscious decision or naturally developed over time is dependent on the business. Regardless of motives, it is not uncommon for businesses to have no grasp on the amount and type of information they are storing. Although data retention and destruction policies are rarely addressed, unchecked and unmonitored data retention is longer advisable and may be contrary to various state and federal laws.

In the context of a data breach, larger volumes of unnecessary records can result in a windfall of negative ramifications. Below are a few of the negative side effects:

- With larger data sets to comb through, the time and cost of the forensic examination can increase and become unwieldy.
- Because breach notification laws vary wildly, a business risks notifying residents and regulators in an untimely fashion, potentially violating states' particular statutes.
- Unnecessary breach notification letters and credit monitoring programs require additional cost, eroding available insurance limits.
- A greater disparity from the data breach event to notification might trigger fines and penalties from various states.¹³⁷ As costs mount, the insurance limits to pay for legally required costs diminishes.
- Larger data breaches increase the odds of litigation.¹³⁸ Should a business find themselves in this unenviable position, the cost to prepare and respond to such litigation will increase due to a larger volume of information that requires sorting. This could further erode insurance limits.¹³⁹
- Businesses risk eroding their cyber insurance limits and might be required to pay for breach costs with business funds. For those businesses holding relatively small cyber insurance endorsements, this could prove financially catastrophic.

- As breach costs increase, actuaries from insurance companies will likely look to recoup those costs by increasing policy costs at renewal. In certain circumstances, they may outright decline to offer renewal terms.

While the disposal of unnecessary data has always been a logical business practice, it may increasingly become a compliance requirement. As of publication, more than half of all states have enacted legislation that requires the destruction or disposal of covered information.¹⁴⁰ As an example, here are a few of the state laws dealing with data destruction:

Alabama Data Breach Notification Act of 2018

Per Alabama's Data Breach Notification Act of 2018, companies that own sensitive PII of Alabama residents will be required to adhere to the state's data disposal rules. Namely: "A covered entity or third-party agent shall take reasonable measures to dispose, or arrange for the disposal, of records containing sensitive personally identifying information within its custody or control when the records are no longer to be retained pursuant to applicable law, regulations, or business needs. Disposal shall include shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards."¹⁴¹

New York "SHIELD" Act

As covered elsewhere in this book, the Stop Hacks and Improve Electronic Data Security Handling ("SHIELD") Act is due to become effective in 2020. Subject to a revenue exception, businesses are required to implement various physical security safeguards¹⁴² if they own or license digital data of New York residents.¹⁴³ Notable to this discussion, businesses must implement a process that:

"(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information, and;

(4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed."¹⁴⁴

Oregon Identity Theft Prevention Act

“(1) A covered entity and a vendor shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information, including safeguards that protect the personal information when the covered entity or vendor disposes of the personal information.”¹⁴⁵

In addition, covered entities shall implement physical safeguards such as:

- “(i) Assessing, in light of current technology, risks of information collection, storage, usage, retention, access and disposal and implementing reasonable methods to remedy or mitigate identified risks;
- (iii) Protecting against unauthorized access to or use of personal information during or after collecting, using, storing, transporting, retaining, destroying or disposing of the personal information, and;
- (iv) Disposing of personal information, whether the covered entity or vendor disposes of the personal information on or off the covered entity's or vendor's premises or property, after the covered entity or vendor no longer needs the personal information for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.”¹⁴⁶

Revisiting FTC Requirements

Recalling the previously detailed case of *In the Matter of BJ's Wholesale Club, Inc.*, in this matter, the FTC had alleged that BJ's stored information for longer than was needed for their legitimate business needs.¹⁴⁷

Certainly, the extensive list of required practices following the consent order would be onerous for most businesses. These requirements included but were not limited to implementation of a comprehensive information security program containing administrative, physical, and technical safeguards, biennial security assessments prepared by a CISSP, CISA, GIAC, or similarly qualified person; a five-year retention requirement for any documents related to the order; and a three-year document retention requirement for all assessment-related material.¹⁴⁸

As with everything cybersecurity-law related, no individual state or federal retention requirement should prove particularly burdensome to follow. When businesses begin to make a good faith effort to follow all applicable state and federal laws, compliance can quickly become a morass of seemingly vague and/or conflicting requirements. Specific businesses may also have federal, international,

and professional data retention and destruction standards included as complicating factors. To adequately tackle data retention and destruction efforts, businesses will likely need both legal assistance and a technical solution. These business partners can further advise on legal safe harbors, resolution of conflicting laws, possible exemptions, and semi-automated data retention and destruction solutions.

It is likely that some businesses will find the upfront cost to deal with data retention compliance costs unpalatable. However, the benefits listed previously, as well as the potential legal ramifications for lack of adherence, should certainly provide motivation for businesses to address this often-overlooked facet of cybersecurity.

Action Items

- ☐ Work with legal counsel to determine your business's unique data retention requirement;
- ☐ Communicate this information to relevant stakeholders and IT staff;
- ☐ Determine if your business is adhering to its own appropriate data retention and destruction policy.

The Limits of Cyber Insurance

Regardless of size, industry, or location, every business is a target for hackers. Therefore, it goes without saying that every business should contemplate their cyber exposure and obtain appropriate coverage. As mentioned at various points throughout this book, cyber insurance is not the cure to all potential digital maladies. For clarity, below are some of the compelling reasons found throughout this book on why cyber insurance should be viewed as only a piece of the cybersecurity puzzle and not the primary method for a business to defend against cyber losses.

- Even if listed as a coverage feature, not all fines and penalties will necessarily be insurable by state or national law.
- Should a business be found to lack reasonable cybersecurity measures, as with many FTC enforcement actions, the ongoing cost to comply with consent orders over many years is generally uninsurable though quite substantial.
- The revenue lost due to a legal injunction, such as a court order which directs a business to refrain from or accomplish specific acts, may not be insurable.
- Data breaches can create long-term damage to a brand's identity, resulting in a slew of negative repercussions for an indeterminable amount of time.¹⁴⁹
- Data breaches can drive otherwise happy customers away. As is well understood in the business community, it is much easier and cost-effective to keep existing customers than it is to attract new customers.¹⁵⁰ While certain policies may contain coverage for reputational loss, the indemnification period in those policies is finite. A customer may simply elect to never return.
- It is increasingly more likely that contracts will require minimum cybersecurity measures. Attempting to enact numerous adequate cybersecurity measures in a short timeframe may be impossible, resulting in a loss of potential business.
- Whenever a business needs to use its cyber insurance policy following a loss, they are testing the limits of the policy. Surely no company wants to discover that they inadvertently made an error on their application, failed to update their insurer on a material change, or lack the appropriate coverage feature.

- Failure to enact reasonable cybersecurity measures could result in multiple breaches during the policy period. This could result in businesses paying large out-of-pocket expenses if the aggregate losses exceed policy limits.
- As the cyber insurance market tightens, businesses who are unable to demonstrate reasonable cybersecurity measures may be considered uninsurable by many, or all, cyber insurers.
- If a business continues to suffer successive breaches, their loss ratio may become too high to be considered palatable to most insurers. At best, a business may end up with very large premiums and deductibles on a policy with limited coverage features. At worst, they will be deemed uninsurable.

Therefore, businesses must understand that, while of great importance, cyber insurance should not be the sole response when a business is questioned about the measures a business is using to keep data safe. Cyber insurance should be viewed as a complement to, and not in lieu of, appropriately defined cybersecurity policies, procedures, and controls. Failure to do so could result in a myriad of negative consequences for businesses.

Action Items

- ☐ Understand that cyber insurance will not, and cannot, cover all breach-related expenses;
- ☐ Work with legal counsel to determine your business's unique requirements;
- ☐ Continually assess how your business is making a good-faith effort to protect sensitive data;
- ☐ Work with legal counsel and/or a knowledgeable broker to maximize necessary coverage elements.

Section 2: State-Level Requirements

Businesses must have a firm grasp on the various state-level requirements that apply to them before and after a breach. Failing to grasp these fundamentals can result in a material misrepresentation on their insurance application. In turn, this could lead to a potential declination of coverage, missing crucial time requirements that can lead to unnecessary fines, or other negative consequences. Knowledge of these laws can impact the security practices and internal controls of protected information. In other words, you must know what to protect before you can protect it appropriately.

State Breach Notification Laws

As recently as 2013, the Government Accounting Office (GAO) issued a report that recommended, with concurrence from the Department of Commerce (DOC) and the Federal Trade Commission (FTC), for Congress to develop a consumer privacy framework to increase privacy protections and thereby increase security requirements for all businesses.¹⁵¹ While there have been numerous attempts to create a federal level breach notification standard, all have failed. As recently as February 2018, two House representatives circulated a draft of the Data Acquisition and Technology Accountability and Security Act. This act was intended to set federal-level requirements on breach notification requirements and data privacy.¹⁵²

In response, 32 state attorneys general wrote a joint letter to the House strongly objecting to this proposal. Although the points of contentions were numerous, their main objections are listed below:

- A federal law would eliminate the state's enforcement actions against consumer reporting agencies and financial institutions.
- Such a law would eliminate all state-level data security and breach notification laws.
- The Act would allow entities who suffered a breach to notify consumers, "on their own judgment," which was deemed to result in a lack of transparency.
- The law appeared to be concerned with addressing large, national-level breaches of major corporations at the expense of more frequent but smaller breaches experienced by local or state-wide businesses.¹⁵³

Even if most of the listed issues could be addressed at the federal level to the satisfaction of most states – a difficult proposition at best – there remains the Constitutional issue of preemption. Per the Supremacy Clause in Article VI of the Constitution, federal law will always prevail over state law.¹⁵⁴

Therefore, if a federal law is passed, any state law addressing the same issue would become unenforceable. No matter how the proposed federal-level legislation is worded, there will be states which want more protection, and those that will want less. No matter how the statutory language is parsed, the possibility of federal-level breach law remains unlikely for the foreseeable future.

Businesses must look to the state-level requirements, but this too provides its own issues. It would be common sense to assume that a business would only need to adhere to the breach notification laws which are enacted by the state in which their e

legally resides. As a common point of confusion among business owners, it is worth the time to understand the mechanics of breach notification law adherence.

To illustrate the point, consider a large law firm whose sole office is in Washington, D.C. attempting to navigate its legal requirements following a breach. Conceivably, they would have clients who are residents of Maryland, D.C., and Virginia at a minimum. Which of the following breach notification laws will guide their breach process?

The applicable Maryland Law considers a covered entity, “[A] business* that owns or licenses computerized data that includes personal information of an individual residing in the State[.]”¹⁵⁵

Under the D.C. law, a covered entity is, “Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information.”¹⁵⁶

Per Virginia’s breach law, a covered entity is, “[A]n individual or entity that owns or licenses computerized data that includes personal information.”¹⁵⁷

To further emphasize how complex breach notification can become, consider the timing of notifications. Maryland requires notice, “as soon as reasonably practicable.”¹⁵⁸ D.C. requires, “notification...made in the most expedient time possible and without unreasonable delay.”¹⁵⁹ Virginia more simply requires notification, “without unreasonable delay.”¹⁶⁰

So, which state’s law should be adhered to, and which residents should receive priority in notification?

Primarily, the answer depends on where the client, not the business, resides.¹⁶¹ In instances where state laws are ambiguous or conflicting, such as with dual residency in New York, it will often be up to legal counsel to advise the breached business on what they deem as the best course of action. For nationwide businesses with multiple offices across the various states, the patchwork of state notification laws serves to further complicate the process. Nationwide businesses could conceivably be required to comply with 50 different breach notification laws following an unauthorized intrusion of their computer system.

Thus, the discussions in this book will include various state’s breach notification laws for the following reasons:

- Breach law requirements vary depending on the residency status of the business’s client requiring notification;
- Each state has a nuanced take on their law which is contrasted against other states for illustrative purposes;

- This book is intended to be used by businesses of differing sizes in different geographical locations. Each business will have vastly different levels of expertise, areas of practice, and access to legal knowledge;
- The laws controlling cybersecurity and breach responses change rapidly and frequently. Thus, an overreliance on one state's laws could otherwise render this book obsolete in a matter of months.

Businesses should strongly consider an on-going relationship with legal counsel familiar with privacy and cybersecurity law to keep up to date with any changes that could affect them.

Protected Information

For any business to adequately understand their need for cyber insurance, they must first understand how the various states and territories – not to discount any federal and international regulatory requirements – define what information they must protect from unnecessary disclosure. Unfortunately, these definitions, and indeed the entirety of the statutes which encompass them, are being continuously and independently changed by the requisite judicial bodies. Therefore, it would be prudent for every business to continuously monitor the laws which they are subjected to with competent legal counsel.

For illustrative purposes, these definitions can be broken down into three categories: 1) Personally Identifiable Information, 2) Protected Health Information, and, 3) Ancillary Information. As this book continues, it will use the term “covered data” or, “protected information” interchangeably as a broad term to describes all three categories.

Personally Identifiable Information (PII)

Each state and territory breach notification law contain its own distinct definition of PII.

For example, California contains the following: “(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements...:

1. Social Security number,
2. Driver’s license number or [State] identification card number,
3. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account. “¹⁶²

By comparison, North Carolina identifies Personal Information as meaning a “person’s first name or first initial and last name in combination with any of the following information:

1. Social security or employer taxpayer identification numbers.
2. Driver’s license, state identification card, or passport numbers.
3. Checking account numbers.
4. Savings account numbers.
5. Credit card numbers.
6. Debit card numbers.
7. Personal Identification (PIN) Code:

- a) as defined in G.S. 14-113.8(6), or;
- b) a username or email address, in combination with a password or security question and answer that would permit access to an online account. (§1798.82(h))

Protected Health Information

Certain businesses may also be exposed to Protected Health Information through the course of their services. They should be aware that certain states consider PHI to be data covered under their breach statutes, even if the business is not directly subject to HIPPA/HITECH.

Per Arkansas, their definition of covered medical data is “(D) Medical Information. * Medical information is defined as “any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.” (§4-110-103(5))

Other states and territories which include health information as covered data include Alabama, Arizona, California, Colorado, Delaware, Florida, Illinois, Missouri, Montana, Nevada, New Hampshire, North Dakota, Rhode Island, Virginia, Wyoming, and Puerto Rico.¹⁶³

Ancillary Covered Information

As before, each state and territory have its own unique definitions as they pertain to data covered under their breach notification law.

Returning to North Carolina’s law, they also include the following elements as “personal information”:

1. Digital signatures;
2. Any other numbers or information that can be used to access a person's financial resources;
3. Biometric data;
4. Fingerprints;
5. Passwords.¹⁶⁴

While the probability of any business storing this information is situationally dependent, it does point toward the need of businesses to investigate applicable breach notification laws and monitor any changes therein. As technology is employed at the business, and service areas changes, businesses must pay close attention to how the dynamic landscape of breach notification law definitions will change their risk

profile. This risk profile will directly impact the cyber insurance policy features and limits that a business will require.

Action Items:

- ☐ Work with legal counsel to understand which breach notification laws your business must follow in the event of a breach;
- ☐ Take an inventory of what information your business is collecting;
- ☐ Continuously monitor applicable breach notification laws for any changes;
- ☐ Check that your business is adequately protecting all covered data appropriately;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business's incident response plan as necessary;
- ☐ Determine if the business's cyber insurance policy covers the unauthorized disclosure of protected information as defined by applicable breach notification laws.

Damage Control

Exempted Information

Not every piece of information requires protection, nor does every breach require notification. Most states and territories contain an exemption to data named under their law. While these definitions tend to be vaguer than those requiring protection, they all follow the same general trend. Information that is publicly available is exempt.

For example, Oklahoma is quite brief in its exception. Personal Information “does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.”¹⁶⁵

Ohio is more detailed in their exemption, stating: Personal information “does not include “publicly available information that is lawfully made available to the general public from federal, state, or local government records, or any of the following media that are widely distributed:

- i. “Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;
- ii. Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section;
- iii. Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;
- iv. Any type of media similar in nature to any item, entity, or activity identified in [this section].”¹⁶⁶

Businesses should take note of what information is not considered covered data. Such considerations will have direct impact on their business activities, network architecture, and cybersecurity controls.

Action Items:

- ☐ Understand what information is *not* mandated to be protected applicable laws;
- ☐ Monitor those applicable states’ breach notification laws for any changes;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business’s incident response plan as necessary;
- ☐ Determine if the business’s cyber policy covers voluntary notification.

Damage Control

The Definition of a Breach

Unsurprisingly, most states generally consider a breach to be the unauthorized acquisition of defined, covered data by a third party. However, there are differences which businesses should take notice of as this will have a direct impact on their internal business practices and cyber insurance needs.

Vermont, for example, defines a security breach as, “unauthorized acquisition of **electronic data** or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the data collector.”¹⁶⁷

Consequently, if a completed tax return, with an unredacted social security number for a Vermont resident was stolen from the desk of a staff member, such an action would not necessarily trigger the need for a breach notification.

Businesses should also note which states place requirements on both digital and paper records. They are Alaska, Hawaii, Indiana, Iowa, Massachusetts, North Carolina, Washington State, and Wisconsin, at the time of publication.¹⁶⁸ Whether or not this requirement is implicit or implied depends upon the state's specific statute.

For example, North Carolina defines a covered entity within their statute as, “Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (**whether computerized, paper, or otherwise**) ...”¹⁶⁹

In contrast, the Washington State does not specifically mention paper records, but rather implies such a standard by defining a breach as the “unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”¹⁷⁰

The question then arises, how should businesses deal with paper documents containing personal information? Actions brought by the FTC regarding paper documents provide useful instruction.

In the Matter of CVS Caremark Corporation, C-2459 (2009), the FTC brought action against CVS, a nationwide pharmacy chain. The FTC began its investigation after news reports alleged that CVS pharmacies were throwing away customer information which included social security numbers, credit card numbers, driver's license numbers, and personal health data.¹⁷¹

According to the complaint, CVS failed to:

- Implement reasonable disposal procedures for personal information;

- Adequately train their employees;
- Use measures which would reasonably assess in-store compliance with CVS's own disposal procedures;
- Employ a process to discover and correct risks associated with the personal information of its customers.¹⁷²

CVS Caremark ultimately agreed to a settlement order. That settlement required CVS to establish an information security plan to protect the sensitive information of consumers and employees. Every two years, for the next 20 years, CVS is required to receive an audit showing compliance with applicable security measures. Additionally, CVS is required to maintain "standard record-keeping and reporting provisions to allow the FTC to monitor compliance."¹⁷³

From this case, businesses should understand that data security extends beyond the keyboard and into the physical realm. Regardless of each state's unique breach definition, every piece of information containing sensitive client data should be treated with reasonable care to avoid inadvertent disclosure. Furthermore, data security procedures involving physical records should be routinely assessed and updated as necessary.

Action Items:

- ☐ Understand if the business is required to provide breach notification for paper documents as well as for digital documents per applicable breach notification law definitions;
- ☐ Determine if the business's cyber insurance policy would respond to the loss of paper documents;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Implement continued training on the proper storage and disposal procedures of paper and digital documents;
- ☐ Consider implementing an "absent desk – clean desk" policy;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business's incident response plan and document retention policy, as necessary.

Damage Control

Exceptions

Most states have included a provision in their breach notification laws which excludes the “good faith” acquisition of covered information if that information is being used by an employee of the business for legitimate purposes.

For example, New York includes the following exception: “Good-faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.”¹⁷⁴

These types of breach notification exclusions provide safety for a business if an employee, in good faith, accesses the wrong file while searching for other material. For example, a staff member is searching the file folders for a previous year’s tax return and opens the wrong, “Smith” file. Immediately, they realize that this is the wrong Smith, and they continue with their search – no harm, no foul. No notification or investigation is likely required.

Further exceptions to investigation and notifications occur with many state’s statutes containing a risk of harm analysis. Such analysis may be implied, as in the case of New York’s law, or specifically stated.

New Jersey contains such a stated provision: “Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.”¹⁷⁵ While they are not specific on how a business can reasonably come to this conclusion, it is advisable that businesses consult legal counsel and, at a minimum, document the event for future reference.

Certain states such as Florida have a more strict interpretation by stating a “notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.”¹⁷⁶

Further, there must be written documentation and preservation of the actions taken by the business regarding this analysis. “Such a determination must be documented in writing and maintained for at least 5 years. The covered entity shall provide the written determination to the department within 30 days after the determination.”¹⁷⁷

A common example could be an accounting firm with a tax organizer sent to the wrong address of a Florida resident. While the organizer may include full socials and

other sensitive information, the receiving entity noticed that the name on the envelope was incorrect and has not opened the packet. The receiving entity immediately notified the firm and returned the packet. In this instance, a firm could reasonably argue that even though the third party had received another's social security number, there is no risk of harm because the packet was not opened, and it was returned immediately.

Action Items:

- ☐ Understand if good faith acquisition is exempted in the applicable breach notification laws;
- ☐ Understand if a risk of harm analysis is allowed in applicable breach notification laws;
- ☐ Work with legal counsel to determine how your business should document an internal risk of harm analysis.
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Consider a review and update of the business's computer use policy and user permission segmentations;
- ☐ Update the business's incident response plan as necessary.

Data Encryption Safe Harbors

There is further guidance for businesses within most state breach notification laws that are attempting to make a reasonable attempt at cybersecurity. As of publication, all states have adopted definitions which exempt encrypted data from requiring notification. Often this is found within the definition of a breach.

For example, South Carolina defines a breach as the “unauthorized access to and acquisition of computerized data **that was not rendered unusable through encryption, redaction, or other methods** that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident.”¹⁷⁸

If a business was to lose an encrypted laptop containing the social security numbers of only South Carolina residents, such as loss would likely not classify as a breach and would not require notification.

It should be noted that Tennessee is currently the sole state with a minor exception to the encryption safe harbor. Tennessee defines a breach as the acquisition of either unencrypted data or where encrypted data is acquired along with the encryption key.¹⁷⁹

Outside of being a security best-practice and a possible mitigating factor in both legal responsibilities and risk, encryption safe harbors should give businesses ample incentive to encrypt data both at rest and in transit. Whether or not a business utilizes encryption depends on a host of factors including network architecture, business structure, access to knowledgeable IT professionals, budgetary constraints, and sophistication of oversight within the business. Regardless, encryption is an avenue best explored by businesses of all sizes.

Action Items:

- ☐ Work with legal counsel to determine if applicable breach notification laws allow for encryption safe harbors;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Consider implementing appropriate encryption for all computer assets, with a special emphasis on portable electronic devices;
- ☐ View Special Publication (NIST SP) 800-111, Guide to Storage Encryption Technologies for End User Devices for additional information on encryption;

Service Provider Requirements

Businesses of all sizes now have some element of hosted data, colloquially known as “being in the cloud.” Many small- and mid-sized businesses may be entirely cloud-based. Other businesses may still have servers in-house manned by full time IT staff, or a hybrid system which utilizes both a local server and a managed service provider. Regardless of size, nearly every business is at least utilizing cloud-based software or transmits locally hosted data through a cloud provider.

Often, businesses believe that because a service provider hosts the data, the hosting party will be responsible for all costs should a breach occur. However, this is likely not the case.

Michigan’s breach notification law provides a common example of how limited the obligations of the service provider can be. A “person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.”¹⁸⁰

Note that *nowhere* in the statute’s wording does it mention that the provider is legally responsible for the data. Merely, it requires the provider to give notice to the business. While such a revelation is not financially palatable to most business’s, it does make sense from an insurance risk perspective. Should a breach occur at a major cloud provider, the cost of notification could be catastrophic and centralized to a relatively minor number of insurers. By minimizing the legal culpability of providers as it pertains to breaches, legislators have distributed the risk to exponentially more insurers and businesses.

Whether any one provider is contractually obligated to assist in notification or cover associated costs is beyond the scope of this book. However, it should be noted that having reviewed the contracts of over a dozen cloud providers, every contract contained a strict “hold harmless” clause for a breach in favor of the provider. While large businesses may have the power to negotiate this limit of liability, small- to mid-sized businesses will likely have to take such contracts as they are presented.

Regardless, businesses should not be surprised to have service providers requiring that the client business maintain their own adequate cyber insurance policy. For example, consider the allegations in *Boardman Molded Products v. Involta, LLC*.

Boardman Molded Products (Boardman) describes itself as a, “reliable turnkey solutions, assisting in the

design/engineering of customer industrial, consumer and automotive products, rapid prototyping, mold design/tooling and the actual production of molded products.” Involta is an IT service provider and consulting firm which provided services to Boardman, among many other clients.¹⁸¹

Disaster struck for Boardman in late January 2018 when hackers allegedly breached Boardman’s email accounts. According to Boardman’s lawsuit, “Multiple fake invoices were provided to Boardman's accounting staff by the malicious hackers with instructions to pay fake invoices. Those invoices were paid to fake sources and, as a result, over \$1.7 million in Boardman's funds were stolen.”¹⁸²

It is unknown if Boardman was able to recoup any of these funds through other methods. While Boardman makes numerous claims, their lawsuit against Involta centered around the following counts: breach of service order, professional negligence, and malpractice.¹⁸³

Ultimately, who was at fault – or to what degree – is not relevant to this discussion. What is of primary relevance is that service providers are increasingly becoming weary of large claims being directed their way. Should a service provider face concurrent claims from multiple clients, the provider could face insolvency and one or more claimants could face the possibility of otherwise diminished awards. For those clients not involved in the lawsuits, they could face the possibility of their service provider ceasing operations; forcing them to immediately scramble to find another provider and potentially facing serious roadblocks in doing so. Therefore, the demand by service providers that their clients carry adequate cyber insurance can be beneficial for all parties and is becoming increasingly common.

Action Items:

- ☐ Understand how applicable breach notification laws generally view service provider requirements;
- ☐ Reference the business’s own contracts with service providers to view any indemnification clauses or “hold harmless” provisions. Consider having these contracts reviewed by a privacy attorney;
- ☐ Determine if/how your cyber policy will respond to a breach or service interruption at a service provider;

- ☐ Reference the business's cyber insurance application to determine if the insurer requested information on vendors indemnifying the business for losses following a breach;
- ☐ Speak with your service providers to understand their view of liability;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business's incident response plan as necessary.

Damage Control

Notice Requirements

Inevitably, all businesses will face a breach at some point; possibly requiring notices to clients. The content of these breach notice requirements is controlled by the many states and they vary greatly depending on the residency status of the client in question. There are, however, several shared elements that require understanding by the business's leadership.

Credit Reporting Agency Notification

Many states have varying requirements to notify credit bureau agencies following a breach.

Certain states, such as Nebraska, have no apparent requirement to notify the credit reporting agencies of the breach of a consumer's personal data.¹⁸⁴ So, the onus would presumably be on the consumer to notify the credit reporting agencies at their own discretion.

The states which do require notification of a breach to the credit reporting agency generally have a threshold on the number of consumers breached before reporting is required.

For example, Minnesota appears to have one of the lowest numbered thresholds at 500 consumers. Stating: "If a person discovers circumstances requiring notification under this section and section 13.055, subdivision 6, **of more than 500 persons at one time**, the person shall also notify, **within 48 hours, all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices."¹⁸⁵

Note that the 48-hour reporting time is particularly onerous and would likely require detailed levels of coordination at the breached business. Most likely, this would be accomplished with a well-documented and thoroughly rehearsed incident response plan.

Other states, such as Texas, require higher levels of the number of customer's affected by a breach before notification is required and a much laxer requirement to timing. "If a person is required by this section to notify at one time **more than 10,000 persons** of a breach of system security, the person shall also **notify each consumer reporting agency**, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the

notices. The person shall provide the notice required by this subsection **without unreasonable delay.**”¹⁸⁶

Businesses should note that the timing requirement can vary drastically by state. As a precautionary measure, businesses should be ready to adhere to the strictest notification requirement found among all the various breach notification laws to which they must adhere. Having this information readily available in the business’s incident response plan can aid greatly in this endeavor and avoid additional regulatory inquiries.

Action Items:

- ☐ Understand how applicable breach notification laws mandate threshold and timing requirements to credit reporting agencies;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business’s incident response plan as necessary;
- ☐ Review the business’s insurance policies, including cyber insurance policy, to determine if coverage is afforded for client notification following a breach.

Timing Requirements

The time that a business can notify clients of a breach ranges from the ambiguous to the specific, and sometimes in between.

On the ambiguous side, most states contain a provision like that found in Georgia’s breach notification law: “The notice shall be made **in the most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement...”¹⁸⁷

How, exactly, the state will effectively determine if a business truly notified affected individuals expediently and without unreasonable delay is likely determined on a case by case basis. Regardless, no business would want to test the limits of a state’s patience in this area.

More definitively, 19 states declare specific notification time requirements for those persons affected.¹⁸⁸ On the higher end, Wisconsin mandates that notice must be given “within a reasonable time, **not to exceed 45 days** after the entity learns of the acquisition of personal information.”¹⁸⁹

Florida has a particularly illustrative example of notification timing requirements. They state that “Notice to individuals shall be made **as expeditiously as practicable and without unreasonable delay**, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security,

to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, **but no later than 30 days after the determination of a breach** or reason to believe a breach occurred unless subject to an authorized delay for law enforcement purposes or an authorized waiver.”¹⁹⁰

One of the less-touted benefits of a cyber insurance policy is that most insurers have a pre-selected list of vendors to assist with breach response. This gives affected businesses the ability to select vendors in each required area and to review contracts before a breach. In turn, this allows the business to expeditiously respond to a breach considering various, state-imposed time requirements.

Action Items:

- ☐ Understand how applicable breach notification laws mandate timing requirements to consumers;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Consider reviewing the contracts of the business’s cyber insurance vendor list with legal counsel prior to a breach occurring;
- ☐ If possible, pre-select the appropriate vendors before a breach to ease time requirements;
- ☐ Update the business’s incident response plan as necessary.

How Notice Is Given Including Content Requirements

All states and territories require notification to individuals when their personal information has been breached. As is the trend, the method of notification, as well as the criteria for substitute methods of notification, vary by jurisdiction.

For primary methods of notification, most states generally allow for three types of notification:

1. A written notice;
2. A telephone notice;
3. An electronic notice that complies with the electronic records and signatures provisions of the Electronic Signatures in Global and National Commerce Act.¹⁹¹

This is seen directly in South Carolina's provision: "The notice required by this section may be provided by: **(1) written notice; (2) electronic notice**, if the person's primary method of communication with the individual is by electronic means or ... **(3) telephonic notice[.]**"¹⁹²

Conditionally, businesses may elect to use substitute methods of notice. Certain states may require multiple methods depending on their statute:

1. Email notification;
2. A conspicuous notice posted on the business's website;
3. Notice given to major statewide media.¹⁹³

However, such substitute notice methods are generally subject to several conditions as dictated by the states. These include, but are not limited to:

1. Exceeding a cost threshold for primary notices;
2. Exceeding a person threshold for primary notification;
3. Lack of contact notification to provide primary notification.¹⁹⁴

For example, Rhode Island states that substitute methods of notification may be used if "the state agency or person demonstrates that **the cost of providing notice would exceed twenty-five thousand dollars (\$25,000)**, or that the affected class of subject **persons to be notified exceeds fifty thousand (50,000)**, or the state agency or person **does not have sufficient contact information**."¹⁹⁵

In relation to how such a substitute notice is to be given, Rhode Island states "Substitute notice **shall consist of all of the following**: (A) **E-mail notice** when the state agency or person has an e-mail address for the subject persons; (B) Conspicuous

posting of the **notice on the state agency's or person's website page**, if the state agency or person maintains one; (C) Notification to **major statewide media**.”¹⁹⁶

For practical purposes, most businesses will, in conjunction with legal counsel, elect to use a written notice sent via registered mail. Other primary methods of notice are often difficult to track or evidence. Substitute notification methods are often situationally dependent and unpalatable for business management who are attempting to control negative publicity.

Regardless of which law(s) businesses must adhere to following a breach, they should plan to comply with the strictest requirements across all states. To adequately prepare for such an event, they should understand where clients claim residency and how those states mandate notification requirements. While the business's breach attorney should have ready access to these requirements, adequate planning can assist greatly in avoiding otherwise costly delays.

Action Items:

- ☐ Understand how applicable breach notification laws mandate notification content requirements to consumers;
- ☐ Consider maintaining a master list of each client's state of residency;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business's incident response plan as necessary;
- ☐ Legal counsel may be able to provide stock letters tailored to the relevant states before the breach occurs. Businesses should consider approving these stock letters before a breach to avoid potentially costly delays.

State-level Enforcement Actions and Penalties

Notwithstanding federal-level actions brought by organizations such as the FTC and HHS OCR, many states have an enforcement action if a business is not reasonably attempting to prevent a breach, or otherwise fails to adhere to the state's breach notification law. Often this power is held within the state attorney general's office.

First, businesses should be aware that many breach notification laws require notification to state agencies following a breach. Thus, most businesses may be legally obligated to notify the state of every breach of meaningful size. This can trigger an agency to begin its investigation or provide oversight to client notification.

As is now expected, each state has varying requirements. Those states that do require agency notification tend to include the following general information:

- The state agency that requires notification;
- The timing and method to the agency following discovery of a breach;
- A threshold of affected individuals that requires notification;
- Specific requirements on the information included with the notification to the agency, if any.

In Hawaii, for example, notification must be given to the Office of Consumer Protection without unreasonable delay if 1,000 or more residents are affected. Included in the letter will be the timing, distribution, and content of the notice to individuals.¹⁹⁷

By comparison, Florida is much more exacting in their requirements. Notice must be given to the Department of Legal Affairs of the Office of the Attorney General no less than 30 days after a breach is believed to have occurred, and if it will affect 500 or more residents. Information included in the notice must include:

- Description of the breach events known at the time;
- Number of state residents actually or potentially affected;
- Any services being offered to residents without charge and directions on use;
- Contact information for the person overseeing the breach response;
- An explanation of any other actions taken in conjunction with providing notification.¹⁹⁸

Due to the varied nature of notification requirements, it is imperative that businesses work closely with legal counsel to ensure that they meet required notification standards in the time allotted to them. Failure to do so could result in stiff penalties as many states have a provision inside of their breach notification laws which allow the state to investigate and fine businesses for compliance failures.

Washington State's breach law allows for an innocuous sounding state enforcement. "The attorney general may bring an action in the name of [Washington], or as *parens patriae* on behalf of persons residing in [Washington], to enforce this section."¹⁹⁹

In a recent case of *State of Washington v. Uber Technologies, Inc.*, businesses were put on notice as to the serious nature of state-level enforcement actions.

Uber had known about their breach as early as November of 2016 when they were notified by a hacker who claimed to have access to Uber user information. Following an internal investigation, Uber confirmed that the hacker had indeed accessed the names and driver's license numbers of approximately 10,888 residents of Washington State.²⁰⁰

Rather than notify the appropriate law enforcement agency and affected consumers, Uber paid the intruder's demands and expected that the offender would delete the data and remain quiet. Not until more than a year after the discovery of the breach did Uber notify the state and consumers.²⁰¹

Washington State specifically noted the following actions by Uber which were in violation of the state's laws:

- Uber was aware of the breach and had internally confirmed its existence;
- Uber understood that Washington State residents were affected by the breach;
- Uber failed to provide notification to affected residents in the maximum allotted time of 45 calendar days in accordance with Washington State breach notification law;
- Uber failed to provide notification to the appropriate Washington State Attorney General in the maximum allotted time of 45 calendar days;
- The failure to notify Washington State residents was a deceptive and unfair trade practice and is in violation of the state Consumer Protection Act.²⁰²

Uber's failure to adhere strictly with the law resulted in a \$2.2 million dollar fine and untold bad publicity. This case should serve as a warning to all businesses that they must strictly follow state notification requirements. Moreover, businesses should also be prepared to do so before a breach occurs due to the stringent timelines in various state's notification laws which can incidentally change without warning.²⁰³

Working closely with legal counsel before a breach can greatly assist in this endeavor.

Action Items:

- ☐ Understand how applicable breach notification laws could penalize your business for late notification to appropriate government agencies;
- ☐ Work with legal counsel to understand which government agencies require notification and the timing requirements thereof;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business's incident response plan as necessary;
- ☐ Review the business's insurance policies, including cyber insurance policy, to determine if coverage may be afforded for claims arising from late or inadequate state-level notification.

Client Claims Following a Breach

A minority of states contain provisions for a private right of action by consumers to bring a suit against a business following a breach. Though these private rights of action may appear daunting, they are rarely pursued and even more rarely successful. Foremost, most states which do allow private right of action limit those actions to an error in the execution of the breach notice, and not necessarily to the loss of data.²⁰⁴

The preponderance of states does not explicitly allow a private right of action by consumers. They are either silent on the issue, limit action only to government agencies, or outright forbid the practice.²⁰⁵

Depending on the state, plaintiffs may use some or all of the following claims when litigating a data-breach.²⁰⁶ For businesses that have defended against a professional liability claim, such action may appear familiar:

- Negligence;
- Negligent Misrepresentation;
- Breach of contract;
- Breach of implied warranty;
- Invasion of Privacy/Publication of Private Facts;
- Unjust Enrichment;
- State Consumer Protection Laws.²⁰⁷

A separate avenue for plaintiffs to bring rise to a claim could come from an attempt to extend federal laws to local data breaches. Most often they will use the following federal laws to plead recovery: HIPAA/HITECH, the Stored Communications Act (SCA), The Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA). However, courts have been hesitant to apply these laws as requested by the plaintiffs. Most often actions brought under these statutes fail to proceed beyond the motion to dismiss as courts find they are ill-suited for consumer data-breach litigation, or the statutes themselves lack private right of action.²⁰⁸

A more in-depth discussion on this topic is found on page 513.

Action Items:

- ☐ Understand which business clients, if any, reside in states which allow for a private right of action following a breach;
- ☐ Continuously monitor applicable breach notification laws for any changes;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary;
- ☐ Determine if the business's cyber insurance policy would cover a private right of action following a data breach.

Section 3: Notable State-Specific Privacy Laws

Though every state privacy law is worth reading and reflecting upon, certain state privacy laws are so specific and potentially burdensome in their requirements that they are worth their own notable mention. Failure to understand and abide by these laws, if applicable, can lead to increased risks for businesses as well as potential coverage declinations.

California Consumer Privacy Act (CCPA)

Soon, there is a possibility that businesses with California residents could see private actions increase dramatically with the upcoming implementation of the California Consumer Privacy Act (CCPA). However, there are various stipulations that will give most businesses solace.

Generally, the CCPA applies to companies which meet one or more of the following threshold requirements:

- Annual gross revenue exceeds \$25,000,000;
- Buys, sells, shares, or receives the personal information of 50,000 or more consumers, devices, or households;
- 50% or more of the annual revenue of the business is derived from selling the personal information of a consumer.²⁰⁹

In practice, these thresholds mean that many small- to mid-sized businesses will likely not be subject to the law. However, there could be small companies that are participating in various practice areas, such as payroll processing, ERISA audits, or data brokering, that could potentially subject them to this law.

Under the CCPA, consumers would have the right to bring a private right of action if their information was accessed or stolen by unauthorized parties. Private actions can also be brought if their personal information was disclosed in a nonencrypted or nonredacted format due to the business failing to properly implement reasonable cybersecurity measures.²¹⁰

If an action is brought by a consumer, the CCPA provides for the following potential damages:

- Awards ranging from \$100 to \$750 per consumer, per incident, or actual damages if those are greater;
- Declaratory or injunctive relief;
- Any additional relief deemed proper by the court.²¹¹

Of immediate concern, there will be a clear path for consumers to bring data-breach-related claims against a business following a breach. Additionally, there will now be a defined avenue for consumers to bring claims after a breach if the business failed to implement “reasonable” cybersecurity measures.²¹²

How businesses that demonstrate “reasonable” cybersecurity measures will likely be the subject of many fines and much litigation. As noted previously in another chapter, a 2016 California Attorney General Breach Report includes recommendations that could point to a source for interpretation. As stated within the report, “The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”²¹³

In addition, businesses might consider the adoption, implementation, and continuous review of an appropriate cybersecurity framework such as the NIST CSF described in this book. Security consultants and legal counsel can also assist in this endeavor. Whether other states will adopt similar legislation is, at this point, up for speculation.

Businesses should note that the California Department of Justice will attempt to make this a self-sustaining program. To do so, they will need to raise more than \$57.5 million in civil penalties related to the rule in order to cover the cost of enforcement. To achieve this outcome, businesses can be assessed up to \$2,500 for each violation, or up to \$7,500 for intentionally violating the CCPA.²¹⁴

If a business were to face claims from clients following a breach, they are most likely to face a class-action claim. However, such a claim would likely be limited to large businesses which held large quantities of personal client information. The rationale for this statement can be found on page 513.

Insurability

Given how quickly violations could add up, businesses are increasingly purchasing cyber insurance policies to mitigate substantial fines and penalties.²¹⁵ At question is whether claims brought under CCPA may be insurable. Per the California Insurance Code, “No policy of insurance shall provide, or be construed to provide, any coverage or indemnity for the payment of any fine, penalty, or restitution in any criminal action or proceeding or in any action or proceeding brought pursuant to ... the Business and Professions Code by the Attorney General, any district attorney, any city prosecutor, or any county counsel, notwithstanding whether the exclusion or exception regarding this type of coverage or indemnity is expressly stated in the policy.”²¹⁶

Further the California Insurance Code states, “No policy of insurance shall provide, or be construed to provide, any duty to defend, as defined in subdivision (c), any claim in any criminal action or proceeding or in any action or proceeding brought pursuant to ... the Business and Professions Code in which the recovery of a fine,

penalty, or restitution is sought by the Attorney General, any district attorney, any city prosecutor, or any county counsel, notwithstanding whether the exclusion or exception regarding the duty to defend this type of claim is expressly stated in the policy. ... Any provision in a policy of insurance which is in violation of subdivision (a) or (b) is contrary to public policy and void”²¹⁷

Even though many cyber insurance policies are now offering coverage for CCPA fines and penalties, whether the policy could legally respond is currently speculative.

As of this writing, the CCPA is being amended with various laws put forward in the California Assembly. While the current proposals do not appear to materially change the substance of the law, this is not to say that a future amendment will not.²¹⁸ Therefore, it is imperative that any business which believes it may be subject to the CCPA continues to stay abreast of any changes in the law and consult legal counsel.

Action Items:

- ☐ Determine if your business will be subject to CCPA;
- ☐ Work with legal counsel to review business policies, procedures, and engagement letters for any additional liability considering CCPA;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary;
- ☐ Review the business’s insurance policies, including cyber insurance policy, to determine if coverage may be afforded for CCPA related claims.

Massachusetts' 201 CMR 17

Massachusetts General Law Chapter 93H, containing regulation 201 CMR 17, warrants scrutiny here as it describes in detail various protocols that must be followed by businesses. Known as the Standards for The Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17 applies to, “all persons that own or license personal information about a resident of the Commonwealth.”²¹⁹ Therefore, if a business handles even one return for a Massachusetts’ resident, they likely have responsibilities unseen and unprecedented in most other states.

None of the definitions in the law are particularly worrisome. Indeed, the first half of the law contains language and definitions common to many other state breach notification laws.²²⁰

Unique to this law is the requirement for a business to create and utilize a written information security plan. This plan must include “administrative, technical, and physical safeguards” that are appropriate to the size of the business and the amount of personal information stored.

Every business is required to enact at the least the following measures in their information security program per section 17.03:

- Designated employee(s) to maintain the program;
- Identifying and evaluating external and internal risks;
- Implementation of training for permanent, temporary, and contract employees;
- A method to detect and prevent failures of the security system.
- Creation of security policies for employees who transport covered records off-site;
- Enact disciplinary actions against employees who violate the business’s information security program;
- Preventing terminated employees from accessing covered data;
- Reasonably limiting the business’s third-party service providers to those providers who maintain data security standards at least as strict as 201 CMR 17.00, as well as other applicable federal level regulations, and requiring them by contract to do so;
- Enact reasonable restrictions on the physical access of covered data;

- Consistent monitoring of the program and updating of safeguards as necessary;
- Mandatory minimum of an annual review of the program, or as business practices change;
- Documentation of actions taken in relation to breach of the business's security, and well as a mandatory post-occurrence review to makes changes in business practices.²²¹

In addition, businesses will be required to include and maintain the following computer security requirements not seen in other states, as mandated in section 17.04:

- Protected user authentication protocols such as restricting and blocking access and control of password location/format;
- Restricting access, including segmented user permissions and assignment of unique user IDs;
- Encryption of all information transmitted either across public networks or wirelessly;
- System monitoring for unauthorized access or use of covered data;
- Encryption for all portable devices which contain covered data;
- Mandatory employee training on computer and personal security;
- Ensuring system security with updated firewall protection, security patches, virus definitions, and supported software.²²²

As shown in the ongoing case of *Commonwealth of Massachusetts v. Equifax, Inc.*, the Massachusetts Attorney General asserts that enforcement of the law does not require a breach or demonstrated harm done to consumers.²²³

In late 2017, the Massachusetts attorney general brought action against Equifax following their highly publicized breach of allegedly 143 million consumers. Within the attorney general's claim, she lists several violations of Massachusetts General Law, but specific to this discussion, multiple violations of the 201 CMR 17. Equifax allegedly violated:

- The responsibility to develop, maintain, and implement a written security plan suitable for the information being protected to meet the basic requirements expected of a business their size;
- The requirement to maintain security updates of their computer systems;

- The requirement to monitor systems for unauthorized access or use as required.²²⁴

Additionally, the attorney general is alleging that, by virtue of violating 201 CMR 17, Equifax also committed various unfair or deceptive trade practices in violation of Massachusetts G.L. c. 93A , § 2, committed deceptive acts or practices in violation of Massachusetts G.L. c. 93A , § 2, committed unfair acts or practices in violation of Massachusetts G.L. c. 93A , § 2, failed to safeguard personal information in violation of Massachusetts G.L. c. 93H , § 2, and failed to notify the appropriate parties as required by law following the breach in violation of Massachusetts G.L. c. 93H , § 3(b).²²⁵

As of publication, the two parties are currently in court. Regardless, no business would want to test the limits of a state's attorney general in court for similar accusations.

Action Items:

- ☐ Determine if 201 CMR 17 applies to your business;
- ☐ Work with legal counsel or other compliance experts to review business policies and procedures to ensure compliance, if applicable;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan, business practices, and other internal documents as necessary;
- ☐ Determine whether the business's cyber policy would cover 201 CMR 17 related claims and expenses.

New York's 23 NYCRR 500

23 NYCRR 500 was unveiled in March of 2017 by the New York Department of Financial Services (DFS). This law places specific requirements on companies to safeguard their consumers' data privacy. The impetus for this new law arose from the concerns of DFS that the financial services industry could face significant disruptions by cybercriminals.²²⁶

It is not immediately clear which entities must comply with this law as there is no definitive list provided by DFS within 23 NYCRR 500. The law only defines a "Covered Entity" as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."²²⁷

NYDFS's website lists the following entity types by name, so presumably they may be required to comply: Agents & Brokers, Banks & Trusts, Check Cashers, Health Insurers, Insurance Companies, Licensed Lenders, Money Transmitters, Premium Finance Agencies, Sales Finance Companies, Student Loan Servicers, Bail Bond Agents, Budgets Planners, Credit Reporting Agencies, Insurance Adjusters, Insurance Education Providers, Life Insurers, Mortgage Companies, Property Insurers, Service Contract Providers, and Virtual Currency Businesses. DFS has attempted to alleviate some of the confusion regarding who must comply. Notably, they clarified in a recent FAQ that non-profit mortgage brokers, health maintenance organizations (HMOs), and continuing care retirement communities (CCRCs) must also comply with the law.²²⁸

Currently, there still exists a large amount of ambiguity regarding who must comply, so it is advised that businesses consult legal counsel to determine compliance questions.

Covered entities must also be aware that the information to be protected may be far broader than that detailed by other state and territory breach notification laws. "Nonpublic Information" means any electronic information that is not publicly available. More specifically, it is defined as:

- "(1) Business-related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a materially adverse impact to the business, operations or security of the Covered Entity;
- (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

- (i) social security number;
 - (ii) drivers' license number or non-driver identification card number;
 - (iii) account number, credit or debit card number;
 - (iv) any security code, access code or password that would permit access to an individual's financial account or;
 - (v) biometric records.
- (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to:
- (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family;
 - (ii) the provision of health care to any individual or;
 - (iii) payment for the provision of health care to any individual.”²²⁹

Broadly speaking, 23 NYCRR 500 requires entities regulated by DFS to assess their cybersecurity to create a risk profile. These activities are quite analogous to those found in other cybersecurity frameworks, such as NIST CSF.

Once a risk profile is completed, the entity must implement a comprehensive data security plan to mitigate the risks that the entity has identified to any nonpublic information in its possession. While apparently simple, there are various mandatory requirements that businesses must follow; unless specifically exempted. Covered entities may be exempt from portions of the law, but no covered entity is entirely exempt from all portions of the law.

500.2: This section describes the cybersecurity program that covered entities shall maintain. Within the cybersecurity program, the entity must meet six core functions. These include identifying and assessing risks to nonpublic information; the use of policies, procedures, and controls to protect the entity's IT system and stored nonpublic information; detection of cybersecurity events; responding to events to mitigate harm; recovering from events to resume normal operations; and reporting of the events in conjunction with the law.²³⁰

The following are notable sections of the law with brief descriptions:

500.3: This section concerns the entity's mandatory written cybersecurity policy. Of note, the cybersecurity program must be approved by the governing body of the entity and based upon the previously completed risk assessment. The policy mandates fourteen specific areas to be addressed by the entity, if applicable. Notable among these areas are business continuity, disaster recovery, physical security, vendor management, and incident response.²³¹ In particular, such areas are often not mandated by other laws, so special effort may be required to fully comply.

500.4: Businesses must, in accordance with this section, designate a qualified chief information security officer (CISO) to oversee and implement its cybersecurity program. What qualifies a person to be considered a, “qualified” CISO is not specified. To alleviate personnel shortages, businesses may elect to use a third-party service provider to act as a CISO. Regardless of origin, the CISO must report on the cybersecurity program and risk at least annually to the governing body of the organization.²³²

500.5: This section mandates that covered entities must undergo continuous monitoring, or periodic vulnerability assessment and penetration testing.²³³

500.6: The “Audit Trail” section mandates that covered entities must meet two criteria. First, they shall maintain a system that can reconstruct material financial transactions to allow for normal operations for no less than five years. Second, they shall maintain a system that includes audit trails for no less than three years. This audit trail must be able to detect and respond to any cyber-event that could harm to the normal operations of the entity.²³⁴

500.7: Each covered entity must limit the access privileges of users to systems that contain nonpublic information. The access privileges to such systems must be reviewed periodically.²³⁵

500.8: Covered entities must assess the security of their applications. This shall include guidelines, standards, and written procedures to any organically developed applications. Further, entities must create similar protocols for externally developed applications. These actions must be periodically reviewed and updated by the CISO.²³⁶

500.9: This section mandates that covered entities shall conduct periodic and documented risk assessments and that those assessments must be updated as necessary to respond to emerging risks and changes to the entity. In particular, this section requires the risk assessment to contain policies and procedures that include: “(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity; (2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks, and; (3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.”²³⁷

500.10: Particularly noteworthy is the requirement for a covered entity to maintain qualified cybersecurity personnel. Such personnel must be provided with updates and training necessary to combat current cybersecurity risks. In addition, the entity must verify that these personnel maintain and update their knowledge base.²³⁸

500.11: This section requires covered entities implement written policies and procedures to maintain the security of their IT system and nonpublic information held by any third-party service provider. In addition, the document must also include the due diligence performed by the entity as well as contractual protections as they relate to the third-party providers.²³⁹

500.12: Each covered entity is required to use effective controls to prevent unauthorized access to nonpublic information. This may include Multi-Factor Authentication (MFA) or other forms of Risk-Based Authentication (RBA). For any individual accessing the entity's internal network from an external network, MFA should be used unless the CISO has authorized an equivalent or superior control in writing.²⁴⁰

500.13: This section concerns limitations on the retention of nonpublic information data. Exemptions are granted where law or regulations, such as those required by the state board of accountancy, require information to be held for longer. If no such exemption exists and nonpublic information is no longer required for legitimate business purposes, that information should periodically be disposed of in a secure fashion.²⁴¹

500.14: A covered entity must monitor the activities of authorized users as well as detect any anomalous access of non-necessary information by authorized users. In addition, all personnel must provide periodic cybersecurity-awareness training that is updated to reflect current risks identified by the entity's risk assessment.²⁴²

500.15: The entity shall implement controls to include encryption for all nonpublic information. Nonpublic information sent over external networks shall be encrypted unless a necessary alternative is approved by the CISO. Nonpublic information at rest shall be encrypted unless a necessary alternative is approved by the CISO.²⁴³

500.16: This section covers the creation of the entity's written incident response plan. Included will be seven key areas, including subjects ranging from pre-breach planning to response and revision of the response plan.²⁴⁴

500.17: When a cybersecurity event has occurred, the entity is required to notify the DFS superintendent within 72 hours. This will occur whenever notice must also be given to another regulatory agency or government body, as well as an event that could materially harm the entity's normal operations.²⁴⁵ The quick notification mandate, in conjunction with the somewhat vague triggering actions, means that entities will likely need to have had dry runs through various notification scenarios to maximize the odds of compliance.

500.18: Generally speaking, information provided by the entity in accordance with 23 NYCRR 500 is still subject to the exemptions and limitations found in other

state and federal laws.²⁴⁶ Therefore, businesses must also understand if other laws require stricter controls than those found in this law.

500.19: This section of the law deals with the exemptions that entities may qualify for. Recall that a covered entity may qualify for some exemptions but will not be exempt from all portions of the law. Due to the ambiguity of the law, as well as the ambiguity of who must adhere to the law, businesses are advised to seek legal counsel to assist in determining if they qualify for exemptions.²⁴⁷

500.20: As detailed in this section, 23 NYCRR 500 will be enforced by the superintendent of the DFS.²⁴⁸ As of publication, the authors were unable to find any business that has been subject to fines and penalties under this law. It has been opined that enforcement actions will be brought by the DFS under the New York Banking Law. This would authorize penalties of up to \$2,500 per day during the violation, \$15,000 per day due to reckless conduct, or \$75,000 due to willful violations.²⁴⁹

Businesses should understand that adherence to 23 NYCRR 500 is not a “one and done” compliance issue. Adherence is a continual process that demands resources and personnel overseen by the highest authorities within the covered entity. In turn, those authorities will need to attest to various security practices and procedures to the NYDFS, often on an annual basis.

Action Items:

- ☐ Determine if 23 NYCRR 500 applies to your business;
- ☐ Work with legal counsel to review business policies and procedures to ensure compliance, if applicable;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary;
- ☐ 23 NYCRR 500 can be found at:
<https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf>;
- ☐ 23 NYCRR 500 FAQs page containing additional guidance can be found at:
https://www.dfs.ny.gov/industry_guidance/cyber_faqs;
- ☐ Determine whether the business’s cyber policy would cover 23 NYCRR 500 related claims and expenses.

Damage Control

New York SHIELD Act

As of 1 March 2020, the Stop Hacks and Improve Electronic Data Security Handling (“SHIELD”) Act will drastically change New York’s data breach notification laws. Due to its sweeping applicability and mandates, it is advisable that any business that reasonably believes it could fall under this law should immediately seek competent legal counsel to assist them with compliance.

Applicability

Under the soon-to-be-defunct New York breach notification law, a covered entity was deemed to be, “Any person or business which conducts business in the New York state, and which owns or licenses computerized data which includes private information.”²⁵⁰ However, the SHIELD Act will change covered entities to include *any* business that now “owns or licenses computerized data”²⁵¹ of New York residents, even if that business does not necessarily reside in New York. Consequently, a business maintaining the private information of even one New York resident, even though physically located in another state, would need to become compliant with the law.

Private Information

As dictated within the SHIELD Act, the scope of “Private information” will be expanded. Notably, this act maintains the prior breach law’s definition, but will now include “account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual’s financial account without additional identifying information, security code, access code, or password.”²⁵² This removes the previous requirement that includes the number being in combination with a, “security code, access code, or password,”²⁵³ making the possibility of breach notification much greater due to the ambiguity.

In addition, the new law also includes “biometric information, meaning data generated by electronic measurements of an individual’s unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual’s identity[.]”²⁵⁴ How the limits of this clause apply will likely be tested through litigation.

“Reasonable” Data Security Requirements

Perhaps garnering the most attention are the new requirements for businesses to enact “reasonable” data security measures. Per the statute, applicable businesses “**shall** develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information....”²⁵⁵

Administrative Safeguards

“Reasonable” administrative safeguards, per the text of the law, are when a person or business:

- “(1) designates one or more employees to coordinate the security program;
- (2) identifies reasonably foreseeable internal and external risks;
- (3) assesses the sufficiency of safeguards in place to control the identified risks;
- (4) trains and manages employees in the security program practices and procedures;
- (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
- (6) adjusts the security program in light of business changes or new circumstances;”²⁵⁶

Technical Safeguards

“Reasonable” technical safeguards, per the text of the law, are when a person or business:

- “(1) assesses risks in network and software design;
- (2) assesses risks in information processing, transmission and storage;
- (3) detects, prevents and responds to attacks or system failures; and
- (4) regularly tests and monitors the effectiveness of key controls, systems and procedures;”²⁵⁷

Physical Safeguards

“Reasonable” physical safeguards, per the text of the law, are when a person or business:

- “(1) assesses risks of information storage and disposal;

- (2) detects, prevents and responds to intrusions;
- (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.”²⁵⁸

The law, however, does provide for both a major and minor exception. For entities that are subject to, and in compliance with, among other provisions, the Gramm-Leach-Bliley Act (GLBA), HIPAA/HITECH, they are preemptively considered a “compliant regulated entity.”²⁵⁹ Small businesses – those with fewer than 50 employees, less than \$3 million in gross annual revenue, or less than \$5 million dollars in total year-end assets, can be considered compliant if they have reasonable safeguards given their size and type of business and the type of personal information they collect.²⁶⁰

For those entities that believe they qualify as a small business, they should not necessarily assume that their safeguards are appropriate to qualify as “reasonable.” Small businesses would be well advised to seek legal counsel to guide them through assessing how reasonable their safeguards might be construed by a regulator.

Breach Notice Issues

For those businesses that must comply with the SHIELD act, client notification must be provided, “immediately following discovery,”²⁶¹ and “without delay.” While not yet tested, this appears to provide a stricter standard than many other states which require notification within a reasonable time frame. For a business without pre-selected breach response vendors, or those without cyber insurance, this could prove to be an exceedingly difficult task.

If even a single New York resident is to be notified, the breached business will also be required to notify, “the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons.”²⁶² This mandatory inclusion of additional parties could be implied to mean that New York is looking to aggressively fine affected businesses.

Finally, businesses should be aware that the statute’s definition of “breach of the security of the system” is very broad. This would include “access to or acquisition of, or access to or acquisition without valid authorization, of computerized data...”²⁶³

In other words, a ransomware event, can, in theory, require breach notification to all those whose information may have “accessed” though not necessarily “acquired.”

Fines and Penalties

While there is no private right of action,²⁶⁴ the Attorney General of the state of New York can bring various actions against any person or business that violates the SHIELD Act.²⁶⁵ Previously, the fine was limited to \$150,000 per violation, but that has been increased to \$250,000.²⁶⁶ Unlike some other states, New York appears quite aggressive in regard to levying fines.²⁶⁷ PWC has estimated that in 2019 alone, New York issued more than \$600 million in fines related to data breaches.²⁶⁸

Action Items:

- ☐ Determine if the New York SHIELD Act applies to your business;
- ☐ Work with legal counsel to review business policies and procedures to ensure compliance, if applicable;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary;
- ☐ Determine if your business’s insurance policy would cover fines and penalties that arise from the NY SHIELD Act.

Illinois' Biometric Information Privacy Act (BIPA)

Increasingly, employers are using employee's biometric information. According to one study, over half of workplaces use biometric information in the workplace for purposes ranging from authentication to security. Most commonly, this is accomplished with fingerprint scanning or facial recognition on smartphones, laptops, or tablets.²⁶⁹ So far, at least three states – Illinois,²⁷⁰ Texas,²⁷¹ and Washington²⁷² – have passed laws detailing an employer's obligations regarding held biometric information. Of those three states mentioned, only Illinois allows a private right of action that has spawned multiple class-action lawsuits of note.²⁷³ Therefore, the Illinois law will be the only one discussed in greater detail below.

Background

As noted by the Illinois Legislative findings intent section, biometric information should require particularly strong safeguards. Unlike other forms of unique identifiers such as social security or drivers' license numbers, biometric information is generally unable to be changed. Furthermore, once an individual has had their biometric information compromised, the affected person has little recourse and is likely to forever be at higher risk for identity theft.²⁷⁴ In other words, biometric information is “permanent PII” that should be handled with great care.

Application

It is not immediately evident from the text of BIPA to whom this law applies. While the law does define a “private entity,” the definition is rather vague. Specifically, the law states that a private entity is “any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.”²⁷⁵ Presumably, the law provides protections to both in-state and out of state Illinois residents.²⁷⁶

Definition and Exemptions

Within the Illinois Biometric Information Privacy Act (BIPA), there are three classifications of information that businesses should be familiar with; biometric identifiers, biometric information, and confidential and sensitive information. Each will be discussed in turn to include exemptions.

- Biometric identifiers specifically mean “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.”²⁷⁷ Information specifically excluded from this definition would include, but is not limited to, demographic data, tattoo descriptions, eye color, height, weight, donated organs, information regulated under the Genetic Information Privacy Act (GINA), and information regulated under HIPAA.²⁷⁸
- Biometric information is defined as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.”²⁷⁹ Per BIPA, this does include information covered or excluded the definition of biometric identifiers.²⁸⁰
- Confidential and sensitive information means “personal information that can be used to uniquely identify an individual or an individual's account or property.”²⁸¹ This could include, but is not limited to, genetic markers, passcodes, drivers' license numbers, or a social security number.²⁸²

Illinois Breach Notification Law Considerations

Under the Illinois relevant breach notification law, there is a separate definition for “biometric data.” Specifically, this definition includes “data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.”²⁸³ Therefore, a breach of biometric identifiers may also trigger breach notification to affected parties and relevant government authorities.

The Illinois breach notification law also states that “data collectors” can be the business proper, or their contractors. Third-party data collectors, such as managed services providers, vendors, or cloud service providers, must notify the owner of the information of a breach of security.²⁸⁴ For example, a business uses a third party to house fingerprint scanning information of their employees to validate monetary transactions. If that third party is breached, it will be the responsibility of the business to provide, and pay for, the necessary notifications and identity theft products.

Furthermore, the law at hand also states that a data collector that “owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.”²⁸⁵ Consequently, both the business proper and their third-party providers must implement “reasonable” security measures.

In addition, “A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.”²⁸⁶ Thus, any business which is utilizing a third party to maintain biometric information must **contractually** obligate that third party to utilize reasonable security measures, which are further detailed below.

Five Important BIPA Features

Returning to BIPA, there are five relevant categories within the law that businesses should understand in detail. These include prior informed consent, limited right of disclosure, mandatory safeguard and retention guidelines, prohibitions on profiting, and private rights of action.

Prior Informed Consent: Before a company is allowed to collect biometric information, it must generally provide notice and obtain written consent from the individual.²⁸⁷ Notably, BIPA requires the defined “written release,” which means “informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.”²⁸⁸

Under BIPA, any company which would, “collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information,”²⁸⁹ must inform the person, or their legally authorized representative (hereinafter “them,” or, “they”) that:²⁹⁰

1. “[A] biometric identifier or biometric information is being collected or stored;”
2. “informs [them] in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and”
3. “receives a written release executed by [them]” Recalling that a written release is defined as, “informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.”²⁹¹

Limited Right of Disclosure: Before any business can “disclose, redisclose, or otherwise disseminate”²⁹² biometric identifiers or information, the following guidelines must be met:

1. They have consented to the disclosure;

2. It is necessary for them to complete a financial transaction and is authorized by them;
3. It is required by, “State or federal law or municipal ordinance,” or;
4. It is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Prohibition on Profiting: As stated quite succinctly in the law, “No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.”²⁹³

Mandatory Safeguards: Interestingly, BIPA is sparse on details regarding which safeguards must be implemented. The law states that any entity holding biometric information of identifiers must both “store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry,”²⁹⁴ and, “in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.”²⁹⁵ Here, businesses would be well served by referencing prevailing case law and consulting with legal counsel to determine their unique requirements.

Retention Guidelines: Unlike the safeguards section, here the law is much more specific. The law states that an entity holding biometric information or identifiers, **must:**²⁹⁶

1. develop a written policy,
2. make that policy available to the public;
3. “Establishing a retention schedule and guidelines for permanently destroying... information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.”

Private Rights of Action

Recently, the right of an aggrieved party under BIPA to bring a private right of action has brought the most attention. As enumerated under the law, a person may bring an action in either a state circuit court or a supplemental claim in federal district court. For each violation, a party can recover the following: ²⁹⁷

- For a negligent violation, whichever is greater of liquidated damages of \$1,000 or actual damages;

- For an intentionally reckless violation, whichever is greater of liquidated damages of \$5,000 or actual damages;
- Reimbursement of reasonable attorneys' fees, expert witness fees, and litigation expenses;
- Any other relief as deemed appropriate by a state or federal court, including an injunction.

In practice, the above ambiguity over keywords and phrases has led to a flood of class action cases being filed under BIPA. Some of the more interesting cases attempting to create precedence to the words found in BIPA are detailed below.

Rosenbach v. Six Flags Entm't Corp.: **When is a person “aggrieved”?**

Stacy Rosenbach took her son to a Six Flags theme park. In connection with the purchase of a season pass for that park, they were allegedly fingerprinted. Both the mother and son brought an action against the park for alleged violations of BIPA.²⁹⁸

Among the many questions posed in this lawsuit, one brought the most attention. Readers will have noticed that “aggrieved” parties can bring a private right of action under BIPA.²⁹⁹ However, the law never actually defines what qualifies a person to be aggrieved?

Ultimately, the Supreme Court of Illinois held that “a person need not have sustained actual damage beyond the violation of his or her rights under the Act in order to bring an action[.]”³⁰⁰

For employers, this should be seen as a chilling turn of events. Even if the safeguards are 100% effective in preventing identity theft, or some other harm, this does not necessarily mean that an entity could not bring a BIPA claim. A purely technical violation may be enough to facilitate the rise of a private cause of action. Therefore, employers are urged to immediately seek legal counsel and determine their compliance standards and potential liability.

Michelle Espinosa v. RevMD Partners, LLC: **What is a “violation”?**

In this class action case, Espinosa was employed by RevMD as a patient account specialist for approximately five months. During that time, Espinosa alleged that RevMD required her and other employees to scan their fingerprints to clock in and out of their shift as a method timekeeping.

Of key interest in this case is how the Espinosa, and her similarly situated class of co-plaintiffs, attempt to define a “violation” under BIPA. As stated in the case, “Defendant required Plaintiff and other employees to scan their fingerprints in Defendant’s biometric time clock each time they started and finished working a shift, and when they clocked in and out for lunch breaks.”³⁰²

Recall from the above that BIPA does not define if a “violation” is every individual alleged instance of non-compliance or the collection of instances of alleged noncompliance.³⁰³

While this may seem pedantic, the ramifications could be enormous. If the court were to agree to the assertions made by the plaintiffs in this case, as stated above, that would account for four violations, per day, per employee. Under BIPA, this could yield damages in favor of each plaintiff for between \$4,000 to \$20,000 *per day of employment*. Using this calculation, it is not hard to see how employers could quickly face a crippling amount of liability for even brief violations.

In re Facebook Biometric Info Privacy Litigation: What is a photograph?

In this class action case, the plaintiffs filed a claim under BIPA for alleged violations under Facebook’s “Tag Suggestions” program. This program allowed users of Facebook to name other Facebook users or non-users who appear in a photograph that had uploaded to the platform. The program allegedly used facial recognition technology to scan uploaded photos and suggest a name if it was able to recognize the face in the photo. It was further alleged that Facebook created “templates” of people’s faces based upon their unique facial geometry. For example, this could include the distance between an individual’s ears, nose, and eyes.³⁰⁴

Recall that “photographs” were included under the description of “biometric identifiers.”³⁰⁵

The plaintiffs alleged that Facebook violated BIPA by failing to adhere to subsection 15 of the act that requires prior informed consent.³⁰⁶

Here, the judge was forced to determine if a photograph was meant to be defined as a physical object, or if it could also be construed as a digital object. Ultimately the court held that “‘Photographs’ is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet.”³⁰⁷

***Liu v. Four Seasons Hotel Ltd.*: Can employees subject to arbitration of employment-related claims bring an action under BIPA?**

In this case, employees of the Four Seasons brought a class action against their employer under BIPA. As employees of the Four Seasons business, the employees were allegedly required to scan their fingerprints for timekeeping purposes. This information was then stored in a database.³⁰⁸ At question was whether employee claims under BIPA were subject to employment arbitration agreements as “wage or hour violations.”³⁰⁹

Four Seasons’ main argument was that the plaintiff’s claim should have fallen under “wage or hour violations” because the fingerprint data was used to track the work hours of employees.³¹⁰

Ultimately the court held that the agreement to arbitrate the employment-related claims in the employment contract, including wage and hour claims, did not cover alleged BIPA violations.³¹¹

With this holding in mind, businesses are encouraged to work with legal counsel to review how a BIPA claim brought by their own employees may or may not be considered under employment contracts.

Insuring against BIPA claims

Given the evolving nature of even basic terms found within BIPA, as well as the multitude of cases being filed under this act, businesses would be rightly concerned about insuring for such a loss. Whether a BIPA claim can be covered by an insurance policy will ultimately depend upon the specific policy’s language and the fact pattern of the case at hand. While the specific language of various policy types will be discussed in greater detail later in this book, there are some general considerations by policy type to consider below.

Commercial General Liability Policies: Broadly, newer form commercial general liability policies will contain a host of endorsements that would exclude coverage for the access or disclosure of confidential or personally identifiable information.³¹²

Employment Practices Liability Policies: In general, businesses would need to reference the definitions of “employment practices,” “wrongful acts,” and “privacy claims” to begin their research. Businesses would also need to delineate the difference in coverage between first- and third-party claimants. Given that BIPA claims only recently became a serious issue for businesses around the country, it is entirely feasible that an employment practices insurance policy may be silent on the issue.

Cyber liability policy: Businesses should begin their assessment by looking at the definition of “personally identifiable information.” If the policy is a named peril type policy, there may be no mention of biometric information, or it may be referred to by another name. In addition, a business should consider if a private right of action is covered under their cyber policy.

Vendor Contracts

As noted previously in this chapter, a business may be responsible for the security of biometric information or identifiers held by third parties.³¹³ As such, a business should consider working with legal counsel to draft appropriate vendor contracts. Topics could include, but are not limited to:

- Vendor acceptance to store biometric data in compliance with all statutory requirements;
- Vendor agreement to indemnify the company for any compliance failures;
- Consideration for having the business named as an additional named insured under vendor policies that could cover a BIPA claim, and where allowable.

Action Items

- ☐ Seek legal counsel to determine evolving responsibilities under BIPA.
- ☐ Businesses are encouraged to seek legal counsel and become proactive in assessing compliance risk.
- ☐ Speak with legal counsel to determine how a BIPA claim might be treated under.
- ☐ Work with legal counsel and/or an appropriate insurance broker to determine how insurance policies held by the business may or may not cover BIPA related claims.
- ☐ Assess your applicable vendor contracts to determine BIPA compliance.

Section 4: Cybersecurity and Privacy Requirements

Businesses are often surprised that they may be subject to various federal level cybersecurity/privacy laws. Certain statutes may be overarching, while others are specific to the practice area of the business. Regardless, businesses should be well familiar with their obligations. Failure to do so can lead to otherwise unnecessary breaches, potential declinations of coverage, and unwanted actions from regulators.

FTC Cybersecurity Oversight

It may seem odd to most businesses that the Federal Trade Commission would have the ability to bring cases against companies following cybersecurity breaches. After all, Congress has never passed a law explicitly allowing the FTC to bring such cases. Rather, the FTC has used the interpretation of controlling statutes passed by Congress to become the de facto, cyber-breach regulatory body.

The FTC points to Section 5 of the Federal Commission Act, a law enacted over 100 years ago to claim authority in data-breach cases. Section 5 states that “unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”³¹⁴

In 1980, the FTC attempted to assist businesses with understanding their interpretation of “unfair.” The FTC had noted that “the concept of consumer unfairness is one whose precise meaning is not immediately obvious, and also recognize that this uncertainty has been honestly troublesome for some businesses and some members of the legal profession.”³¹⁵

Generally, the FTC would be looking for cases of substantial and unjustified consumer injury which “involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services¹³ or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction.”³¹⁶

Going further, the FTC noted, “the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces.” Finally, “the injury must be one which consumers could not reasonably have avoided.”³¹⁷

In 1983, the FTC released a policy statement on deception to aid the public. In short, they noted that “the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.”³¹⁸

How precisely companies were and are supposed to structure their cybersecurity to avoid the FTC from bringing a claim based on “unfair and deceptive trade practices” has never been detailed. Historically, when the FTC brought an action against companies under its presumed cybersecurity enforcement authority, those companies rarely, if ever, challenged such action. Generally, companies who are threatened with a lawsuit accepted their maximum, 20-year consent orders to avoid public scrutiny.³¹⁹ As noted by the GAO, of the over 100 instances of privacy enforcement actions filed by the FTC in the last ten years, virtually all companies

have acquiesced to changes in their business and security practices by agreeing to consent orders.³²⁰

Perhaps the first company to question whether the FTC had the authority to regulate and enforce cybersecurity was Wyndham Worldwide Corporation, a hotel chain, in the case of *F.T.C. v. Wyndham Worldwide Corp.*

In 2008 and 2009, Wyndham had been the victim of at least three breaches where hackers were able to access Wyndham's computer network. Through this access, the hackers were able to view customer's personal information, including payment card numbers, expiration dates, and security access codes. As a result, more than 619,000 consumers were affected and suffered more than \$10.6 million in fraud losses.³²¹

In 2014, the FTC alleged that following the discovery of the first two breaches, Wyndham was negligent in their handling to prevent additional compromises in their network through "reasonable and appropriate security measures." The numerous failures of Wyndham, per the FTC, included:

- Clear text storage of consumer's payment card data;
- Failure to employ firewalls;
- Lack of oversight in implementing security procedures and policies as necessary before hotels could connect their computers to the host network;
- Servers utilized operating systems that were no longer supported and thus could not receive updates or patches necessary to avoid publicly known security vulnerabilities;
- Servers could be accessed using default passwords and user IDs;
- Lack of management for devices which could access the network;
- No apparent monitoring of networks for malware which had previously been used to infiltrate the company network;
- Failing to limit access by third parties as necessary;
- Lack of stringent requirements for usernames and passwords.³²²

Rather than agree to a consent order by the FTC, Wyndham responded to the FTC by filing a lawsuit in federal court where they could fight the case.

Wyndham attempted to have the lawsuit dismissed on multiple grounds. Specific to this discussion, Wyndham asserted that the FTC's authority did not extend to data security. Congress had passed statutes to deal with cybersecurity in specific industries, but no such statute had granted the FTC authority to create data and

cybersecurity standards. Further, they asserted that “it defies common sense to think that Congress would have delegated [this] responsibility to the FTC[.]”³²³

In response, the FTC asserted that it was acting with due authority under Section 5 of the FTC Act of 1914, and the district court disagreed with the assertions of Wyndham.³²⁴ In particular, the court noted that “the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme.”³²⁵

Ultimately, the case was brought before the Third Circuit Court of Appeals. Here too, Wyndham was unsuccessful. The Court of Appeals affirmed FTC's ability to bring actions against companies alleged to have engaged in unreasonable computer and data security practices.³²⁶

Gramm Leach Bliley Act and the Safeguards Rule

Although every business must adhere to applicable state and territory breach notification laws, there are additional requirements at the federal level for being considered a financial institution. Most notable is the Gramm-Leach-Bliley Act (GLBA), also known as the “Financial Modernization Act of 1999.” Under the GLBA, the FTC would be the most likely body to bring an action against a financial services business.³²⁷ Indeed, a recent report by the GAO noted that most interviewed stakeholders favored the FTC’s continued enforcement practices and that their power to do so should be expanded.³²⁸

Whereas the states generally referred to Personally Identifiable Information as needing protection under their relevant breach laws, GLBA uses the term “nonpublic personal information.” The GLBA describes ‘nonpublic personal information’ as the following:

“(A) The term “nonpublic personal information” means personally identifiable financial information:

(i) provided by a consumer to a financial institution;

(ii) resulting from any transaction with the consumer or any service performed for the consumer, or;

(iii) otherwise obtained by the financial institution.”³²⁹

For purposes of businesses researching their cybersecurity requirements under GLBA, the Safeguards Rule is the most immediately relevant.

Safeguards Rule

The GLBA required each designated agency or authority to establish standards and physical safeguards:

1. to ensure the security and confidentiality of customer records and information;
2. to protect against any anticipated threats or hazards to the security or integrity of such records, and;
3. to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.³³⁰

The FTC, being granted authority to do so, has published guidance on how they want the Safeguard Rule implemented within businesses. Specifically, the FTC notes that businesses will be required to “develop a written [emphasis added] information security plan that describes their program to protect customer information.”³³¹

The specifics of the plan are “allowed” to be flexible, dependent on business size, services offered, and type of client information stored.

Regardless, the FTC requires every business to:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company’s operation and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information, and;
- evaluate and adjust the program considering relevant circumstances, including changes in business operations or the results of security testing and monitoring.

Regarding the above requirements, the FTC has placed importance on three areas: “Employee Management and Training; Information Systems; and Detecting and Managing System Failures.” FTC guidance on this area is too lengthy to list, so every business should consider visiting the following FTC website to glean further information:

<https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

Recently, the FTC brought an enforcement action against a nationwide tax preparer for, amongst other allegations, violating the Safeguards Rule.

In the Matter of TaxSlayer, LLC, the FTC brought an action against TaxSlayer for allegedly allowing nearly 8,882 TaxSlayer accounts to be accessed by hackers from October 10th, 2015 until December 21st, 2015. The FTC charged TaxSlayer with violating the GLBA’s Safeguards Rule.³³²

The FTC noted the following select violations of the Safeguards Rule, alleging TaxSlayer failed to:

- have a written information security plan until November 2015;

- failed to conduct a risk assessment;
- implement appropriate password requirements;
- implement risk-based authentication, such as two-factor authentication;
- failed to notify users when there was a material change made to their account.

333

In their settlement with the FTC, TaxSlayer is “prohibited from violating the... Safeguards Rule of the Gramm-Leach-Bliley Act for 20 years.” Further, TaxSlayer was required to obtain third-party compliance verification of these rules. biennially, for the following ten years.³³⁴

Such a case should serve as a stark warning to businesses of all sizes. Understanding the significance of the fact that only 8,882 people were affected but the FTC moved forward with an action is an indication that even smaller businesses could be subject to other FTC actions. Failure to adopt security standards as deemed appropriate by the FTC’s interpretation of the Safeguards Rule could result in legal action and significant trailing costs for years to come.

Regardless, compliance with GLBA is mandatory. Violation can result in up to five years in prison as well as potential fines. Businesses can be fined \$100,000 per violation. Officers and directors can face a \$10,000 fine per violation.³³⁵

Businesses should also note that the FTC periodically proposes amendments to its Safeguard and Privacy Rule under the GLBA. It is speculated that future proposals will more closely align FTC rules with notable cybersecurity standards such as the NY Department of Financial Services recent cybersecurity regulation, 23 NYCRR 500, and the NIST Cybersecurity Framework.³³⁶ This should spur continued research by businesses into understanding these regulations and how a similar adoption could impact their business.

Action Items:

- ☐ Work with legal counsel to review business policies and procedures to ensure compliance with FTC Guidelines;
- ☐ Review the FTC’s cybersecurity guide at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> ;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary;

- ☐ Review the previous chapter regarding FTC interpretation of reasonable cybersecurity requirements;
- ☐ Work with legal counsel to remain compliant with any changes in FTC guidance;
- ☐ Determine if your insurance policy would respond to allegations of FTC Safeguards Rule violations. Most often this will be found as “Regulatory Investigation” coverage.

Securities and Exchange Commission (SEC) Regulation S-P

Regulation S-P sets the GLBA Safeguard Rule requirements for investment advisers, investment companies, brokers, and dealers.³³⁷ For broker/dealers or an RIA licensed with the SEC, they should be aware of how the SEC interprets and enforces Regulation S-P. Not only does this have insurance implications, but it can have a direct impact on business practices.

Broadly speaking, Regulation S-P advises businesses on how they should maintain written information policies and procedures that address administrative, technical, and physical safeguards to protect client records and information. These policies and procedures must follow the same general goals of the GLBA; namely:

1. to ensure the security and confidentiality of customer records and information;
2. to protect against any anticipated threats or hazards to the security or integrity of such records, and;
3. to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.³³⁸

Additionally, the SEC provides guidance under Regulation S-P as to how businesses should dispose of consumer report information. Though sparse on specifics, “Disposal” means:

6. (A) The discarding or abandonment of consumer report information, or;
7. (B) The sale, donation, or transfer of any medium, including computer equipment [emphasis added], on which consumer report information is stored.³³⁹

In a recent Risk Alert, the SEC related the most common Regulation S-P compliance issues experienced by RIAs and broker-dealers.³⁴⁰ For purposes of brevity, these entities will collectively be referenced to as “firms” hereafter.

Privacy and Opt-Out Notices

Inspectors noted that firms failed in providing initial, annual, and opt-out notices to the customers. When these notices were provided, they often failed to accurately portray the firm’s true policies and procedures. In addition, the privacy notices did not give adequate notice to the clients that they could opt-out of having their personal information shared with “unaffiliated third parties.”³⁴¹

Lack of policies and procedures

Inspectors found that firms did not have the required written policies and procedures as required by Regulation S-P. Firms did possess documents that restated the regulation but did not include the policies and procedures necessary for administrative, technical, and physical safeguards. The inspectors also found firms where policies had adequately addressed the Privacy Notice but did not contain written policies and procedures required by the regulation.³⁴²

Policies did not reasonably safeguard client information or were not implemented

Here, the inspectors found numerous errors in how firms with written policies did not implement those policies or the policies were inadequate to safeguard client information. This included a lack of reasonable security on personal devices storing client information, lack of safeguards to prevent sending PII via unencrypted email, unsecured networks, unsecured physical locations, inadequate incident response plans, former employees who retained access, and lack of inventory for systems that maintained PII.³⁴³

Naturally, the SEC takes these violations seriously and has a website page dedicated exclusively to cyber-enforcement actions.³⁴⁴ As an example of a Regulation S-P enforcement action, consider the cases involving Morgan Stanley Smith Barney.

In this case, trouble initially began for Morgan Stanley when the FTC began an investigation on allegations of unfair or deceptive trade practices. From 2011 until 2014, an employee had unduly gained access to and transferred the data of 730,000 customers to his personal server. In turn, this server was hacked by third parties, and the client information appeared on numerous websites. Ultimately, the FTC decided to close the case because they believed that Morgan Stanley had taken the necessary steps to protect against insider theft.³⁴⁵

In turn, the SEC conducted its own investigation *In the Matter of Morgan Stanley Smith Barney*. The SEC released a finding that Morgan Stanley had “failed to adopt written policies and procedures reasonably designed to protect customer data.” As stated by the Director of the SEC Enforcement Division, “Given the dangers and impact of cyber breaches, data security is a critically important aspect of investor protection. We expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information[.]”³⁴⁶

Though the SEC’s press release is worthy of a read, the basis of their enforcement action was that Morgan Stanley had violated Rule 30(a) of Regulation

S-P, known as the “Safeguards Rule.” Morgan Stanley did not admit or deny the SEC’s findings but agreed to a \$1,000,000 penalty. The employee was ultimately sentenced to 36 months of probation and agreed to a \$600,000 restitution order.³⁴⁷

Greater guidance on how rules are applied should be investigated by businesses who may fall under SEC Regulation S-P. Businesses should seek guidance from their Compliance Officer and competent legal counsel.

Action Items:

- ☐ Work with legal counsel to determine if your business is subject to SEC Regulation S-P;
- ☐ Regulation S-P can be found at: https://www.sec.gov/rules/final/34-42974.htm#P80_19305;
- ☐ Work with legal counsel to review business policies and procedures to ensure compliance with SEC Guidelines;
- ☐ Determine if your policy would respond to allegations of SEC Regulation S-P violations. Most often this will be found as “Regulatory Investigation” coverage;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Damage Control

SEC Custody Rule

The SEC Custody Rule, Rule 206(4)-2 under Section 206(4) of the Investment Advisers Act of 1940, is not a “cybersecurity” rule, *per se*, but can have internal cybersecurity controls and business practice implications.

In December of 2009, the SEC adopted amendments to the custody rule for investment advisors as it applies to the client’s funds or securities. Notably, these amendments were created to provide an additional level of client safeguards when an advisor had custody of client assets. Among provisions in the rule are requirements to maintain client assets with a qualified custodian, or to engage an independent CPA to conduct a surprise examination.³⁴⁸

Trouble began in June of 2012 for GW & Wade when a client’s email account had been compromised, and a hacker posed as the client. The hacker then requested GW & Wade to wire a total of \$290,000 via three separate wires to a foreign bank. Ultimately, the fraud was discovered, and the client was reimbursed the lost sum.³⁴⁹

In late 2013, the SEC issued an order instituting administrative proceedings *In the Matter of GW & Wade, LLC*. The SEC asserted that the firm was subject to the custody rule due to having pre-signed letters of authorization. This enabled GW & Wade to transfer client funds without obtaining a client’s contemporaneous signature. Further, the SEC alleged that GW & Wade had “not adopted or implemented policies and procedures reasonably designed to prevent violations of the securities laws and rules governing custody of client assets or kept required books and records for certain custodial accounts” and had erred in its mandatory Form ADV disclosures.³⁵⁰

The SEC also noted that there were other practices within the firm that could have caused issues. This includes GW & Wades’ being granted third-party delegation on clients’ check-writing accounts, as well as login and password information for those accounts.³⁵¹

GW & Wade ultimately consented to a censure and cease-and-desist order. They paid a \$250,000 penalty.³⁵²

Action Items:

- ☐ Determine if your business is subject to SEC Custody Rule; the SEC Custody Rule can be found at: <https://www.sec.gov/rules/final/2009/ia-2968.pdf>;
- ☐ SEC Staff response to questions about the Custody Rule can be found at: https://www.sec.gov/divisions/investment/custody_faq_030510.htm;

- ☐ Work with legal counsel to review business policies and procedures to ensure compliance with SEC Custody Rule Guidelines;
- ☐ Determine which policies may respond to allegations of SEC Custody Rule violations. This may be a professional liability policy, or a cyber policy dependent up the allegations;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary.

Red Flag Rule(s) – SEC & FTC

In 2012, the Dodd-Frank Wall Street and Consumer Protection Act amended the Fair Credit Reporting Act. Effectively, this transferred the rulemaking and enforcement authority for identity theft Red Flag Rules to the various agencies.

You have to mark one in the win column for the AICPA lobbying efforts that undoubtedly was part of the reason the FTC's authority to make businesses adhere to the Red Flag Rule ended with the Red Flag Program Clarification Act of 2010.³⁵³ However, for businesses with a broker-dealer, or investment advisers registered with state regulators, they may still have that portion of their business needing to adhere to the FTC Red Flag Rule. The FTC has its own Red Flag Rules that roughly mirror those propagated by the SEC. Per the statute, a red flag means "a pattern, practice, or specific activity that indicates the possible existence of identity theft."³⁵⁴

Known as Regulation S-ID: Identity Theft Red Flags, but generally referred to as the "Red Flags Rule," the SEC requires financial institutions and creditors that offer any number of covered accounts to develop a written identity theft program.

The written plan concerning Red Flag Rules is used to help the business meet the four following goals:

1. Identification of relevant Red Flags: Factors that should be considered include the type of covered accounts, the method it provides to open and access such accounts, as well as any previous incidents of identity theft. The sources of Red Flags should also be considered to include prior incidents of identity theft and any methods of identity theft that have been identified that would change the risk of identity theft. Categories of Red Flags should also be addressed, such as reports from service providers, suspicious documents, and any other doubtful activity.
2. Detecting Red Flags: Businesses should obtain and verify the proper ID of anyone opening a covered account. They should also monitor all transactions and verify the validity of a covered account requesting a change of address.
3. Preventing and mitigating identity theft: When Red Flags are detected, the business must respond appropriately. This could include customer contact, notifying law enforcement, changing methods of access, or even no response if that is warranted.

Updating the Program

The business's written plan should be a living document that requires periodic updates. Such updates should reflect the evolving risk to customers based on factors such as changing methods of identity theft, experience by the business, and changes in available methods to detect, mitigate, or prevent such theft.

In the Matter of Voya Financial Advisors, Inc., was the third known action brought against a firm for violating Regulation S-P (the Safeguards Rule), and the first action brought against a firm for violating the Identity Theft Red Flags Rule.³⁵⁵

Per the SEC, at least one person impersonating Voya's contractor representative interacted over the phone with Voya's tech-support line to reset three representative's web portal passwords. These web portals allowed access to customer information.³⁵⁶

On two occasions, the impersonator used phone numbers that the firm had previously flagged as being associated with fraudulent activity. Regardless, Voya's support staff reset the three passwords and provided temporary passwords via phone. In two of those instances, Voya staff had also provided the username of the representative to the impersonator.³⁵⁷

The first indication that foul play had occurred happened three hours following the first impersonator request when a representative whose account had been affected called Voya's support staff. He notified the staff that he had received an email confirming the password on his account had been changed, but he had never requested such action be initiated.³⁵⁸

Voya responded to the intrusion but failed to prevent the intrusion of two other representative accounts using the same attack vector. Ultimately, the impersonators were able to use the obtained usernames and passwords to gain access to at least 5,600 customer's personally identifiable information. There were no known fraudulent transfers of money or securities from the affected customer's accounts.³⁵⁹

Though Voya had policies and procedures to protect their customer's information as well as to prevent and respond to cybersecurity incidents, SEC alleged that they were not "reasonably designed to meet these objectives." More specifically, Voya policies were not designed properly for their representatives, and they did not identify those representatives and customers that were higher risk and thus required additional security measures. As such, SEC alleged that Voya violated Regulation S-P (Safeguards Rule).³⁶⁰

Finally, Voya had written and adopted a Theft Prevention Program. However, their program was deemed to have been an additional violation of the Red Flag Rule. The SEC alleged that it was not reviewed and updated as necessary to include changes to customer risks seen at the time. The SEC also alleged that Voya did not

provide adequate training to their employees to properly identify and respond to identity theft red flags.³⁶¹

Though Voya did not admit or deny the allegations of the SEC, they agreed to be censured in addition to paying a \$1 million penalty.³⁶²

Action Items:

- ☐ Determine if your business is subject to the SEC or FTC Red Flag Rules;
- ☐ Work with legal counsel to review business policies and procedures to ensure compliance with applicable SEC and FTC Guidelines;
- ☐ Determine which policies may respond to allegations of SEC or FTC Red Flag Rule violations. This may be a professional liability policy, or a cyber policy; dependent up the allegations;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary.

EU-US & Swiss-US Privacy Shield frameworks

The EU-US Privacy Shield replaced the International Safe Harbor Privacy Principles after the latter was deemed to be invalid.³⁶³ Broadly speaking, Privacy Shield is a voluntary framework that regulates the transmission of personal data for commercial reasons that occur between the European Union and the United States.³⁶⁴ The Swiss-US Privacy Shield is identical to the EU-US Privacy Shield.

The Department of Commerce maintains a list of companies that have voluntarily joined Privacy Shield. FTC acts as the enforcement body for the program within the United States. Failure to fully comply with the principles of the Privacy Shield Framework will be enforced under Section 5 of the FTC Act which prohibits unfair and deceptive acts.³⁶⁵

Naturally, the Privacy Shield is a complex undertaking with seven privacy principles:

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation
- Access
- Recourse, Enforcement, and Liability³⁶⁶

In addition to the above privacy principles, Privacy Shield also contains 16 supplemental principles that either augment or explain the privacy principles. These include:

- Sensitive Data
- Journalistic Expectations
- Secondary Liability
- Performing Due Diligence
- The Role of the Data Protection Authorities
- Self-Certification

- Verification
- Access
- Human Resources Data
- Obligatory Contracts for Onward Transfers
- Dispute Resolution and Enforcement
- Choice - Timing of Opt-out
- Travel Information
- Pharmaceutical and Medical Products
- Public Record and Publicly Available Information
- Access Requests by Public Authorities³⁶⁷

To date, the FTC has but a handful of enforcement actions related to Privacy Shield. The actions have focused on a lack of proper registration or failures to maintain accurate privacy policies reflecting the status of their programs.³⁶⁸ It has been reported that the FTC is looking to bring a higher number of actions against companies that show “substantial violations” of the Privacy Shield.³⁶⁹

Consider the allegations made by the FTC *In the Matter of SecurTest, Inc.*

SecurTest is a Florida-based company that provides employment background checks, drug testing, and other employment-related services.³⁷⁰ The FTC alleged that SecurTest published statements related to its participation in the EU-US Privacy Shield framework on its website. One such alleged statement was the following:³⁷¹

SecurTest, Inc. complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from European Union and Switzerland to the United States, respectively. SecurTest, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit <https://www.privacyshield.gov/The> [sic] terms of this policy apply to SecurTest’s Web site and Background Screening Solutions, except where noted.]

In its complaint, the FTC alleged that SecurTest had begun its Privacy Shield application with the Department of Commerce in September of 2017. In October of 2017, SecurTest had added a note on the bottom of its webpage noting that their application was pending. Although they allegedly failed to meet the certification timelines as established by the Department of Commerce, SecurTest continued to display the EU-US Privacy Shield paragraph shown previously, on its website.³⁷²

FTC subsequently contacted SecurTest regarding the matter. SecurTest subsequently completed the necessary steps to participate in the Privacy Shield framework and received certification on August 31, 2018.³⁷³

The FTC alleged SecurTest to have violated Section 5 of the FTC Act.³⁷⁴

In its decision and order, the FTC mandated SecurTest to engage in the following:

- Acknowledge the order;
- Deliver a copy of the order to all relevant parties within the business and have them acknowledge the order in writing within 30 days;
- Submit a compliance report to the FTC within 60 days;
- Submit a compliance notice to the FTC within 14 days of any material changes to the business;
- Create records for 10 years, and keep for 5 years, as they pertain to the order;
- Adhere to compliance orders as deemed necessary by the FTC;
- The order will be effective for 20 years.³⁷⁵

For businesses who are currently, or are contemplating, adherence to the Privacy Shield Frameworks, there are various insurance implications to consider.

Most importantly, businesses will need to be careful regarding how they complete any section on their cyber insurance application regarding federal or international security and privacy laws affecting their business. Privacy Shield requires an annual re-certification as well as year-round compliance. Failure to adhere to these mandates could be deemed a material misrepresentation by an insurer leading to a potential coverage declination.

In addition, businesses will need to reference the relevant language in their cyber insurance policy. At a minimum, they will need to determine if a regulatory proceeding brought by the FTC regarding the Privacy Shield frameworks would be considered a covered claim. It is unlikely that any follow-on compliance costs will be covered, though businesses should also consider them when looking for coverage.

Action Items:

- ☐ Requirements to participate in the EU-US Privacy Shield can be found at: <https://www.privacyshield.gov/article?id=Requirements-of-Participation;>
- ☐ Determine if your business is currently a participant in the EU-US or Swiss-US Privacy Shield frameworks;
- ☐ Reference your cyber policy to determine if “regulatory proceedings” brought under the Privacy Shield are considered a covered claim;
- ☐ Work with relevant stakeholders, including IT and Legal, to ensure year-round compliance within the framework;
- ☐ Update the business’s incident response plan as necessary.

Damage Control

Payment Card Industry Data Security Standards (PCI DSS)

Payment Card Industry Data Security Standards (PCI DSS) compliance is not legally mandated, but rather is founded and governed by the major credit card companies such as Visa, Mastercard, Discover, and American Express.

On their website, PCI DSS lists the following six goals. Numerous requirements exist within each goal:

- **“Build and Maintain a Secure Network”**: Includes the use of a firewall and checking that default system passwords are changed;
- **“Protect Cardholder Data”**: Includes protecting cardholder data that is stored, along with the encryption of cardholder data when it is sent across public networks;
- **“Maintain A Vulnerability Management Program”**: Includes the use of anti-virus software and maintaining secure applications and systems;
- **“Implement Strong Access Control Measures”**: Includes physical safeguards to cardholder data and the implementation of unique IDs to everyone with computer access;
- **“Regularly Monitor and Test Networks”**: Includes the regular testing of computer security systems and well as the monitoring of access to the computer network;
- **“Maintain an Information Security Policy”**: Includes the maintenance of a policy that addresses security for both contractors and employees.³⁷⁶

Many businesses mistakenly believe that if they are using a third-party payment processor, PCI DSS does not apply to them, and thus coverage for PCI DSS is unnecessary in their cyber policy. Of note, the PCI DSS website states, “If you accept or process payment cards, the PCI Data Security Standards apply to you.” Businesses should also refer to their Merchant Service Agreement to assess any further liability.

When a business decides to utilize a third-party payment processor, they will often be asked to complete one of the PCI DSS Self-Assessment Questionnaire and Attestation of Compliance forms. The depth of these forms will depend upon the circumstances of the business, as there are nine different types of questionnaires available.³⁷⁷

For a business where the payment card is not present and all payment processing functions are fully outsourced, they would likely be required to complete “Self-Assessment Questionnaire A and Attestation of Compliance.” Businesses should understand that they are attesting to various security controls that must be adhered to.

Assuming a business uses a webpage for billing purposes which is hosted by a payment processor, how could a business reasonably be subject to PCI DSS fines, penalties, or assessments?

Outside of a sophisticated attack, it could be as simple as an email breach where clients had sent the business their credit card information via email despite the business warning otherwise. Another common example could be physical copies of billing information data being stolen from the business.

Regardless of the myriad scenarios that could lead to a breach, it is worth noting that credit card companies and banks do not take lightly to payment card breaches which result from non-compliance with PCI DSS. While the total fines are generally not made public, it has been estimated that fines for non-compliance can range from \$5,000 to \$500,000, with large businesses facing fines in the millions.³⁷⁸ Such fines do not include assessments for additional Operational Reimbursement and Fraud Recovery Costs, as detailed in the latter mentioned case of *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*³⁷⁹ Further, the ability to utilize the payment card system could be revoked entirely, leading to potentially severe income issues.³⁸⁰

Indeed, even if businesses were to purport that they had adhered to PCI DSS standards, such representations may not persuade the FTC that a business has enacted reasonable security standards. Such was the case of *FTC v. LifeLock, Inc.*

In 2010, the FTC brought a complaint against LifeLock, a popular identity theft protection company. In their complaint, the FTC alleged that LifeLock advertisements regarding the protection of their customers were misleading as there was no definitive way to guarantee against identity theft. Furthermore, LifeLock was not adhering to advertised controls such as encryption and “need to know” access rights.³⁸¹

FTC Chairman Jon Leibowitz noted, “While LifeLock promised consumers complete protection against all types of identity theft, in truth, the protection it actually provided left enough holes that you could drive a truck through it.”³⁸²

As an additional word of warning concerning a previous explanation of state-level actions, the following attorneys general participated in the LifeLock settlement: Alaska, Arizona, California, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Missouri, Mississippi, Montana, Nebraska, Nevada, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, and West Virginia.³⁸³

Ultimately, LifeLock agreed to a \$12 million settlement. Additionally, they agreed to a biennial third-party assessment of a broad data and cybersecurity program.³⁸⁴

Trouble returned for LifeLock approximately five years later when the FTC filed a contempt proceeding. Following an investigation, the FTC alleged the numerous deficiencies in LifeLock's 2010 order. In particular, they failed to "maintain reasonable security measures to protect its users' sensitive personal data, including credit card...and bank account numbers..." This, despite LifeLock asserting that they had complied with PCI DSS and that there was no evidence of a breach having affected their customers.³⁸⁵

Notably, the FTC commission issued a stark warning on their view of the difference between certification and compliance. "Certifications alone will not suffice to meet those obligations if we find evidence of security failures that put consumer information at risk...PCI DSS certification is insufficient in and of itself to establish the existence of reasonable security protections [underline added]... [T]he existence of a PCI DSS certification is an important consideration in, but by no means the end of, our analysis of reasonable security."³⁸⁶

The FTC noted that a previous case had called for "additional significant protections, including the implementation of risk assessments, certification of untrusted networks, and certification of the assessor's independence and freedom from conflicts of interest."³⁸⁷

Under the terms of the settlement, LifeLock was required to deposit \$100 million into the U.S. District Court for the District of Arizona's registry. Of that, \$68 million would be used to refund fees paid by class-action consumers who alleged injuries noted by the FTC. Any money not specified for use in consumer actions would be "provided to the FTC for use in further consumer redress."³⁸⁸

Regardless of whether businesses consider the FTC's arguments to be pedantic, they should consider how the PCI Security Standards Council described their data security standards before the U.S. House Financial Services Committee. "PCI Standards, along with many other tools [underline added], will provide a strong baseline for card data protection programs."³⁸⁹

Meeting baseline standards of PCI DSS compliance and evidencing appropriate and reasonable security measures before the FTC are two very different undertakings. Businesses must take additional cybersecurity measures suitable to their business's exposure to maximize their chances of avoiding FTC actions.

Action Items:

- ☐ Determine if your business is subject to PCI DSS. You will also likely need to reference your Merchant Services Agreement (MSA);

- ☐ Continuously monitor compliance with PCI DSS requirements. Failure to do so could result in a declination of coverage;
- ☐ Check that the business is adequately protecting all covered payment card data appropriately;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary;
- ☐ Additional information regarding PCI DSS can be found at: <https://www.pcisecuritystandards.org/>
- ☐ Determine if the business has coverage for any PCI DSS-related claims and associated expenses.

AICPA/IRS Requirements

The AICPA seemingly has nothing to say regarding the enforcement of cybersecurity within accounting firms. It appears that they wholly defer to the FTC and IRS when dealing with cybersecurity.

In Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*, the IRS noted, “Failing to take necessary steps to implement or correct your security program may result in sanctions from the FTC. Failures that lead to an unauthorized disclosure may subject you to penalties under sections 7216 and/or 6713 of the Internal Revenue Code (I.R.C.).”³⁹⁰

I.R.C. 7216 notes in part, “Any person who is engaged in the business of preparing, or providing services in connection with the preparation of, returns of the tax imposed by Chapter 1, or any person who for compensation prepares any such return for any other person, and who knowingly or recklessly...discloses any information furnished to him for, or in connection with, the preparation of any such return...shall be fined not more than \$1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution [underline added].”³⁹¹

I.R.C. 6713 notes in part, “Imposition of penalty: If any person who is engaged in the business of preparing, or providing services in connection with the preparation of, returns of tax imposed by chapter 1, or any person who for compensation prepares any such return for any other person, and who...discloses any information furnished to him for, or in connection with, the preparation of any such return...shall pay a penalty of \$250 for each such disclosure or use, but the total amount imposed under this subsection on such a person for any calendar year shall not exceed \$10,000 [underline added]... Exceptions: The rules of section 7216(b) shall apply for purposes of this section.”³⁹²

Outside of immediate monetary penalties assessed by the IRS, firms registered as Electronic Return Originators (EROs), or Transmitters, may have additional concerns. As stated in IRS Publication 1345, “Providers with problems involving fraud and abuse may be suspended or expelled from participation in IRS e-file, be assessed civil and preparer penalties or be subject to legal action.”³⁹³ Regarding e-file, the IRS noted in a late 2018 Tax Tip that they “may treat a violation of the FTC Safeguards Rule as a violation of IRS Revenue Procedure 2007-40.”³⁹⁴

As a brief synopsis of Revenue Procedure 2007-40, the IRS stated, “This procedure specifies the requirements for participating as an Authorized IRS e-file Provider and is the official set of rules that govern participation in IRS e-file. The procedure revises [previous Revenue Procedures] by providing for denial of

application or revocation of an Authorized IRS e-file Provider's participation in IRS e-file if it has been enjoined from filing returns by a federal or state court injunction or other legal action that would prevent its participation in the program.”³⁹⁵

More succinctly, if a firm fails to properly secure client data, they could:

- have their e-file access revoked or suspended;
- be subject to action by the FTC;
- face penalties and possible prison sentences by the IRS.

As firms are investigating their adherence to the FTC Safeguards Rule, they should reference IRS Publication 4557, *Safeguarding Taxpayer Data: A Guide for Your Business*. This is a short guide with convenient checklists to assist firms in understanding their compliance requirements. The publication appears to provide non-mandatory guidance on security best-practices but is based upon The FTC Safeguards Rule.

Publication 4557 is unique in that it attempts to assist accounting firms with directly safeguarding taxpayer data. Keep in mind that the included “Safeguards Rule Checklist” does not guarantee full compliance with the FTC’s interpretation of the Safeguard Rule. However, it is a good starting point for most firms looking to increase their cybersecurity posture and awareness.

It is unknown at the time of publication whether the IRS has investigated and fined a firm for violations of IRC 7216 or IRC 6713 following a breach of confidential client information. Further, it is unknown if the IRS has sanctioned an e-file Provider for a breach of their computer system. However, if tax fraud continues to plague the IRS and significant dollar losses accumulate, it is conceivable that action will eventually be taken.

Were such fines, penalties, and actions to befall a firm, there are two primary policies that may respond: professional liability and cyber insurance policies.

Foremost, many firms would look to their professional liability policy. While most professional liability policies do include a sublimit for regulatory proceedings and disciplinary actions, they generally cover between \$5,000 and \$50,000 for defense costs but do not typically cover monetary fines, assessments, or penalties. Whether the policy would respond to an IRS proceeding or hearing is likely speculative as the defense is limited to actions brought by entities regulating the practice of accountancy.³⁹⁶

Finally, firms may also look toward their cyber insurance policy for coverage. The inclusion and applicability of coverage and defense for regulatory claims varies by insurer and policy. Thus, firms should investigate the coverage features, and definitions therein, with scrutiny.

Action Items:

- ☐ IRS Publication 1345: Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns can be found for free at: <https://www.irs.gov/pub/irs-pdf/p1345.pdf>;
- ☐ IRS Publication 4557 can be found for free at: <https://www.irs.gov/pub/irs-pdf/p4557.pdf>;
- ☐ Continuously monitor IRS publications for any changes in the law;
- ☐ Check that the firm is adequately protecting all covered data appropriately;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the firm's incident response plan and other internal documents as necessary.

American Bar Association Requirements

For licensed attorneys and law firms, the American Bar Association has additional guidance concerning data security. While it may seem strange that hackers would attempt to specifically infiltrate an attorney's computer, the information stored on those computers could be worth big money.

In one notorious example, hackers gained access to some of the country's largest law firms to access confidential client information. Their goal was to utilize that information with insider trader schemes.³⁹⁷

While large firms are obvious targets, smaller firms may inadvertently fall in the crosshairs of ideologically driven hackers. In 2012, the law firm of Puckett & Faraj was targeted by the hacktivist group "Anonymous." The firm was known for defending U.S. military service members accused of war crimes. The following is a series of emails allegedly from the firm of Puckett & Faraj, released by Anonymous after the breach.³⁹⁸

One of the firm leaders apparently first learned of the breach via the news.

```
From: "[REDACTED]" <[REDACTED]@puckettfaraj.com>
Date: Fri, 3 Feb 2012 13:54:57 -0500
Subject: Damage assessment
Cc: [REDACTED] <[REDACTED]@puckettfaraj.com>,
    [REDACTED] <[REDACTED]@puckettfaraj.com>
To: [REDACTED] <[REDACTED]>

[REDACTED],

News agencies are reporting that our website was hacked and that the
hackers claim our emails and sensitive personal information was taken.
Is that possible?

Neal
[REDACTED]
Puckett & Faraj, PLLC
1800 Diagonal Rd, Suite 210
Alexandria, VA 22314
703.706.9566
www.puckettfaraj.com
```

On the next page, a firm member who was cc'd on the previous email vents his frustration concerning their cloud service provider:

From: [REDACTED] <[REDACTED]@puckettfaraj.com>
 Subject: Re: EMERGENCY!!!!
 Date: Fri, 3 Feb 2012 13:37:38 -0500
 To: "[REDACTED]" <[REDACTED]@puckettfaraj.com>

Why the fuck does [REDACTED] not know about this before we have to tell them.

Sent from my iPhone

Here is a portion of the email sent from the cloud service provider to the firm:

From: [REDACTED] <[REDACTED]>
 In-Reply-To: <[REDACTED]@puckettfaraj.com>
 Date: Fri, 3 Feb 2012 10:55:08 -0800
 Cc: [REDACTED] <[REDACTED]@puckettfaraj.com>,
 [REDACTED] <[REDACTED]@puckettfaraj.com>
 To: "[REDACTED]" <[REDACTED]@puckettfaraj.com>

Hi [REDACTED],

This was done by someone who clearly knows what they are doing. Anonymous is one of the largest, if not THE largest group of hackers in the world at this time. They've taken down Sony, DoD and many others in recent months.

This isn't like the previous hack where one file was replaced and it redirected. In this case Anon was able to gain FTP access directly to the server and remove ALL files to your site. We're working on restoring the backups now, and looking to see how far this attack went. At this time, it only looks like the web files were removed, but the database was left intact and untouched.

We're going to have to lock down not only the front end (as done previously), but we are going to have to limit the IP addresses that can access anything to do with the server.

Unfortunately, there are a couple things to consider with this one:

- This was clearly not a random attack.
- If this truly is anon, it may not be limited to just your site or just this one attack. Currently, your domain is on a web server that hosts some of our other sites and clients as well. It may be a good idea to host your site on a fully secured private web server. This can run from \$400 - \$2,000 per month. On a shared server, the other domains could be vectors for possible access to your site as well.
- Anonymous is a little out of my league. Since you are being targeted, I would suggest hiring a specialist for this type of matter.

As far as reporting this, and to who, I must admit that I'm not exactly sure. I believe it would be the FBI. Here's a government resource I was able to find on the matter: <http://www.cybercrime.gov/reporting.htm>

Please feel free to give me a call on my cell phone to discuss further.

With Best Regards,

[REDACTED]

An email sent by a hacker to a member of the firm confirmed the breach:

From: [REDACTED]@gmail.com
Subject: HAHHAHAHA
Date: February 3, 2012 12:53:24 PM EST
To: [REDACTED]@puckettfaraj.com

YOU GOT OWNED, YOU SICK, TWISTED RUBBISH

Here, a member of the firm acknowledges to their mother that they are in serious trouble:

On Fri, Feb 3, 2012 at 2:35 PM, [REDACTED]
<[REDACTED]@comcast.net> wrote:

Mom, this group who hacked the law firm has stolen
all our Emails and client information. They may
have the ability to send you Emails by |
impersonating me. Please don't answer any emails
from [REDACTED]@puckettfaraj.com. We are on hold with
Google trying to get the Emails completely shut
down.

This may completely destroy the Law Firm.
[REDACTED]

Assuredly, high-profile episodes such as the one above spurred the American Bar Association (ABA) into action. In mid-2017, ABA released an update to the arguably antiquated Formal Opinion 99-413, via Formal Opinion 477R, *Securing Communication of Protected Client Information*. This opinion, while lengthy, fundamentally detailed “a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.”³⁹⁹

This opinion included a brief description of the Duty of Competence, the Duty of Confidentiality, and the Duty to Communicate as they relate to cybersecurity. While it did not specify what “reasonable steps” a lawyer should take, it did offer the following considerations that should be understood:

- The nature of threats;

- Where client information is stored and how it is transmitted;
- The use of cybersecurity tools to prevent disclosure of confidential client information;
- How a client's electronic communications should be protected;
- Labeling of confidential client information;
- The training of attorneys and staff members on information security;
- Providing due diligence on technology vendors.⁴⁰⁰

Picking up where Formal Opinion 477R ended, the ABA more recently issued Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack*. With this new guidance, the Standing Committee on Ethics and Professional Responsibility has provided detailed guidance on an attorney's obligations to both former and current clients when either the client or the firm has become the victim of a data breach.

While Formal Opinion 483 is exhaustive and should be read by anyone who believes they may be required to follow its mandates, there are a few key points worthy of further consideration.

Per the ABA, a "data breach" is defined as "a data event where material client confidential information is misappropriated, destroyed, or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."⁴⁰¹ This greatly expands an attorney's obligations beyond information specifically mentioned in other statutory regimes noted in this book.

To comply with this provision, firms should understand whether their cyber policy allows for voluntary notifications. Whether anyone cyber insurer will agree to adhere to the obligations seen in this opinion is unknown and should be investigated by the firm prior to the purchase of a cyber insurance policy.

When a data breach is detected or suspected, a lawyer has the duty to act "reasonably and promptly" to both mitigate damage and stop the breach.⁴⁰² Performing these actions faithfully will require foresight by the firm and likely require an incident response plan.

According to the opinion, the Model Rules do not impose different standards on a physical breach or an electronic breach.⁴⁰³ This should give firms pause to assess both the physical and digital security of their clients' confidential information.

Following the detection of a breach, a lawyer should conduct a post-breach investigation to verify that the intrusion has been halted. Following the stoppage, a

lawyer should assess what data was lost or accessed.⁴⁰⁴ Most commonly, this could be accomplished with a computer forensic expert.

When a lawyer knows or should have known that a data breach occurred, they must provide a notice to their current client(s) “to permit the client to make informed decisions regarding the representation.”⁴⁰⁵

Interestingly, Opinion 483 does not explicitly require lawyers to notify formal clients of a data breach. However, the ABA does mention that attorneys should reference any contractual obligations they may have, as well as any other regulatory or statutory requirements to which they must adhere.⁴⁰⁶

The ABA also refers to a firm’s document retention schedule/policy. This is meant to limit the amount of information that would fall into the hands of unauthorized parties and ultimately require notification by the lawyer.⁴⁰⁷

Formal Opinion 483 then circles back to the previously mentioned Formal Opinion 477R to discuss how the ABA views, “reasonable” security. A firm is not required to be “invulnerable or impenetrable,” but they are obliged to make a reasonable effort. What “reasonable” means is ultimately a term that will be defined depending on the firm. As referenced in the ABA Cybersecurity Handbook:

“Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.”⁴⁰⁸

While this may not be particularly enlightening, firms may find greater guidance in cybersecurity, such as NIST CSF, to evidence a “reasonable” cybersecurity posture. NIST CSF is covered later in this book, though there are numerous other frameworks or formalized approaches that may fulfill this obligation.

In total, both Formal Opinions contain a litany of references to various Model Rules that have implications on cybersecurity and thus require constant vigilance. In addition, each state’s Bar Association may have additional requirements that warrant further study. As stated by the ABA, violations of the Model Rules can lead to significant sanctions; to include:

- Disbarment;
- Suspension;
- Probation;

- Reprimand;
- Admonition by disciplinary counsel;
- Reimbursement for fees associated with the disciplinary action;
- Limitation by the court on a respondent's future practice.⁴⁰⁹

From all this, firms should understand that by employing JDs within their practice, they may be subjecting themselves to greater cybersecurity requirements. These additional requirements will need to be understood and dealt with before a firm can confidently complete a cyber insurance application without risking a declination in coverage for material misrepresentations.

Action Items:

- ☐ Formal Opinion 483; Lawyers' Obligations After an Electronic Data Breach or Cyberattack can be found for free at: https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf;
- ☐ Understand if your firm is subject to any ABA cybersecurity rules;
- ☐ Continuously monitor those rules for any changes;
- ☐ Check that your firm is adequately protecting all covered data appropriately;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the firm's incident response plan and other internal documents as necessary;

Determine if the firm's cyber insurance or professional liability policy would cover actions brought by the ABA – or equivalent state-level bodies – for breach related claims.

Financial Industry Regulatory Authority (FINRA)

FINRA, the Financial Industry Regulatory Authority, is a self-regulatory organization that oversees several areas, including broker-dealers. For firms that operate a broker-dealer, they should understand and continuously assess FINRA's view of cybersecurity.

It does not appear that FINRA has any specific cybersecurity mandates that broker-dealers must follow, though FINRA rule 4370 does require a business continuity plan that may require disclosures on data backup and recovery methods and procedures.⁴¹⁰

To date, the only discovered FINRA disciplinary action mentioning cybersecurity revolved around the format of electronic record retention.

In 2017, FINRA imposed fines on twelve firms alleging significant deficiencies in preserving customer records in a non-alterable format. Per the report, both federal securities laws and FINRA rules mandate that business-related records in electronic format are to be kept in a "write once, read many" (WORM) format. This data format is deemed crucial by the SEC for "monitoring compliance with applicable securities laws, including antifraud provisions and financial responsibility standards."⁴¹¹

FINRA also found that three of the 12 firms also failed in their retention requirements under certain record retention rules.

Recently, FINRA issued recommendations and best practices to address the most common cybersecurity risks for broker-dealer firms, the *Report on Selected Cybersecurity Practices – 2018*. They acknowledge that the report does not create a legal opinion nor does it create a new legal requirement for broker-dealers to follow. Topics include:

- Branch controls such as written security plans (WSPs), asset inventories, technical controls, and a branch review program;
- Useful tips on countering common social engineering ploys such as "phishing;"
- A discussion on insider threats with useful countermeasures;
- Penetration testing;
- Mobile device security.

More immediately useful for most firms would be FINRA's *Small Firm Cybersecurity Checklist*. This checklist is derived from the NIST Cybersecurity

Framework and FINRA's 2015 Report on Cybersecurity Practices. However, the website mentions that the checklist does not create a safe harbor for any law, so firms will still need to perform their own due diligence.

Finally, FINRA has issued at least one investor alert urging consumers to question their brokerage firms about the topic of cybersecurity. Questions included the naming of safeguards, reimbursement of assets following a breach, and whether the brokerage monitors the customer's assets to ascertain whether their information has been unduly used or stolen.⁴¹² Firms should be ready to answer these questions without hesitation as consumers become savvier of cybersecurity in their lives.

Action Items:

- ☐ FINRA's *Small Firm Cybersecurity Checklist* can be found at: <http://www.finra.org/industry/small-firm-cybersecurity-checklist>;
- ☐ FINRA's *Report on Selected Cybersecurity Practices – 2018* can be found at: https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf;
- ☐ FINRA's *Small Firm Business Continuity Plan Template* can be found at: <http://www.finra.org/industry/small-firm-business-continuity-plan-template>;
- ☐ If your firm falls under the oversight of FINRA, make sure that you are following are required security practices;
- ☐ Continuously monitor for any changes made by FINRA regarding cybersecurity;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the firm's incident response plan and other internal documents as necessary;
- ☐ Determine if the firm's cyber insurance policy covers a claim brought by FINRA following a data breach.

Government Contractors: Cybersecurity Maturity Model Certification Model (CMMC)

Previously, DoD contractors would self-attest to their cybersecurity posture as there was no mandatory third-party certification process, even for those contractors handling Controlled Unclassified Information (CUI).⁴¹³ Apparently, this self-attestation was not working as Katie Arrington, the special assistant for cyber in the Office of the Assistant Secretary of Defense for Acquisition, stated that the United States was “losing \$600 billion a year to our adversaries in exfiltration, data rights, R&D loss.”⁴¹⁴ To combat this loss, the government has created the Cybersecurity Maturity Model Certification Model (CMMC) to mandate and quantify contractor’s cybersecurity.

CMMC’s governing body will train and license Certified 3rd Party Assessment Organizations (C3PAOs) and their assessors. In turn, these C3PAOs will be comprised of at least two assessors who can certify a contractor’s CMMC License Level. The assessors will not be CMMC Accreditation Board (CMMC-AB) employees.⁴¹⁵ According to one source, the Pentagon wants these assessors to be independent, so assessors will not be allowed to sell contractors other cyber services.⁴¹⁶

When CMMC will become “live” is speculative as of this publication. According to Lockheed Martin, CMMC will be included in RFI’s starting roughly in June of 2020, and in RFPs starting roughly in September of 2020.⁴¹⁷ Many industry experts believe that CMMC will undergo changes in the future, so contractors should remain vigilant.

How the CMMC will apply to subcontractors is not explicitly apparent in the controlling documents. Merely, the CMMC V1 states that a contractor can “adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.”⁴¹⁸ Nevertheless, it is safe to assume that every contractor handling sensitive information will need to be certified to at least the fundamental level.

Covered Information Types

CMMC is designed to cover two types of information which are commonly held by contractors:

- Federal Contract Information (FCI), which is, “information, not intended for public release that is provided by or generated for the Government under a

contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.”⁴¹⁹

Initially, this definition is found outside of the CMMC within the Federal Acquisition Regulation (FAR) 52.204-21. This regulation is also known as “Basic Safeguarding of Covered Contractor Information Systems.”

- Controlled Unclassified Information (CUI), which is, “information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under EO 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.”⁴²⁰ Broadly, the safeguarding of CUI is found in Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7012).⁴²¹

The CUI Registry is quite extensive and contains numerous categories and subcategories. Depending on the engagement and specialty of the contractor, they could be handling information from any number of CUI categories.⁴²² Contractors are encouraged to reference the CUI categories found at:

<https://www.archives.gov/cui/registry/category-list>.

CMMC Levels

The CMMC contains five cumulative levels that will be mandated by the government, depending on the particular contract. They can generally be understood with the following descriptions:

- **Level 1:** The contractor practices basic cyber hygiene by utilizing the basic safeguarding requirements found in FAR 52.204-21.⁴²³ At this level, contractors will presumably be dealing only with FCI.
- **Level 2:** The contractor satisfies the requirements of Level 1, but also documents and implements practices and policies to comply with part of NIST SP 800-171 and selected other sources.⁴²⁴ At this level, contractors will presumably be dealing with CUI though in the CMMC, it is described as a “transition step.”⁴²⁵
- **Level 3:** The contractor satisfies the requirements of Level 2 but must also demonstrate “good cyber hygiene.” They must also have a plan that demonstrates the management of implementation. This could include having necessary training, plans, goals, and buy-in from stakeholders.⁴²⁶ This level

includes safeguards and other practices from NIST SP 800-171, DFARS 252.204-1702, and other selected requirements.

- **Level 4:** The contractor satisfies the requirements of Level 3, but also reviews and quantifies their security practices for effectiveness. In addition, they must demonstrate a proactive approach to combating advanced persistent threats (APTs). This level includes safeguards from NIST SP 800-171, DFARS 252.204-7012, certain requirements from NIST SP 800-171B, and other practices.⁴²⁷
- **Level 5:** The contractor satisfies the requirements of Level 4 but must also optimize their safeguards implementation across the business. This level further refines the protection of CUI from APTs. This level includes safeguards from NIST SP 800-171, DFARS 252.204-7012, certain requirements from NIST SP 800-171B, and other practices.⁴²⁸

For further clarification, contractors should reference CMMC Version 1 Appendix B found at:

https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf

CMMC Domains

CMMC contains the following 17 domains. These domains contain titles that may be distinct from those found in the soon to be mentioned publications on which CMMC is based. However, these domains are detailed in CMMC Appendix A to level requirements, which are mapped mainly against the various referencing requirements noted below. The seventeen CMMC domains are:⁴²⁹

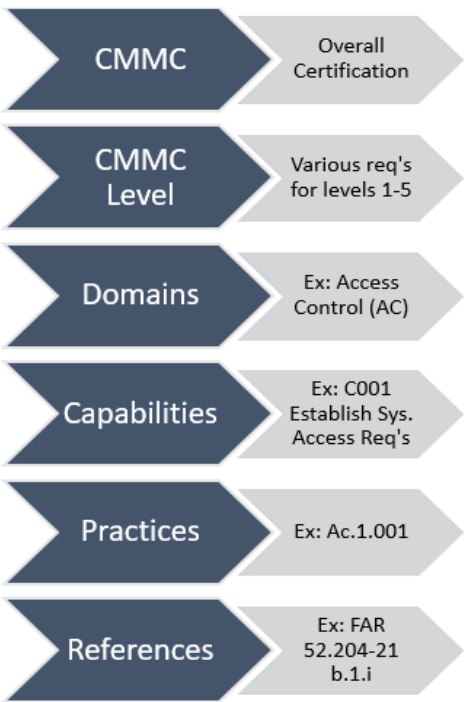
- Access Control (AC)
- Asset Management (AM)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)

- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System and Communication (SC)
- System and Information Integrity (SI)

Within the CMMC Appendices, each domain listed above is broken down into capabilities. In turn, the capability lists the required practices for each level with reference material.

As stated within CMMC, most compliance efforts at all levels originate from FAR 52.204-21 and DFARS 252.204-7012.⁴³⁰ For this reason, they will be discussed in detail below. Levels 2 through 5 also contain other compliance references. These additional references will not be mentioned below, so they should be reviewed with the necessary consulting expert and/or legal counsel.

In a hierarchy chart, the CMMC system can be displayed as the following:



FAR 52.204-21

As noted within CMMC, Level 1 encompasses the FCI basic safeguarding requirements found in (FAR) 52.204-21. Level 1 of the CMMC is, “equivalent to all of the safeguarding requirements from FAR Clause 52.204-21.”⁴³¹ Per FAR Regulation 52.204-21, the following safeguards are **mandatory** and are considered the **minimum** requirements for any business handling FCI:

- “(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

- (2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.
- (c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.”⁴³²

Naturally, complying with the above is no easy task. However, any company wishing to do business with the government – either as a prime or subcontractor – should consider CMMC Level 1; at a minimum.

NIST SP 800-171 & DFARS 252.204-1702

Within the Code of Federal Regulations, Title 48 is commonly referred to as the “Federal Acquisition Regulation” (FAR). This regulation governs the formation and administration of contracts with the federal government. Within FAR, there are more than 20 supplements, but the cybersecurity requirements within the Department of Defense FAR Supplement (DFARS) are the most important for businesses with the Department of Defense (DoD) contracts. Broadly speaking, DFARS governs most procurements made by DoD, General Services Administration (GSA), and all branches of the armed forces. CMMC Levels 2 through 5 are, variously testing the CUI security requirements found in 48 C.F.R. 252.204–7012 Safeguarding Covered Defense Information and Cyber Incident Reporting; with the addition of selected other practices.

DFARS contains the relatively new provision known as Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7012).⁴³³ If a contractor stores, processes, or transmits covered defense information, they are likely subject to the 7012 regulation. Per the DoD, covered defense information is defined as “unclassified controlled technical information (CTI) or other information as described in the CUI Registry...that requires safeguarding/dissemination controls AND IS EITHER marked or otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract; OR collected/developed/received/transmitted/used/stored by the contractor in performance of contract.”⁴³⁴

To remain compliant with DFARS 252.204-7012, businesses and their legal counsel should be aware that the regulation contains two main provisions.

The first deals with protecting covered defense information – generally synonymous with CUI – via NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Proper compliance with this framework can require significant time and resources as it covers policies, processes, secure IT configurations, and possibly additional hardware and security-related software.⁴³⁵

NIST SP 800-171 contains the following fourteen specific requirements with general explanations:

- **Access Control** – Who can view this data?
- **Awareness and Training** – Are those who can view the data trained properly?
- **Audit and Accountability** – Can the business identify and track who accesses the system?
- **Configuration Management** – Can the business establish, maintain, and enforce secure configuration requirements?
- **Identification and Authentication** – Does the business possess the ability to verify the identity of users, devices, or process prior to viewing the information?
- **Incident Response** – Does the business have a system for testing and handling incidents?
- **Maintenance** – How will routine maintenance be handled, and who is responsible?
- **Media Protection** – How does the business handle hard copy and electronic records, including backup storage?
- **Personnel Security** – Are those allowed access to information appropriately screen before access and is there access revoked upon termination?
- **Physical Protection** – Does the business limit physical access to systems and is access recorded?
- **Risk Assessment** – Are there routine vulnerability scanning and risk assessments of the organization and its systems?

- **Security Assessment** – How will the business continuously assess and improve their security controls?
- **System and Communications Protection** – Are communications monitored, controlled, and protected at crucial internal and external system boundaries?
- **System and Information Integrity** – How is the system integrity maintained and monitored for intrusions?⁴³⁶

While that may seem relatively straightforward, contractors should understand that within the fourteen requirements, there are an additional 118 total basic and derived security requirements.⁴³⁷ Previously, if the contractor wanted to vary from the standards present in NIST SP 800-171, they will need to submit a request in writing to the Contracting Officer, who will forward it for consideration to the DoD CIO.⁴³⁸ It is currently unknown if this requirement will change under CMMC.

If the contractor wants to use an external cloud provider to store, process, or transmit covered information, the business must contractually require and ensure that the cloud provider meets the security requirements listed in the Federal Risk and Authorization Management Program (FedRAMP).⁴³⁹ The cloud provider must still meet the requirements of DFARS 252.204-7012 pertaining to “cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.”⁴⁴⁰ Any IT system or service other than the cloud provider requirements are still subject to the security restrictions found in DFARS 252.204-7012,⁴⁴¹ and CMMC.⁴⁴²

The second main provision deals with the rapid reporting of cyber incidents and cooperation with the DoD.

Per the regulation, cyber incidents are “actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.”⁴⁴³ When a cyber incident is discovered, the business will review the incident in accordance with the regulatory requirements and report the incident within 72 hours.⁴⁴⁴

CMMC has a slightly different definition of a breach, stating, “An incident where an adversary has gained access to the internal network of an organization or an organizationally owned asset in a manner that breaks the organizational policy for accessing cyber assets and results in the loss of information, data, or asset. A breach usually consists of the loss of an asset due to gained access.”⁴⁴⁵

Contractors should note the particular use of the word “usually” in the above definition. With a strict interpretation of the definition, a ransomware event may require notification as information could have been accessed even if not potentially

acquired. This is a topic that contractors should clarify with their assessors, and if possible, the CMMC-AB.

Per DFARS 252.204-7012, if it is determined that malicious software was on the computer system that contributed to the incident, the business must submit the offending code to the DoD's Cyber Crime Center. From there, the DoD can decide to formally assess the damage caused by the incident. During this assessment, the business may be required to submit the media to the DoD and further aid in their evaluation.⁴⁴⁶

Failure to follow the safeguarding requirements of DFARS 252.204-7012 could result in detrimental actions against the contractor per DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information:

“A breach of these obligations or restrictions may subject the Contractor to:

- (i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States, and;
- (ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third-party beneficiary of this clause.”⁴⁴⁷

The potential for government action should not be brushed off as was common in the past. The government is increasingly taking cybersecurity more seriously than before and may investigate, with the intent to prosecute contractors who fail to adhere to their requirements. As an example, in December of 2017, the DOJ's National Security Division and the U.S. Attorney's Office for the Eastern District of Virginia investigated Netcracker Technology Corporation (NTC).⁴⁴⁸

NTC is a software engineering firm that specializes in network solutions for large corporations. Like many large software companies, NTC used both American and foreign staff to develop software.⁴⁴⁹

Through a series of contracts, NTC provided services to the DoD's Defense Information System Network (DISN). This network operates the services for the governments classified and unclassified networks. Due to a series of misunderstandings regarding contract language and requirements, it was ultimately discovered that foreign nationals without the required security clearances were performing work on the contract. Further, the NTC server was stored in Moscow, where the Russian Intelligence Services could legally monitor all network traffic, compromising the project. The contract with NTC was immediately canceled, and their work product was removed from DISN.⁴⁵⁰

NTC was subsequently investigated by the DOJ's National Security Division and the U.S. Attorney's Office for the Eastern District of Virginia. NTC denied that it had engaged in any wrongdoing but agreed to comply with an Enhanced Security

Plan (ESP), likely to avoid criminal prosecution.⁴⁵¹ The agreement includes both three-year and seven-year provisions.⁴⁵²

Within the three-year provision, NTC must seek the “non-objection” of the investigation government bodies before bidding on any new local, state, or federal contracts as the prime contractor, or as a sub-contractor. The seven-year provision includes retaining a third-party auditor to assess NTC’s adherence with the ESP, and annual reports on NTC’s adherence with the ESP. Among numerous other provisions, the agreement includes a \$35 million fine to be paid to the United States Treasury if it is determined that NTC has failed in their responsibilities to uphold their promises as set forth in the plan.⁴⁵³

Draft NIST SP 800-171B Requirements -CMMC Levels 4 & 5

Of note, NIST SP 800-171B is not a new standard, per se, but merely a supplement to the previously noted NIST 800-171. The purpose of the supplement is to protect CUI from advanced persistent threats (APTs).⁴⁵⁴ Some or all of the approximately 32 requirements found in NIST SP 800-171N may be contractually required – via the CMMC – to be implemented in addition to the basic and derived requirements found in NIST SP 800-171.⁴⁵⁵

It is not unreasonable to assume that implementing enhanced security controls will be costly. According to the NIST report on the estimated cost of implementing NIST SP 800-171B, compliance could easily exceed \$10M for a company with 25-50 endpoint networks.⁴⁵⁶ For interested parties, the DoD cost estimate for NIST SP 800-171B implementation can be found for free at:

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf>

Perhaps more interesting than the cost analysis found in the above document is the estimated number of affected contractors that will require NIST SP 800-171B implementation. Per the analysis, “We estimate that 69,000 contractors have controlled unclassified data. However, less than one half of 1% of DoD contractors develop critical capabilities for DoD.”⁴⁵⁷ Although there have been no official pronouncements yet on the number of contractors requiring Level 4 or 5 compliance, this would point to only less than 400 companies nationwide.

Other Referenced Requirements

As stated previously, the majority of CMMC is based upon FAR 52.204-21 and DFARS 252.204-7012.⁴⁵⁸ However, there are additional references found in the appendices that will require investigation by contractors should they be deemed necessary or mandatory. These include, but are not limited to, CERT RMM v1.2, CIS Controls v7.1, NIST SP 800-53, UK NCSC Cyber Essentials, ACSC Essential Eight Maturity Model, DOE's C2M2, NIST SP 800-39, NIST CSF V1.1, and FIPS PUBs 199, 201, and 197. While important, these publications will not be detailed here, as doing so would prove too lengthy. Any contractor who is interested in these references should seek qualified compliance experts and/or legal counsel.

CMMC Certifications and Compliance

In January 2020, the CMMC-AB (Accreditation Board) was formally incorporated. As of this publication, there are no licensed CMMC assessors who can issue a certification. The CMMC-AB is still waiting on several issues to be resolved before assessors can be trained. Directly from the CMMC-AB website, "The CMMC Standard is not yet finalized, and no Assessors or C3PAOs are formally accredited or certified by the CMMC-AB. Therefore, it is currently inappropriate for any Assessor or C3PAO to claim to provide formal CMMC assessments that will meet the requirements for a DoD contract."⁴⁵⁹

This does not mean that businesses should neglect preparation until assessors are available. With hundreds of thousands of potential contractors that will require certification in short order, there could be a serious lack of assessor for the foreseeable future. Any business that could work with the DoD should consider a good faith internal assessment considering their perceived future requirements.

For smaller contractors, or those with smaller cybersecurity budgets, there is hope when considering the costs associated with CMMC Compliance. According to Katie Arrington, the special assistant to the Assistant Secretary of Defense for Acquisition for Cyber in the Office of the Under Secretary of Acquisition and Sustainment in DoD, "security is an allowable cost."⁴⁶⁰ However, she also noted that eventually, certification requirements will be placed in contracts and will be used as a "go or no-go decision."⁴⁶¹ Contractors are thus highly encouraged to begin working towards their applicable certification level as soon as possible.

Additional Legal Concerns

Beyond failing to secure new contracts or falling victim to a cyber-attack and losing critical national defense information, businesses must remain vigilant of the

cybersecurity claims they make to the government. Consider the allegations found in the case of *United States v. Aerojet Rocketdyne Holdings, Inc.*, where the U.S. District Court for the Eastern District of California held that an alleged failure to adhere to government contracting cybersecurity requirements.⁴⁶²

In this case, the relator, Brian Markus, worked for Aerojet as the senior director of Cyber Security, Compliance, and Controls for approximately 15 months.⁴⁶³

The defendants, Aerojet Rocketdyne Holdings, Inc., and Aerojet Rocketdyne, Inc. (hereafter referred to as “Aerojet”) develop and manufacture products for both the aerospace and defense industries. Through the course of business, it was alleged that Aerojet dealt with contracts that required compliance with DFARS 252.204-7012 as well as 48 C.F.R. § 1852.204-76 – NASA’s functional equivalent to DFARS 252.204-7012.⁴⁶⁴

Markus alleged that Aerojet fraudulently misrepresented their compliance with the minimum required cybersecurity standards as required by the contracts. He further alleged that Aerojet knew they were not compliant with the requisite standards after a third-party compliance audit. Nonetheless, Markus alleged that Aerojet nonetheless continued to misrepresent their compliance status when communicating with government officials. Markus alleged that these misrepresentations led to Aerojet receiving a government contract.⁴⁶⁵

Among other causes of action, Markus filed a False Claims Act (FCA). Based on Markus’s claims on this count, the court held that he, “plausibly pled that defendants’ alleged failure to fully disclose its noncompliance was material to the government’s decision to enter into and pay on the relevant contracts.”⁴⁶⁶

Understanding these rulings, contractors should keep a close eye on their cybersecurity compliance requirements lest they find themselves subject to similar claims. Adequate adherence will likely require constant vigilance *between* CMMC certifications.

Action Items:

- ☐ Determine if your business must comply with CMMC; and if so, which applicable parts;
- ☐ Consider seeking legal counsel to assist your business with compliance;
- ☐ Visit the CUI categories: <https://www.archives.gov/cui/registry/category-list>;
- ☐ Visit the CMMC Accreditation Board website at: <https://www.cmmcab.org/>;

- NIST SP 800-171 (Rev. 1) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations can be found at: <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>;
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* will provide more detail on the controls mentioned in NIST SP 800-71 (Rev. 1), and can be found at: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>;
- Draft NIST SP 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets can be found at: <https://csrc.nist.gov/publications/detail/sp/800-171b/draft>;
- FedRAMP can be found at: <https://www.fedramp.gov/resources/documents/>.

Healthcare: HIPAA/HITECH

The Health Insurance Portability and Accountability Act (HIPAA) and its partial update via the Health Information Technology for Economic and Clinical Health Act (HITECH Act), are quite expansive. Indeed, these laws alone could, and do, comprise entire books dedicated to their nuances. For the purposes of cybersecurity law and its implications on cyber insurance, two specific provisions will be addressed here: The Privacy Rule, and the Security Rule.

Generally speaking, HIPAA applies to “Covered Entities.” As defined by HHS, the following are considered covered entities:

- Health care providers which includes providers like doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies if they are transmitting PHI in an electronic form;
- Health plans, including health insurance companies, HMOs, company health plans, and various government health programs such as Medicare or Medicaid;
- Health care clearinghouses which process nonstandard health information they have received from a different entity.⁴⁶⁷

The addition of HITECH greatly expanded the reach of HIPAA by adding a new class of entity referred to as a “Business Associate” (BA). A business associate is a person or organization that performs services which require the covered entity to disclose PHI to that organization. This could include claims processing, billing, legal, or accounting services, among others. The HIPAA Administrative Simplification Regulation Text defines a business associate as the following:

8. (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information;
9. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity;
10. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.⁴⁶⁸

Any subcontractor, or subcontractor of a subcontractor and so forth, that creates, receives, transmits, or maintains PHI on behalf of a BA, is automatically considered

a BA in their own right.⁴⁶⁹ For example, if an accounting firm is auditing various aspects of BA which discloses the PHI of individuals – even without a formal BA agreement (BAA) – the accounting firm may automatically be deemed a BA under HIPAA and must adhere to all applicable laws and safeguards.

Specifically excluded are the following:

- (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual;
- (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met;
- (iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law;
- (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.⁴⁷⁰

Data to be protected under HIPAA/HITECH includes information quite like information considered PII in the various state and territory breach notification law. Generally, such information is referred to as Protected Health Information (PHI).

As stated in the regulation, PHI means:

[I]ndividually identifiable health information:

- (i) Transmitted by electronic media;
- (ii) Maintained in electronic media, or;
- (iii) Transmitted or maintained in any other form or medium.⁴⁷¹

This is a very broad definition, and could include, but is not limited to: fingerprints, voiceprints, photographs, X-rays, Social Security number, name, address, employer's name, medical record number, account number, health plan number, and more.⁴⁷²

Information excluded from being considered PHI is stated as follows in the regulation:

[I]ndividually identifiable health information:

- (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
- (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
- (iii) In employment records held by a covered entity in its role as employer, and;
- (iv) Regarding a person who has been deceased for more than 50 years.⁴⁷³

Antipodal to PHI is the term “De-identified Health Information.” This is an altered type of information that does not allow for the identification of the person. There are very specific elements required to de-identified information under the privacy rule, but they can be summarized by two primary methods.⁴⁷⁴ Either a qualified statistician can make a formal determination, or specific identifiers can be removed.⁴⁷⁵

Unbeknownst to many accounting businesses, they may be considered a business associate handling PHI. Referencing the above, businesses can be business associates by definition, not necessarily solely through a contract, though a contract may be necessary. Services, where a business may fall under these rules, could include providing an audit of internal controls, basic bookkeeping and accounting services, consulting services, and litigation support.⁴⁷⁶ Indeed, the HHS lists CPA firms, third party administrators, attorneys, utilization review consultants, health care clearinghouses, medical transcriptionists, and pharmacy benefits managers as examples of business associates on their website.⁴⁷⁷ If a business believes that they are currently – or could be construed as – a business associate, they should seek further guidance from competent legal counsel familiar with their particular circumstance.

Privacy Rule:

The Privacy Rule is the portion of HIPPA, which, unsurprisingly, deals with privacy and confidentiality of PHI – also known as “individually identifiable health information” (IIHI). The rule provides federal-level protections but does not supersede any other federal, state, or local law that would require greater protections on PHI. Covered Entities (CEs) must comply fully with the Privacy Rule. Business Associates (BAs) must only comply with certain sections of the rule.

As a reminder, HIPAA defines CE to include:

- Health plans;
- Health clearinghouses;
- Health care providers that transmit health information in electronic form for transactions.⁴⁷⁸

For Covered Entities (CEs), the Privacy Rule has the following four major components:

11. A CE must notify individuals of their privacy rights and how the individual's information can be used. Generally, this is accomplished with a notice of privacy practices (NPP). The NPP should detail how the CE will use and disclose PHI, the legal duties and privacy practices borne by the CE, and the individual's rights regarding PHI – such as a restriction of disclosure in certain circumstances.⁴⁷⁹
12. Each CE must adopt and implement certain privacy procedures. These privacy procedures should minimize the request, disclosure, and amount of PHI in use.⁴⁸⁰
13. The CE shall train their employees to understand mandatory privacy procedures.⁴⁸¹
14. An individual at each CE shall be designated as being responsible for ensuring that privacy procedures are followed and implemented. These tasks will be accomplished with a Privacy and Security Officer.⁴⁸² In addition, the privacy officer must create policies and procedures for persons to submit complaints regarding the CE's HIPAA compliance with a specified person.⁴⁸³

The Privacy Rule states that Business Associates are directly and/or contractually liable for any use or disclosure of PHI that is not allowed under the Privacy Rule, or as further dictated by its Business Associate Agreement (BAA). BAs may also be liable for various other shortcomings such as a failure to limit the disclosure and use of PHI or to fail in providing breach notifications to the CEs. Finally, violations of HIPAA will subject BAs to the same civil and criminal penalties as those experienced by CEs.⁴⁸⁴

The penalties for violating the Privacy Rule are significant. The penalty amounts can range from \$100 to \$50,000 or more per violation. The calendar year cap for violations is \$1,500,000.⁴⁸⁵ As such, businesses should be well acquainted with all obligations they may have regarding the Privacy Rule.

Security Rule:

The security rule is perhaps the most important HIPAA rule regarding cybersecurity as its goal is to protect the confidentiality of PHI in electronic form (ePHI). The Security Rule applies to ePHI while it is being transmitted, stored, or maintained. The provisions of this rule are generally mandatory to both CEs and BAs unless otherwise specified.

Broadly speaking, the Security Rule mandates several essential functions; such as:

- Keeping ePHI secure at all times;
- Ensuring that their workforce is complying with the rule;
- Protecting against unauthorized disclosures of ePHI from reasonably anticipated threats or errors.⁴⁸⁶

To accomplish these goals, the Security Rule has three organizational levels of safeguards. The three organizational levels of safeguards are Administrative safeguards, Physical safeguards, and Technical safeguards. Each safeguard is comprised of “standards.” In turn, some of those standards may be broken into further, “implementation specifications” to provide a more detailed explanation of implementing a standard.

Administrative Safeguards

Administrative safeguards comprise many safeguards that must be implemented. The administrative safeguards include:

- A security management process that implements policies and procedures which will “prevent, detect, contain, and correct security violations.” This will include specific implementation of risk analysis, risk management, sanction policy, and information system activity review;
- An assigned security official who is responsible for the requirements of the administrative safeguards;
- Policies and procedures regarding the access of ePHI by appropriate staff members, as well as the denial of access for those staff not cleared to view ePHI. Specific implementations include authorization and supervision, clearance procedures, and termination procedures;

- The implementation of policies and procedures regarding the access of ePHI including the isolation of health care clearinghouse functions, access authorization, and initiation and modification of access;
- Mandatory security awareness training to include security reminders, protection for malware, log-in monitoring, and password management;
- Security incident procedures to deal with various types of incidents;
- Contingency plans for dealing with emergencies such as system failures or natural disasters. This would specifically include data backup plans, disaster recovery plans, as well as the testing and updating the plan;
- A periodic evaluation – both technical and non-technical – to test the entity’s compliance with the various administrative safeguards;
- Business associate contracts and other arrangements to ensure that BAs safeguard ePHI appropriately.⁴⁸⁷

To evidence that entities are adhering to the administrative safeguards appropriately, each entity must adhere to certain documentation requirements. This includes a six-year document retention policy, a review of those documents to ensure confidentiality, and updates to those documents as threats evolve or arise.⁴⁸⁸

Physical Safeguards

Physical safeguards are designed to protect a business’s computer system and ePHI from unauthorized physical access. Within the physical safeguards rule, there are three primary standards:

- Facility access controls that limit the physical access of information systems to only those people who are authorized access. This includes contingency operations, facility security plan, access control and validation procedures, and maintenance records;⁴⁸⁹
- Workstation use and security, including the appropriate functions to be performed at those workstations, how those functions will be performed, and the physical environment of those workstations that have access to ePHI.⁴⁹⁰ Per a recent HHS sub-regulatory guidance, this also includes portable electronic devices such as laptops, tablets, and smartphones;⁴⁹¹
- Device and media controls which concern the accountability, receipt, storage, back-up, and disposal of hardware and electronic media in and out of the facility;⁴⁹² In recent newsletter guidance from the HHS, they identified

numerous questions that entities should consider when developing device and media controls. These questions include whether the entity has a record that tracks the media and devices through their entire lifecycle and whether workplace members, including management, are appropriately trained on the safeguarding of ePHI.⁴⁹³

Technical Safeguards

Any information system that contains ePHI requires entities to develop and implement technical policies and procedures to safeguard that data. While the regulations are technology- and vendor-neutral, they require entities to implement those safeguards which are reasonable and appropriate for their organization. More specifically, technical safeguards include the following five standards:

- Entities must develop and implement access controls for any information system that contains ePHI. This will include unique user identification and emergency access procedures for obtaining ePHI during an emergency. In addition, this may include automatic logoffs and encryption/decryption of ePHI.⁴⁹⁴
- At their discretion, and consistent with internal risk analyses, entities may implement hardware, software, and procedural mechanisms to examine and record the activity on their systems that contain ePHI.⁴⁹⁵
- Entities must develop and implement policies and procedures to protect the integrity of ePHI from any improper destruction or alteration.⁴⁹⁶ This may be accomplished by electronic means.⁴⁹⁷
- Entities must implement policies and procedures to verify that anyone seeking access to ePHI is authentic and authorized to do so.⁴⁹⁸
- When ePHI is being transmitted over an electronic network, entities will ensure that the information is guarded from unauthorized access.⁴⁹⁹ This may be accomplished with integrity controls or encryption.⁵⁰⁰

Policies, Procedures, and Documentation Requirements

In addition to complying with the Security Rule, entities must also comply with various document retention policies and procedures. Entities shall:

- Retain documents required by this rule for six years from their creation, or the date of when they were last in effect, whichever is longer;

- Make those documents available to any individual who is responsible for implementing the required procedures;
- Maintain a record of actions, activities, or assessments that are required to be documented by the rule;
- Periodically review and update the documents as operational or environmental factors change the security of ePHI to ensure their confidentiality and security.⁵⁰¹

Breach Notification Rules

Per HIPAA, a Breach means “the acquisition, access, use, or disclosure of protected health information in a manner not permitted...which compromises the security or privacy of the protected health information.”⁵⁰²

Any PHI that is accessed, used, or disclosed is presumed to be a breach. This is unless the CE or BA can successfully demonstrate via risk assessment that there is a low probability of misuse based upon at least the following four factors:

- The nature and extent of the PHI involved and the likelihood of re-identification;
- The unauthorized person to whom the disclosure was made, or who used the PHI;
- Whether PHI was viewed or acquired;
- The extent to which any risks to the PHI have been mitigated.

As a warning, many breach notifications by a CE will result in an enforcement investigation. These investigations often result in a CE or BA making large payments to the government as well as acquiescing to a corrective action plan (CAP).⁵⁰³ These plans can be lengthy and burdensome, so all efforts should be made by CEs and BAs to ensure strict compliance with the law.

Furthermore, breach notifications involving PHI are consistently the most expensive on a per-record basis.⁵⁰⁴ While CEs are required to provide notice to affected individuals, those responsibilities may delegate that responsibility to a BA.⁵⁰⁵ For any business serving as a BA, such notices could prove financially burdensome and will have serious implications on prudent limits available under their cyber insurance policy. Businesses should seek legal counsel to assist in reviewing their BAA to determine if they are liable for breach notifications to individuals, or liable to reimburse the CE for breach notification costs.

Business Associate Agreements and Cloud Computing

HIPAA requires that CEs obtain contractual assurances from BAs that they will adhere to all applicable security issues. Broadly speaking, the statute requires the following two implementation specifications:

- BA contracts must provide that the BA will comply with applicable HIPAA security standards for protecting ePHI. Any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the BA must agree to comply with the HIPAA security standards via their own contract. BAs must report any security incident to the CE immediately.
- BA contracts with their own subcontractors will apply the same standards as stated between CEs and BAs.⁵⁰⁶

As cloud computing becomes more prevalent, these implementation specifications could pose additional risks to CEs and businesses acting as BAs. Recently, HHS released guidance on complying with HIPAA when entities utilize cloud service providers (CSPs). Most notably, HHS stated, “[w]hen a covered entity engages the services of a CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate [underline added] under HIPAA. Furthermore, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate [underline added]. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data. Lacking an encryption key does not [underline added] exempt a CSP from business associate status and obligations under the HIPAA Rules. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules.”⁵⁰⁷

As such, CSPs that are business associates are still responsible for implementing appropriate controls under the Security Rule. HHS states that the CSP and its customer – in this case, a BA or CE – should confirm how each party will address their Security Rule requirements. For businesses that have control over which security features are present at the CSP, HHS warns that OCR will consider any shortcomings in these choices in their investigation of the CSP and/or the business. In addition, the BA and CSP must ensure that both parties are still staying compliant with the Privacy Rule.⁵⁰⁸

Therefore, if a business is currently, or could be considered a BA under HIPAA, they should consider whether their CSP is HIPAA compliant. This would likely avoid many of the potential pitfalls inherent with such a complex set of rules and regulations. OCR, as a matter of policy, does not endorse, recommend, or certify any CSPs.⁵⁰⁹ Businesses should engage legal counsel when selecting and reviewing contract language of CSPs.

Action Items:

- ☐ Determine if your business is, or could reasonably be construed as, a CE or BA under HIPAA/HITECH;
- ☐ Determine if the business has entered into any CE or BA agreements;
- ☐ Determine if the business's CSP is compliant, as applicable;
- ☐ Continuously monitor applicable breach notification laws for any changes;
- ☐ Check that your business is adequately protecting all covered data appropriately;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Determine which, if any, of the business's insurance policies would cover a claim regarding failures of the Privacy or Security Rules.

Notable OCR Enforcement Action Examples

Business Associate Enforcement

In April of 2017, the U.S. Department of Health and Human Services (HHS) took a public position with CEs on how seriously it takes Business Associate Agreements (BAAs).

Earlier in 2015, the HHS Office of Civil Rights (OCR) had begun a compliance review of the CE, The Center for Children's Digestive Health. This came after OCR had initiated an investigation of a BA which was storing inactive medical records for the center. Of concern to OCR was that the CE began providing PHI to BA in 2003, but neither party had been able to produce a signed BAA.⁵¹⁰

Through its investigation, OCR determined various deficiencies. Foremost, the CE failed to obtain necessary assurances from the BA, via the written agreement, that the BA would safeguard the PHI as required by law. As such, the CE unlawfully disclosed the PHI of thousands of individuals to the BA, potentially violating the Privacy Rule.⁵¹¹

In addition to a \$31,000 payment, the CE was required to carry out an extensive corrective action plan (CAP) that focused on numerous compliance requirements. These requirements included sending all policies and procedures to HHS for review and approval, collecting signed compliance certifications from all its staff, maintaining BAA documentation for six years after contract termination, and disclosing various BAA information to HHS.⁵¹²

Enforcement Actions Against Business Associates

In what was the first enforcement action by HIPAA regulators against a BA, federal regulators have put all business associates on notice.

In February of 2014, six nursing homes separately sent notifications to the HHS OCR regarding a breach of unsecured ePHI. Two months later, OCR notified the Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) of an investigation regarding its compliance with HIPAA rules. CHCS was a nonprofit that provided management and information technology services and was the sole corporate parent, of the six nursing homes.⁵¹³

In its findings, the OCR alleged that the CHCS failed to adhere to the HIPAA Security Rule with the following actions:

- CHCS failed to assess potential risks and vulnerabilities to ePHI.

- CHCS failed to implement security measures necessary to reduce risks and vulnerabilities as required.⁵¹⁴

In addition to a \$650,000 Resolution Amount, CHCS agreed to an extensive Corrective Action Plan (CAP).⁵¹⁵

Cloud Providers as HIPAA Business Associates

In 2016, HHS surprised many when it argued that at least some cloud providers could be considered business associates. Before this ruling, cloud providers had successfully argued that they fell within the “conduit exception” of HIPAA’s business associate status. Later that year, HHS clarified its position on CSPs as BAs with a FAQ guidance.⁵¹⁶

Problems began in 2013 when HHS received a breach notification from Oregon Health & Science University (OHSU), deemed to be a covered entity under HIPAA. That breach centered around a stolen laptop containing unsecured ePHI. Later that year, OHSU notified HHS of another breach involving unauthorized access of ePHI at a CSP without a required business associate agreement.⁵¹⁷

Subsequently, HHS’s OCR investigated the matters and acknowledged that OHSU had implemented policies and procedures compliant with most HIPAA rules. However, it had erred in disclosing ePHI to the CSP without BAA, resulting in a breach of over 3,000 individuals. In addition, OHSU violated HIPAA by not obtaining a BAA with the CSP, and among other violations, failed to implement the necessary policies and procedures to address security violations and incidents.⁵¹⁸

Per the HHS Resolution Agreement, OHSU agreed to pay a \$2,700,000 resolution amount (fine) and comply with a corrective action plan (CAP).⁵¹⁹

HIPAA May Enforce Actions Against Defunct Companies.

HHS has signaled that even out-of-business associates will be liable for improper retention and disposal of PHI in accordance with the Privacy Rule.

In 2015 HHS’s OCR fielded an anonymous complaint that a “dumpster diver” had attempted to exchange medical records for cash at a shredding and recycling facility. Following an investigation, OCR determined that FileFax, an out-of-business BA, had either left PHI in an unlocked truck in their parking lot or allowed an individual to remove the PHI from the FileFax facility who disposed of it in an unsecured location.⁵²⁰

Regardless of the cause, the court-appointed receiver for FileFax agreed to a \$100,000 resolution amount. The receiver also agreed to a CAP, which among

numerous other provisions, mandated appropriate disposal of the remaining records containing PHI in accordance with HIPAA standards.⁵²¹

Considering this resolution agreement, HHS is taking document security seriously. Any firm with access to medical records should ensure that they are properly maintained, secured, and destroyed. If OCR is willing to pursue action against a bankrupt company for a relatively small infraction, they will certainly pursue an operating business.

Cyber-Attacks Can Result in Significant Settlements

Potentially unavoidable cyber-attacks will not deter HHS from investigations and penalties. Consider the allegation found with *In re Anthem, Inc.*

In 2015, Anthem, an American health insurance company, filed a breach report with HHS after discovering that unauthorized individuals had gained access to their IT systems. This was accomplished via an undetected and continuous cyber-attack. Anthem later discovered that the attackers had infiltrated their computer system through a spear-phishing email after at least one employee had responded to the email. A subsequent OCR investigation revealed that the attackers had stolen the ePHI of nearly 79 million people, including names, social security numbers, medical identification numbers, and dates of birth.⁵²²

Numerous potential violations of the Privacy Rule and Security Rule were noted, including Anthem's failure to:

- Conduct an accurate and thorough risk analysis of risks to ePHI;
- Implement procedures to regularly review IT system activity records;
- Identify and address detections of the incident which lead to the breach;
- Implement adequate technical policies and procedures to ensure that only authorized persons had access to ePHI.⁵²³

As a result, Anthem agreed to a record-setting \$16 million settlement with HHS, including a comprehensive corrective action plan (CAP).⁵²⁴

The OCR Director noted, "The largest health data breach in U.S. history fully merits the largest HIPAA settlement in history[.] Unfortunately, Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information. We know that large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by OCR."⁵²⁵

State Attorneys General May Also Enforce HIPAA violations

In 2015, the Indiana attorney general reminded entities who must remain compliant with HIPAA that the states may sometimes action. Such was seen in *State of Indiana v. Joseph Beck, Beck Family Dentistry*.

In 2013, then dentist Joseph Beck had hired a data company to securely destroy paper records of his former patients. In an investigation by a local news station, it was alleged that 63 boxes, comprising over 7,000 files, of former patients were discovered in a dumpster. The new station alleged that it discovered names, addresses, social security numbers, credit card numbers, and other health information in the files.

Beck subsequently entered into a consent order with the Indiana attorney general. As part of the order, Beck was fined \$12,000 and agreed to a CAP.⁵²⁶ Indiana joins the ranks of numerous other states which have recently enforced actions against those they believe have violated HIPAA.⁵²⁷

From this, businesses should take away two main points. First, small entities are not immune to HIPAA-related enforcement actions. Second, electronic disclosures may gain nationwide attention, but physical documents still require care in accordance with HIPAA mandates.

Private Rights of Action

While several patients have filed private lawsuits involving HIPAA violations, none so far appear to be successful. Also, HIPAA contains no explicit private right of action. As a federal law, HIPAA both explicitly and implicitly preempts state laws that are contrary to HIPAA – except in a case where a state’s law is more rigorous than HIPAA regarding privacy protection.

An illustrative case of courts generally refusing to extend a private right of action can be found in the case of *Hope Lee-Thomas v. Labcorp*.

Lee-Thomas was a hospital patient who was allegedly instructed to submit her medical information on a computer near a separate intake station. She asserted that her health information was visible to another patient who was using the separate intake station. Upon discovery of this alleged violation, she informed the lab technician and took a photograph of the two stations.⁵²⁸

Early the following month, Lee-Thomas sent a letter to the hospital informing them of a possible HIPAA privacy violation. She then registered a complaint with the Department of Health and Human Services Office of Civil Rights (OCR).⁵²⁹ While both complaints were denied by their respective oversight agencies, the

District of Columbia informed Lee-Thomas of her right to bring a private action before the D.C. Superior Court.⁵³⁰

When bringing her action in front of the D.C. Superior Court, Lee-Thomas's sole complaint rested with her assertion that the computer station violated HIPAA's privacy protections. Though she filed her lawsuit *pro se* (on her own behalf and without formal legal representation), and thus was subject to a "less stringent standard than formal pleadings," she was unsuccessful.⁵³¹

The court dismissed her claim because HIPAA provides no private cause of action. After this definitive statement, the court wrote in length, referencing numerous cases which have reached the same conclusion.⁵³²

While HIPAA does provide civil and criminal penalties for improperly disclosed or handled information, the statute specifically entrusts those actions with HHS and each state's attorney general.⁵³³ Businesses can rest a little easier knowing that individual plaintiffs will likely be unsuccessful with individual actions.

Action Items:

- ☐ Determine if your business has insurance which would respond to the various enforcement action types listed previously;
- ☐ Work with legal counsel to ensure continued compliance as HHS may change policy at any time;
- ☐ Update your business's incident response policy as necessary.

Damage Control

HIPAA Audit Program

Businesses acting as BAs may be curious as to how they could be subject to an investigation by HHS's OCR.

The most direct method would be a party notifying HHS of a complaint involving HIPAA. Under HIPAA, HHS has the authority to conduct compliance reviews and engage in investigations where there has been an alleged violation of any rules therein. Namely, this would include alleged violation of the Privacy, Security, and Breach Notification Rules.

However, there is a separate program whereby OCR will investigate compliance and implementation of HIPAA standards without an alleged violation.

In 2016, OCR implemented its Phase 2 HIPAA Audit Program. This program is designed to “review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.”⁵³⁴

The audit program is focused on evaluating the compliance of randomly selected businesses that are not currently facing an open investigation or undergoing a compliance review. OCR has indicated that they will be instructing CEs to list and identify their BAs with included contact information. They will use both desk and on-site audits.⁵³⁵

HHS has indicated that these audits are intended primarily as a “compliance improvement activity.” However, if the audit report prepared by OCR brings to light a serious compliance issue, they may begin a compliance review.⁵³⁶

Action Items:

- ☐ Work with legal counsel to ensure that, if applicable, your business is ready for a HIPAA audit.

Educational Institutions: The Family Educational Rights and Privacy Act (FERPA)

Schools – to include primary schools through schools of higher education – are particularly susceptible to data breaches. By their very nature, schools will contain vast amounts of sensitive information accessible to many users in various security and network configurations. Ironically, many of these same schools will also be in the business of teaching their students programming and cybersecurity skills, which can be used in a malicious manner if inappropriately applied. Whether the threats are internal or external, malicious or benign, the danger to a data breach is very real.

Unfortunately for schools, there is no one overriding cybersecurity law that governs their activities. Far from being comprised of only traditional classrooms, schools may also control medical centers, research laboratories, eating facilities, and financial loan centers. This means that schools could fall under a litany of various laws that govern their behaviors and mandate various responses. For any school considering these requirements, the first logical starting point is The Family Educational Rights and Privacy Act (FERPA)

FERPA was enacted in 1974 to both guarantee access to, and provide protection for, student records.⁵³⁷ In general, FERPA applies to any public, private, state, or local school, if they are receiving federal education funds.⁵³⁸ This includes elementary, secondary, and higher education institutions.

FERPA is voluminous, confusing, and at times, utterly silent on issues relevant to the modern student.⁵³⁹ Pertinent to the discussion of cyber insurance, cybersecurity, and cybersecurity law, the following three provisions are of note:

- In general, schools are not permitted to release education records, or PII contained in those records, to any third party without the prior written consent of the adult student, or their parents in the case of a minor.⁵⁴⁰
- Adult students or parents may seek an internal and informal hearing if they believe that their records are inaccurate or there has been an invasion of privacy.⁵⁴¹
- Schools must provide adult students or parents with a notice of their rights under FERPA.⁵⁴²

What is a record under FERPA?

FERPA has three different but somewhat related categories of protected information:

- Education Records
- Personally Identifiable Information (PII)
- Directory Information

Particular to this discussion, PII includes a litany of information that is not necessarily included in the previously noted state and territory breach notification statutes.

“The term includes, but is not limited to...

- a. The student's name;
- b. The name of the student's parent or other family members;
- c. The address of the student or student's family;
- d. A personal identifier, such as the student's social security number, student number, or biometric record;
- e. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- f. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- g. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.”⁵⁴³

As recently late as 2017, the Government Accounting Office (GAO) issued a report which raised concerns over the effectiveness of schools protecting student aid information.⁵⁴⁴ Combined with an extensive list of information requiring protection, and the ever-increasing list of cybersecurity events occurring at educational institutions,⁵⁴⁵ it would be logical to assume that federal authorities have enacted mandatory cybersecurity legislation for those entities covered under the authority FERPA to combat this threat. Yet, little progress has been made on this front.

As far as FERPA is concerned, the only official security requirements are as follows: “An educational agency or institution **must use reasonable methods** to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement...”⁵⁴⁶

FERPA and Cloud Computing

Regarding cloud computing requirements, FERPA guidance is relatively sparse. The only section applicable notes that if a school discloses information to a third party, that party must “not disclose the information to any other party without the prior consent of the parent or eligible student.”⁵⁴⁷

At issue is the school’s control over any data turned over to the third party. Here, FERPA only stipulates that the school must exert, “direct control” over the third party, but does not mention any specific cybersecurity standards from the third party.⁵⁴⁸

Protection of Pupil Rights Amendment (PPRA)

Another privacy law that may apply to a school is the Protection of Pupil Rights Amendment (PPRA). PPRA is primarily concerned with protecting student privacy in three areas. These are:

1. Restricting the participation of students in surveys, analysis, or evaluations without the prior consent of the parent or adult student.⁵⁴⁹
2. Restricting the use and collection of students PII for marketing purposes.⁵⁵⁰
3. Providing for rights regarding the administration of physical examinations to minors.⁵⁵¹

FERPA Enforcement

The enforcement arm of FERPA/PPRA resides in the Family Policy Compliance Office (FPCO). FPCO is tasked with receiving and investigating FERPA complaints, determining penalties for violations, and promulgating FERPA regulations.⁵⁵²

Revocation of funding is the primary penalty for institutions that fail to meet FERPA requirements. In addition, the Secretary of the Department of Education can also compel compliance by way of cease and desist orders, or through the termination of eligibility to receive funds for a program. Within the statute, there are other penalties for violations committed by third parties. For those third parties which improperly disclose student PII, or fail to provide appropriate notification, they may be banned from access to PII from education records for five years.⁵⁵³

Notice that none of the above approves for a private right of action under FERPA.

In the 2020 case of *Gonzaga University v. Doe*, the defendant had previously been awarded over \$1 million by lower courts for the release of personal information to an “unauthorized person.”⁵⁵⁴ Ultimately the case reached the U.S. Supreme Court.

There, Chief Justice Rehnquist delivered the opinion of the Court.

In part, he noted, “there is no question that FERPA's nondisclosure provisions fail to confer enforceable rights. To begin with, the provisions entirely lack the sort of “rights-creating” language critical to showing the requisite congressional intent to create new rights.”⁵⁵⁵

He continued, stating, “[I]f Congress wishes to create new rights enforceable under § 1983, it must do so in clear and unambiguous terms—no less and no more than what is required for Congress to create new rights enforceable under an implied private right of action.”⁵⁵⁶

Therefore, should a data breach occur, it is unlikely that an individual could bring a claim under FERPA. This is not to say that FERPA should be treated without due care.

In the recent case of *United States v. Miami University*, the U.S. government, on behalf of the Department of Education (DOE), brought an action against the university for allegations of violating FERPA. The main thrust of the action was for the government to establish that disciplinary records are “education records” with the context of FERPA.⁵⁵⁷

State Student Privacy Laws

Not content with FERPA, most states have explicitly or implicitly enacted a series of laws that deal with educational information and students' PII. Many have adopted FERPA-like principles into their own statutes, while others have adopted FERPA with various limitations. Perhaps the most robust state laws were enacted in California's Students Online Personal Information Protection Act (SOPIPA)⁵⁵⁸ and their Early Learning Personal Information Protection Act (ELPIPA).⁵⁵⁹

Due to the highly complex patchwork of state laws in this area, some of which may preempt other state law, schools researching this topic are highly encouraged to consult competent legal counsel familiar these provisions for further guidance.

State Law Issues

Schools should also consider the various data breach state law requirements – covered previously in this book – following a breach. The preponderance of states contain provisions that could require notification by any business type – to include schools – that suffers from breach of personal information.⁵⁶⁰

As most institutions of higher education will have students from every state and territory, it is entirely feasible that breach notification may be required for at least most of the records held. Even if a school is not legally liable to provide notification, consideration should be given to voluntary notification to mitigate damage to the school's brand among past, present, and future students.

Consider the following allegations in the case of *Roberts v. Maricopa County Community College District*.

In April of 2013, the Maricopa County Community College District was notified by the FBI that they had been subjected to a large data breach. This exposed the personal and academic data of roughly 2.4 million current and former students, vendors, and employees. Although the breach was said to have occurred in April, it was not until November – seven months later – that students were notified. The compromised information included employee social security numbers, bank account information, driver’s license numbers, and student academic details.⁵⁶¹

Following notification, the District faced a class action complaint brought by victims of the breach. The class alleged negligence, negligence *per se* under two Arizona state-specific statutes, breach of fiduciary duty, bailment, breach of the right of privacy under the Arizona state constitution, and the violation of a federal statute for the unlawful disclosure of personal information from motor vehicle records.⁵⁶² Ultimately, the district approved a settlement.⁵⁶³

It is unclear whether the district had the appropriate insurance to deal with such a massive breach. The governing board subsequently authorized nearly \$20 million to deal directly with breach costs such as those for attorney fees, consulting fees, breach notification, and credit monitoring.⁵⁶⁴ To assist in paying for the breach, the district increased property taxes for the second year in a row to spend an additional \$7.2 million on upgrading the IT department.⁵⁶⁵

Further complicating matters, the Electronic Privacy Information Center (EPIC) and a privacy advocate for DataBreaches.net filed a complaint with the FTC; urging an investigation. They strongly admonished the District for a failure to allegedly “remedy known security vulnerabilities” that had, in part, been identified in a prior breach. In total, the complaint alleges no fewer than 22 separate issues, including the failures too, “respond to an employees’ oversight report in 2011 that outlined data security concerns...and respond to an employees’ grievance report in 2012 that included ongoing data security concerns.”⁵⁶⁶

Revisiting the Gramm-Leach-Bliley Act (GLBA)

As stated previously in this book, GLBA is primarily concerned with governing the privacy and safeguards of financial institutions. However, certain education institutions may also fall under the authority of GLBA as they could be deemed to be “significantly engaged” in numerous financial activities such as lending or providing financial advisory services. Of note, the term “significantly engaged” is not defined within the text of the law,⁵⁶⁷ so educational institutions at all levels will need to seek legal counsel to assess the applicability of this generic term. Logically, many public

K-12 schools will not be significantly engaged in ongoing financial activities, whereas the preponderance of most post-high-school education programs could easily fit into this category.⁵⁶⁸

Due to the unique circumstance of categorizing certain educational institutions as financial institutions under GLBA, the FTC has provided some flexibility as it relates to the Privacy Rule. Notably, the FTC has stated, “Any institution of *higher education* that complies with the Federal Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with [the GLBA Privacy Rule] if it is in compliance with FERPA.”⁵⁶⁹

Yet again, this could result in even greater confusion as FERPA applies to not only “institutions of higher education,” but potentially to elementary and secondary schools as well. Therefore, a K-12 school which could be deemed a financial institution under GLBA, and must comply with FERPA, may still need to comply with the GLBA’s Privacy Rule.⁵⁷⁰

Privacy Rule

As stated previously in this book, the Privacy Rule requires regulated entities to provide privacy notices to consumers. Although there are certain exceptions, the rule generally allows consumers to limit the “nonpublic personal information” that can be shared by the regulated entity to non-affiliated third parties.⁵⁷¹

This type of covered information is extensive, as is the description of such information found in the statute. However, the information can be generalized into the following three areas:

1. Any information that a consumer has provided to obtain a financial product or service.
2. Any information that results from a transaction between the institution and the consumer.
3. Any information that a regulated entity obtains about a consumer (such as a credit report, Internet “cookie,” or purchase information).⁵⁷²

While an exception to complying with the Privacy Rule may be found for certain K-12 institutions, no such exemption applies to the Safeguards Rule. Consequently, every educational institution deemed a financial institution under GLBA must comply with the Safeguards Rule.

Safeguards Rule

The Safeguards Rule is covered elsewhere in this book in greater detail. However, for a quick overview, the Safeguards Rule requires, among other provisions, to establish standards and physical safeguards:

1. to ensure the security and confidentiality of customer records and information;
2. to protect against any anticipated threats or hazards to the security or integrity of such records, and;
3. to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.⁵⁷³

(Pretexting) Identity Theft Red Flags Rule

As also noted in the GLBA dedicated chapter, the Red Flags Rule attempts to prevent the foreseeable risks of identity theft. As stated by the FTC, at a minimum, the associated mandatory Identity Theft Prevention Program must include, “reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

- Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program;
- Detect red flags that have been incorporated into the Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically to reflect changes in risks from identity theft.”⁵⁷⁴

Dear Colleague GEN-16-12: Protecting Student Information

In July 2016, the U.S. Department of Education released an update to inform institutions of their legal obligations as it pertains to protecting student information used in financial aid programs, as well as how their security programs will be assessed. This marks a distinct departure in that schools will now be audited on GLBA security controls compliance as part of their annual student aid compliance audit.⁵⁷⁵

Among the listed audit objectives are whether the school has:

- Designated an individual to coordinate the infosec program;⁵⁷⁶

- Performed a risk assessment that addresses at least the following: employee training and management, information systems, and detecting, preventing and responding to attacks, intrusions, and other system failures;⁵⁷⁷
- Documented safeguards for each identified risk from the prior step.⁵⁷⁸

Because the objectives do not explicitly state what the auditor will require for compliance, schools will need to begin working early to ensure a smooth result. Auditors without a strong background in information technology and cybersecurity will be crucial for schools to avoid later troubles.

In addition, the Department “strongly encourages” schools to adopt and maintain the standards of NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations). Adopting such a standard is no small feat. From a high level, NIST SP 800-171 contains the following requirements as stated within the Dear Colleague letter:⁵⁷⁹

- Limit information system access to authorized users (Access Control Requirements);
- Ensure that system users are properly trained (Awareness and Training Requirements);
- Create information system audit records (Audit and Accountability Requirements);
- Establish baseline configurations and inventories of systems (Configuration Management Requirements);
- Identify and authenticate users appropriately (Identification and Authentication Requirements);
- Establish incident-handling capability (Incident Response Requirements);
- Perform appropriate maintenance on information systems (Maintenance Requirements);
- Protect media, both paper and digital, containing sensitive information (Media Protection Requirements);
- Screen individuals prior to authorizing access (Personnel Security Requirements);
- Limit physical access to systems (Physical Protection Requirements);
- Conduct risk assessments (Risk Assessment Requirements);
- Assess security controls periodically and implement action plans (Security Assessment Requirements);
- Monitor, control, and protect organizational communications (System and Communications Protection Requirements); and
- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

The Department of Education acknowledges that the above will require significant investment and effort. Nonetheless, they once again “strongly suggest”

that schools that fail to meet NIST standards use NIST as a model to overcome those shortcomings. In other words, it appears that NIST SP 800-171 is a mandatory standard in everything but title. It would not be surprising if this “strong suggestion” is a steppingstone to making NIST SP 800-171 the eventual mandatory standard.

International Law Issues

Also covered previously in this book, international students affected by a breach may also require their own unique notification requirements. Naturally, this will add further complexity and cost when responding to a breach and should be accounted for as appropriate.

Insurance Considerations

The threat of a data breach, and the numerous legal, monetary, and reputational consequences which follow, are very real to schools. A quick Internet search will yield thousands of results for schools that have already had to deal with such issues following a breach.

Surprisingly, it appears that schools have not yet universally adopted cyber insurance as a risk transference mechanism to offset the massive costs they must deal with following a breach. “Cybersecurity insurance in higher education remains a rarity, despite a consensus among those working in the field that the likelihood of such a breach involves “when,” not “if.””⁵⁸⁰ Nor are they necessarily prepared to personally pay for breach costs.⁵⁸¹ Consider that one prominent study listed the cost per capita of an education record at \$166.⁵⁸² Any one university could have tens of thousands of active students, along with five to seven years of previous student records.⁵⁸³ Add in covered financial data from fundraising efforts, payment card information from on-campus eating establishments, and health care data from the school’s hospital. Suddenly, a school could face a very expensive problem.

For public universities, this is an especially troubling pattern which could result in significant financial issues as they may need to rely on their state and its residents to pay for the cost of a breach.⁵⁸⁴

Regardless, cyber insurance is a worthwhile investment that can assist with many, if not most, of these costs.

Action Items:

- ☐ K-12 Guidance found at: <https://studentprivacy.ed.gov/security>;
- ☐ Post-secondary education institution guidance found at: <https://ifap.ed.gov/eannouncements/Cyber.html>;

- 2 CFR Part 200, Appendix XI, Compliance Supplement can be found at: https://www.whitehouse.gov/wp-content/uploads/2019/07/2-CFR_Part-200_Appendix-XI_Compliance-Supplement_2019_FINAL_07.01.19.pdf;
- Work with legal counsel to determine all regulatory regimes, FERPA or otherwise, that your institution of higher education must follow;
- Work with legal counsel and/or a knowledgeable broker to determine how your cyber policy would respond to the various regulatory regimes that could bring fines and penalties.

TCPA – Telephone Consumer Protection Act

The Telephone Consumer Protection Act (TCPA) was enacted in the early 1990s to govern telecommunications commerce. In short, it attempts to regulate the tools that a telemarketer would use, such as automatic telephone dialing systems and voice recordings, as well as the type of telephone line that is contacted. All three types of lines are covered, including wireless phones, landlines, and fax lines.⁵⁸⁵ The TCPA does not govern the transmission of emails.⁵⁸⁶

Cyber insurance policies may offer coverage for media liability claims. However, claims relating to TCPA are often explicitly excluded from coverage.

For example, one prominent cyber insurer specifically notes the following “Spam” exclusion:

“...based upon or arising out of any actual or alleged violation of any federal, state, local, or foreign statutes, ordinances, regulations, or other laws regarding or relating to unsolicited telemarketing, solicitations, emails, faxes, text messages, mobile video messages, or any other communications of any type or nature, including but not limited to the Telephone Consumer Protection Act, CAN-SPAM Act, or any anti-spam or do-not-call statutes, ordinances, or regulations.”⁵⁸⁷

To elucidate this point, consider the case of *Flores v. ACE American Insurance Company*.

The insured in the underlying case, GrubHub, Inc., was a food-ordering company that faced a class-action claim for allegedly violating the TCPA. The plaintiffs alleged that the violation came as a result of sending text messages to customers without their consent. Ultimately, GrubHub settled with the plaintiffs, agreed to a consent judgment, and assigned their rights against their insurer, ACE American. Notably, ACE American had denied coverage to GrubHub, so with this assignment, the class plaintiffs proceeded to attempt collection from the insurer.⁵⁸⁸

When the insurer filed a motion to dismiss, the court held that there were two primary exclusions which prevented coverage.

GrubHub’s cyber policy contained an exclusion for any claim, “alleging, based upon, arising out of or attributable to any unsolicited dissemination of faxes, emails or other communications by or on behalf of the Insured to multiple actual or prospective customers of the Insured or any other third party, including but not limited to actions brought under the Telephone Consumer Protection Act.”⁵⁸⁹

A further exclusion stated that there was no coverage for any claim, “alleging, based upon, arising out of or attributable to false, deceptive or unfair business

practices or any violation of consumer protection laws.”⁵⁹⁰ Here, the court specifically noted that the TCPA is considered a “consumer protection” law, thus no coverage would be afforded.⁵⁹¹

If a cyber policy explicitly excludes coverage, businesses may look toward their general insurance policies for advertising injury or property damage provisions. Whether courts will require general insurance policies to defend insureds for claims alleging a violation of the TCPA is a complex legal area unto itself. Broadly speaking, it depends upon the policy, the state where the case is being decided, and the type of medium used to transmit the data.⁵⁹² This area of the law is often exceedingly complex and seemingly contradictory.⁵⁹³ Therefore, businesses should seek competent legal counsel to address their compliance and insurance concerns.

Action Items:

- ☐ The FTC’s Complying with the Telemarketing Sales Rule can be found for free at: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule>;
- ☐ Understand if your business is subject to TCPA;
- ☐ Continuously monitor the TCPA for any changes to the law or its interpretations;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Determine if any of the business’s insurance policies would cover a TCPA related claim.

CAN-SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act

Digital marketing is a necessity for the modern business. However, there are limitations a business can go to market their services. Businesses should consider the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) enacted in 2003. Though somewhat of a misnomer, the act is broadly designed to protect consumers from unsolicited, bulk, commercial email (UCE) sent by online marketers. UCE can generally be classified as bulk emails for the advertising of goods or services that were not sent to the recipient with their approval and where no previous business relationship could be implied.⁵⁹⁴

Unlike many other laws, the CAN-SPAM Act preempts all other state laws in the area of UCE. However, it does preserve states' common law rules and statutory provisions to the extent they would prohibit email that is false or deceptive.⁵⁹⁵

Email messages sent from commercial entities must generally adhere to the following requirements:

- Email header information cannot be false or misleading;
- There should be no deceptive subject lines;
- An opt-out mechanism should be included;
- The sender's physical address should be included;
- The message should be identified as an advertisement or solicitation.⁵⁹⁶

The FTC is the primary enforcer of alleged CAN-SPAM violations, though other federal agencies such as the SEC and FCC may also have enforcement authority. State attorneys general and other state agencies may also bring an action where state residents were affected.⁵⁹⁷ Interestingly, Internet service providers (ISPs) can also bring claims for certain CAN-SPAM violations.⁵⁹⁸

The cost of non-compliance to businesses can be crippling. The FTC alone notes, "Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to \$42,530, so non-compliance can be costly."⁵⁹⁹ At the state level, statutory damages are limited to \$2,000,000 with a \$6,000,000 cap for willful, knowing, or aggravated violations.⁶⁰⁰

With such sizeable penalties on the line for businesses, they will certainly be looking towards their insurance policies to provide a financial backstop should they

run afoul of CAN-SPAM. Unfortunately, standard general liability policies often exclude coverage for these types of claims.⁶⁰¹

Furthermore, many cyber insurance policies exclude coverage for any CAN-SPAM or similar type claims. As shown previously, one prominent cyber insurer specifically notes the following “Spam” exclusion:

“...based upon or arising out of any actual or alleged violation of any federal, state, local, or foreign statutes, ordinances, regulations, or other laws regarding or relating to unsolicited telemarketing, solicitations, emails, faxes, text messages, mobile video messages, or any other communications of any type or nature, including but not limited to the Telephone Consumer Protection Act, CAN-SPAM Act, or any anti-spam or do-not-call statutes, ordinances, or regulations.”⁶⁰²

Another prominent cyber insurer did not explicitly name the CAN-SPAM act as being excluded from coverage. However, it did note a broad exclusion for “a Claim brought by or on behalf of any state, federal, local or foreign governmental entity, in such entity’s regulatory or official capacity; but this exclusion will not apply to the Regulatory Defense & Penalties insuring agreement[.]” The Regulatory Defense & Penalties agreement within the policy only provides coverage for penalties and claims expenses arising from data breaches or security events.⁶⁰³

Thus, it is reasonable to assume that no cyber insurance coverage would be afforded from at least these prominent cyber insurers for CAN-SPAM related claims.

Given these considerations, businesses should, at a minimum, seek input from legal counsel and compliance experts regarding their marketing practices to determine if they reasonably conform to CAN-SPAM.

Action Items:

- ☐ The FTC’s CAN-SPAM Act: A Compliance Guide for Business can be found at: <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>;
- ☐ Understand if your business is subject to CAN-SPAM;
- ☐ Continuously monitor CAN-SPAM for any changes to the law or its interpretations;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Determine if any of the business’s insurance policies would cover a CAN-SPAM related claim.

Americans with Disabilities Act (ADA)

A growing concern for businesses in the modern age is the conflicting rulings seen at various circuit courts of appeal on whether their website needs to be ADA-compliant. At the heart of the matter is whether ADA Title III's definition of "public accommodations" extends to the Internet, and thus a business's website. Generally, ADA applies to any business with 15 or more employees.⁶⁰⁴

Currently, the First, Second, and Seventh Circuit Courts of Appeals have held that a website can be considered a place of public accommodation without a direct connection to any physical place. However, the Third, Sixth, Ninth, and Eleventh Circuit Courts of Appeals have found that a public accommodation must be a physical place. However, they also noted that a goods or service which is provided by a public accommodation – such as through a website – might fall under the purview of the ADA if there is a sufficient nexus to a business's physical location.⁶⁰⁵

Complicating matters, Stephen E. Boyd, Assistant Attorney General for the Department of Justice, recently responded to a letter sent by a group of U.S. House Representatives regarding ADA-compliant websites. In his September 2018 response letter, Boyd noted:

"[T]he Department has consistently taken the position that the absence of a specific regulation does not serve as a basis for noncompliance with a statute's requirements. Absent the adoption of specific technical requirements for websites through rulemaking, public accommodations have flexibility in how to comply with the ADA's general requirements of nondiscrimination and effective communication. Accordingly, noncompliance with a voluntary technical standard for website accessibility does not necessarily indicate noncompliance with the ADA."⁶⁰⁶

How businesses should interpret this "guidance" from the DOJ is ultimately dependent on a conversation between them and their attorney. Though in the broadest sense, it is generally advisable to voluntarily comply rather than be forced through legal action.

More definitely, the U.S. Architectural and Transportation Barriers Compliance Board, also known as the United States Access Board, has a more definitive say. By way of background, the Access Board is an independent federal agency that coordinates among the other federal agencies to enforce accessibility standards.

Within their 2017 publication, the Information and Communication Technology (ICT) Standards and Guidelines, the Access Board noted that federal contractors, agencies, and vendors are subject to Section 508 of the Rehabilitation Act of 1973.

Thus, federal contractors, agencies, and vendors must have their websites and other electronic material accessible to disabled individuals. To accomplish this, they stipulated that covered entities should adhere to Web Content Accessibility Guidelines 2.0 Levels A and AA (WCAG 2.0 AA) by January 18, 2018.⁶⁰⁷

For clarification, WCAG 2.0 contains four main principles for accessible website designs. They should be perceivable, operable, understandable, and robust. The four levels of conformance with WCAG 2.0 include Level A, Level AA, and Level AAA.⁶⁰⁸ Level A is the minimum level of conformance, and Level AA is the conformance generally cited by the DOJ and various courts.⁶⁰⁹ Level AAA may be impossible to meet for certain types of content, so it is not recommended by the originating authors for entire sites.⁶¹⁰

Given the unique nature of ADA related website claims, it is difficult to determine how any insurance policies would respond to such actions. Broadly speaking, cyber insurance policies will respond to regulatory proceedings, but only when initiated by a data breach or security breach.

More applicable may be a business's Employment Practices Liability Insurance (EPLI) policy if it offers coverage for third-party claims. However, this is far from assured, and businesses should consult their own policies for clarification. Even if a policy were to respond to the claim, they might still lack coverage for any costs necessary to bring their website into compliance, as well as for any relief awarded by the court.

Action Items:

- ☐ Work with legal and compliance experts to determine if your website should be ADA-compliant. If so, consider if your business will make the website WCAG AA Level AA compliant;
- ☐ Continuously monitor ADA accessibility laws and applicable cases for any changes;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Determine if any of the business's insurance policies would cover an ADA related claim;
- ☐ An overview of WCAG accessibility guidelines can be found at: <https://www.w3.org/WAI/standards-guidelines/wcag/>.

The Consumer Financial Protection Bureau

Much like the FTC, the Consumer Financial Protection Bureau (CFPB) has entered the data security and privacy enforcement sphere. As stated by the CFPB website, their goal is to “protect consumers from unfair, deceptive or abusive practices and take action against companies that break the law” in the financial sector.⁶¹¹

The CFPB holds broad authority to take action against to, “*prevent* covered persons or services providers from committing or engaging in an unfair, deceptive, or abusive act or practice under Federal law in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service.”⁶¹²

In early March of 2016, the CFPB issued a press release detailing its first action regarding the alleged misrepresentation of data security practices. Consider the allegations of *In the Matter of Dwolla, Inc.*⁶¹³ Note that there was no indication that Dwolla suffered a data breach.

Dwolla, Inc was an online payment network that allowed consumers to transfer funds to another account or merchant. To open an account, a consumer would first need to provide a litany of information, including name, date of birth, social security number, bank account number, and routing number.⁶¹⁴

As stated by the CFPB, Dwolla represented from 2011 through 2014, that both its network and transactions were “safe” and “secure.” Dwolla’s website stated that their transactions were “safer [than credit cards] and less of a liability for both consumers and merchants.” They also, among other representations, noted that all customer information was securely encrypted, their data security standards surpassed and exceeded industry standards, and that they were PCI compliant.⁶¹⁵

According to the CFPB, Dwolla failed to:⁶¹⁶

- a. adopt and implement data-security policies and procedures reasonable and appropriate for the organization;
- b. use appropriate measures to identify reasonably foreseeable security risks;
- c. ensure that employees who have access to or handle consumer information received adequate training and guidance about security risks;
- d. use encryption technologies to properly safeguard sensitive consumer information; and
- e. practice secure software development, particularly with regard to consumer facing applications developed at an affiliated website, Dwollalabs.

In addition, CFPB stated that Dwolla's servers, data centers, and transactions were not PCI compliant, nor was all the sensitive consumer information stored by held at rest by Dwolla encrypted. Finally, they failed to adopt a written data-security plan to govern their activities and provided little to no data-security training for employees.⁶¹⁷

Ultimately, CFPB found that Dwolla's practices had violated 12 U.S.C. §§ 5531(a) and 5536(a)(1)(B) of the Consumer Financial Protection Act (CFPA). In addition to a \$100,000 civil monetary penalty deposited in the Civil Penalty Fund, Dwolla was ordered to:

- Halt misrepresenting any data security practices.
- Implement and maintain a data security plan to include administrative, technical, and physical controls;
- Designate a person to oversee and be accountable for the data-security plan;
- Conduct risk assessments twice annually;
- Conduct mandatory employee training on a regular basis;
- Fix all security flaws as they are identified;
- Obtain a yearly data-security audit.⁶¹⁸

Although the CFPB likely put substantial resources into the above action, in early 2018, the then-acting director decided to pull back the reigns. Director Mick Mulvaney stated that he would be scaling back the enforcement actions at the bureau,

stating that the CFPB would be “looking to the state regulators and state attorneys general for a lot more leadership when it comes to enforcement.”⁶¹⁹

At face value, the CFPB withdrawing – at least in part – from data security enforcement activity would appear to provide a lack of oversight to entities under the purview of CFPB. However, this could embolden other federal and state regulators to begin taking a more decisive role in regulating unfair and deceptive data security practices.⁶²⁰ Time will tell if data security enforcements will increase in the absence of the CFPB, or if a future administration will allow CFPB to once again take the reins for data security enforcement.

Action Items:

- ☐ Work with legal counsel to keep abreast of any changes in how the CFPB views its role in enforcing data security.

Public Companies & Cybersecurity

As far back as late 2011, the Division of Corporation Finance had issued guidance on their view that although there was no explicit guidance requiring disclosure of cyber-related risks and incidents, companies may nevertheless need to disclose those topics. Quickly following an enforcement action against Altaba Incl, f/d/b/a Yahoo! Inc. for allegedly failing to disclose a data breach affecting 500 million user accounts for almost two years,⁶²¹ the Securities and Exchange Commission released additional guidance. This came in Release Nos. 33-10459; 34-82746, known as the Commission Statement and Guidance on Public Company Cybersecurity Disclosures. The guidance provides for a litany of new considerations for public companies and their disclosure obligations.

Unlike the 2011 guidance, the 2018 guidance made two additional declarations.

15. “Companies are **required** to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws.”⁶²²
16. “Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.”⁶²³

General Guidance

The SEC once again reinforced that current disclosure requirements do not yet specifically reference cybersecurity risks or cyber-related incidents. However, there are several reports which might include cybersecurity risks or cyber-related incidents, dependent up the company’s circumstance. These include:⁶²⁴

- Periodic reports such as annual reports found on Forms 10-K and 20-F, and quarterly reports on Form 10-Q;
- The overarching Exchange Act obligations in that statements should be free from misleading statements and should disclose material facts;
- Current reports such as those on Forms 8-K and 6-K.

Additional Guidance

Risk Factors: Regulation S-K, item 503(c) and Form 20-F, item 3.D mandate that companies disclose factors that could make a securities investment in their company risky or speculative. That cybersecurity risk and cyber-related incidents should be disclosed are a factor. The issues which the SEC considers material to evaluating cybersecurity risk factor disclosure include prior cybersecurity events, probability of occurrence, the impact of an occurrence, adequacy of preventative actions and the limits thereof, industry-specific risks, third party risks, the potential costs of these risks, cost of maintaining cybersecurity protections, cybersecurity regulatory requirements, and any ongoing related regulatory investigation, litigation, or remediation costs.⁶²⁵

Management Discussion and Analysis of Financial Condition and Results of Operations (MD&A): Regulation S-K, item 303, and Form 20-F, item 5, require a company to discuss its financial condition and any changes. The SEC notes that the cost of cybersecurity efforts may need to be included in its analysis. These efforts could include, but are not limited to: the continuing costs of cybersecurity, risks of potential cyber incidents, the cost of a loss of intellectual property due to a cyber event, maintaining necessary insurance, and the costs associated with complying with current and future cybersecurity legislation. The applicable paragraph ends with the SEC explicitly stating that “the Commission expects companies to consider the impact of such incidents on each of their reportable segments.”⁶²⁶

Description of Business: Regulation S-K, item 101 and Form 20-F, Item 4.B mandate that companies discuss their business. If a cyber event could materially affect the, “company’s products, services, relationships with customers or suppliers, or competitive conditions,” then the company is required to disclose those risks appropriately.⁶²⁷

Legal Proceedings: Regulation S-K, item 103, requires a company to disclose information regarding pending legal proceedings of both parent and subsidiary companies. The SEC notes that this could include legal proceedings as they relate to a cybersecurity event, such as litigation involving the theft of consumer information.⁶²⁸

Financial Statement Disclosures: Here, the SEC states that a company’s financial reporting and control systems must be intended to give a reasonable assurance that

the financial impact of a cybersecurity event is incorporated into the financial statements.⁶²⁹

Board Risk Oversight: Regulation S-K, item 407(h), and Schedule 14A – Item 7 both require that a company disclose how its board of directors oversees the company. The SEC is now stating that, to the extent that a cyber risk could materially affect a business, the company should disclose how the board is overseeing the management of that risk.⁶³⁰

SEC Discussion on Policies and Procedures and Disclosure Controls and Procedures: In this portion, the SEC conversation focuses on three main “suggestions” for companies. These include:

17. Companies are encouraged to create and implement comprehensive cybersecurity policies and procedures.
18. These same companies are encouraged to regularly assess their compliance.
19. The creation of a system with adequate controls and procedures to allow senior management the ability to make appropriate disclosure decisions, which also prohibits insider trading on the knowledge of cybersecurity events.⁶³¹

In addition, companies should evaluate their controls and procedures for the following:

- Will the system allow the company to properly record, process, and summarize their cyber-related risk and incidents in required filings?
- Are the company executives and financial officers sufficiently informed to avoid misstatements in their certifications?
- Could there be any deficiencies or oversights in disclosure that would render the controls and procedures ineffective?⁶³²

Insider Trading: Due to the previously mentioned concerns the SEC has with insiders complying with the laws related to insider trading, companies are further “encouraged” to consider the following points:

- How does the company’s code of ethics and policies on insider trading consider and prevent insider trading based on material nonpublic data related to cyber events?
- Has the company considered implementing restrictions on insider trading of securities following a cyber event to avoid the appearance of impropriety?⁶³³

Regulation FD and Selective Disclosures: Under Regulation FD, a company may be required to disclose information regarding cybersecurity. If a company selectively discloses material nonpublic information related to cybersecurity matters, they should consider the following:

- The company should not disclose any material nonpublic information to specified Regulation FD persons before they disclose that same information to the public.
- The company is expected to avoid disclosing material, nonpublic information selectively.
- Any required public disclosure under Regulation FD is done in compliance with appropriate regulations. 634

Businesses should keep in mind that the SEC is putting increasing pressure on companies via their Cyber Unit under the SEC Enforcement Division. A list of SEC cyber enforcement actions can be found for free at <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>

Whether an SEC enforcement action is covered under a cyber insurance policy is speculative at this point. The authors could find no case that would point to an answer. Interested parties should reference their own policies to determine if coverage is afforded for violations of the Securities Exchange Act of 1934 or any similar acts.

Action Items

- ☐ As noted in the SEC's document, general questions should be directed towards the Office of the Chief Counsel, Division of Corporation Finance, U.S. Securities and Exchange Commission.
- ☐ The Commission Statement and Guidance on Public Company Cybersecurity Disclosures can be found for free at <https://www.sec.gov/rules/interp/2018/33-10459.pdf>
- ☐ Businesses are encouraged to read the Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, report on Cybersecurity and Resiliency Observations found for free at <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>

- Business are encouraged to read the Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, found for free at <https://www.sec.gov/litigation/investreport/34-84429.pdf>
- Businesses are encouraged to seek ongoing legal counsel to determine the reasonability of their own compliance efforts, as well as for any changes in SEC guidance.
- Businesses are further encouraged to understand how their own insurance policies could respond to an action brought by the SEC under these guidelines.
- Any entity which falls under the referenced SEC guidance is encouraged to further investigate the AICPA's SOC offering to determine if their accountant can also assist with cybersecurity. A general description of these service can be found later in this book.

GDPR – EU General Data Protection Regulation

The European Union's General Data Protection Regulation became effective in mid-2018. This regulation is notable in that it greatly expanded the definition of personal data to be protected, the jurisdiction to apply and enforce GDPR was increased, the consent requirements became more stringent and gave greater rights to the individual to control their data – including the right to erase that data, and includes very tough penalties among other requirements.⁶³⁵

To fully explain the intricacies of GDPR in such a limited space would be impossible. However, there are a few key points, starting with definitions, that businesses should understand. Generally speaking, GDPR is structured to protect the processing of personal data of EU citizens.⁶³⁶

Processing means “[A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”⁶³⁷

Personal Data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”⁶³⁸

As shown from the definitions, if a business is performing nearly any service that involves the personal data of an EU individual, or the business maintains any data on an EU individual, the business may be subject to GDPR. This could reasonably include sign-up forms for newsletters on websites, the tracking of IP addresses for marketing purposes, or even an EU individual finding the business's ad via an Internet search.

Additionally, GDPR contains a provision that allows EU member states to adopt the rules contained in portions of GDPR by determining more specific requirements.⁶³⁹ Conceivably, this could result in a situation where a business subject to GDPR must also be required to stay compliant with the various stipulations of each EU member state. Such an endeavor is certain to be expensive and time-consuming.

Penalties

Article 58 of the GDPR lists over 20 investigative, advisory, and corrective powers.⁶⁴⁰ Notably, Article 58(2)(i) allows for administrative fines in conjunction with, or instead of, all the other powers listed in the article. Including other actions listed in GDPR, this allows regulators to fine businesses the greater of up to €10,000,000 or 2% of the business's worldwide revenue from the previous year.⁶⁴¹ Article 58(2) also allows for a public reprimand, which could damage brand value as well as demanding compliance within a specific time frame. The latter action could specifically lead to significant costs and turmoil in a company that must now work to meet an imposed timeframe that it may otherwise have rejected as being too disruptive to operations.⁶⁴²

Businesses with company locations inside the EU have been pursued for years by regulators. Whether fines will be levied against non-EU businesses without EU-territory representation remains speculative. Issuing fines against entities where the EU lacks jurisdiction could undermine the gravitas that the EU is hoping to wield with this law.

Regardless, wholly based U.S. companies may agree to submit to GDPR fines for practical business purposes. The business may comply to avoid appearing out of step with current data security standards, which could impact future revenue.⁶⁴³ They may also acquiesce if pressured by other businesses who are registered under the EU-US Privacy Shield agreement so that these other businesses are not found to be non-compliant with GDPR.⁶⁴⁴

For any US-based business which has voluntarily registered under the EU-US Privacy Shield agreement, they are likely bound to any enforcement actions, fines, or injunctions imposed under GDPR.⁶⁴⁵

Exemptions

Given the confusing definitions, potentially excessive cost of compliance, and the high cost for non-compliance, many businesses are naturally interested in any part of the regulation that would definitively exempt them from participating in GDPR. Unfortunately, most, if not all, of the possible exemptions are currently speculative in nature.

There does not appear to be any blanket exemption for small businesses. GDPR makes no compliance exemption for the amount or frequency of data collected. Article 2 does contain limited exemptions, but these do not appear relevant to businesses as they would mainly apply to personal or household activities and the action of member states.⁶⁴⁶ The UK's Information Commissioner's Office (ICO), an

independent regulatory body responsible for enforcing GDPR in the UK, has specifically stated, “You’ll have to comply with the GDPR regardless of your size if you process personal data.”⁶⁴⁷ There may be, although, some exemptions for parts of the regulation that are determined on an individual basis.

Given the complexity and ambiguity of the regulation, the determination of specific clauses will likely remain the subject of litigation for years to come. Businesses are advised to immediately seek competent legal counsel familiar with GDPR to determine their own compliance exemptions or requirements. Most businesses will not have the resources or will to fight prolonged legal battles in this arena.

Action Items:

- ☐ Seek legal counsel to give a qualified opinion on whether your business is subject to GDPR;
- ☐ Determine if your business’s cyber policy would cover GDPR related actions;
- ☐ Keep up to date with enforcement actions at <https://www.enforcementtracker.com/>
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

APEC - Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation (APEC) is a group of 21 Pacific Rim member economies that was created to encourage free and open trade.⁶⁴⁸ Notably, the United States is also a member country.⁶⁴⁹ While still relatively unknown, APEC comprises 55% of the world's real GDP and 44% of world trade.⁶⁵⁰ Thus, there is the possibility of significant growth in relevance in the coming years.

APEC is a large organization with varied goals. For the purposes of cybersecurity and cyber insurance, the voluntary APEC Privacy Framework is the most important for this discussion. The framework consists of the following nine principles:

- Preventing Harm
- Notice
- Collection Limitations.
- Uses of Personal Information
- Choice
- Integrity of Personal Information
- Security Safeguards
- Access and Correction
- Accountability

While the framework is voluntary, certification must come from a certified CBPR Accountability Agent. Currently, there are three accountability agents worldwide, with two in the United States.⁶⁵¹ Only a business certified by an APEC Accountability Agent can claim to be a participant of the APEC CBPR system. The APEC CBPR system can be thought of as somewhat analogous to EU-US Privacy Shield discussed later.⁶⁵²

Within the United States, the Federal Trade Commission (FTC) is the primary enforcement agency regarding violations of the CBPR system. In July of 2016, the FTC began enforcement when it sent a letter to 28 companies that falsely claimed APEC CBPR system participation. This came on the heels of the FTC's first-ever settlement with a company that had allegedly misrepresented participation.

In the Matter of Very Incognito Technologies, Inc., a corporation d/b/a Vipvape, the FTC gave notice to companies nationwide that it will take CBPR enforcement seriously.

In its complaint, the FTC alleged that Vipvape had made statements on its website that related to their participation in the APEC CBPR system. However, Vipvape was never certified to participate by any Accountability Agent. The FTC discovered this alleged oversight by quickly referencing a website that lists all certified companies, www.cbprs.org.⁶⁵³

The FTC, therefore, asserted that VipVape had violated Section 5(a) of the Federal Trade Commission Act, and their actions constituted, “deceptive acts or practices.”⁶⁵⁴

In the settlement agreement, VipVape neither admitted nor denied the allegations made by the FTC. The FTC ordered numerous actions to be taken by VipVape, including the following:

- Acknowledgment of the receipt of the order;
- For 20 years, the business must deliver the order to all relevant and necessary principals, officers, directors, managers, members, employees, agents, and representatives;
- VipVape must obtain a signed and dated acknowledgment of the order within 30 days of delivery;
- Within 60 days, VipVape must submit a compliance report;
- VipVape will have 14 days to submit compliance notices regarding material changes to their business;
- For 20 years, they must maintain specific records as listed in the order and retain those records for a minimum of five years;
- Continued compliance monitoring as dictated by the FTC.⁶⁵⁵

Would a cyber policy cover an APEC related claim?

Unfortunately, there does not appear to be any definitive legal action that can be referenced. Likely it would depend on how the claim arose and what allegations were brought against the business.

If the FTC were to investigate a business following a breach for failure to adhere to the APEC Framework, this might be covered under a regulatory coverage. Businesses will need to reference their own policy language to determine how their insurer defines regulatory actions and policy territory.

If a business falsely or mistakenly claims APEC compliance on their website, coverage will likely depend on the opposing party's allegation, but nonetheless, are unlikely to be afforded coverage. While many cyber policies provide coverage for media liability claims, they also tend to include exclusions for false or misleading advertising.

Looking toward the future, APEC could gain ever greater relevance. In September of 2018, the final draft of the United States-Mexico-Canada Agreement (USMCA) was released. Within the final draft, it was noted that APEC CBPR is a valid method of facilitating cross-border information and data transfers.⁶⁵⁶

Action Items:

- ☐ Understand if your business is a certified member of APEC;
- ☐ Continuously monitor changes to APEC's framework to maintain compliance;
- ☐ Check that your business is adequately protecting all covered data appropriately;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary;
- ☐ Determine if the business's cyber insurance policy would cover an APEC related claim.

Other Foreign “Cyber” Laws

Businesses should be aware that many foreign nations have their own statutes, which may require additional research if residents of those countries are engaged in business with the business, or if the business has offices in those countries. Due to the number of foreign laws, in conjunction with the unknown nature of their legal systems by these authors, they will not be covered in this book.

While the laws naturally vary between nations, businesses should begin their search by looking for consumer protection, cybercrime, data protection and privacy, and electronic transaction laws. It is *highly* advised that businesses engage legal counsel familiar with foreign laws in this area as applicability and enforcement may vary greatly.

Action Items:

- ☐ Consult the United Nations Conference on Trade and Development: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx;
- ☐ If you believe that you may be subject to foreign statute, it is recommended that you seek assistance from legal counsel immediately;
- ☐ Determine if your policy’s coverage territory would respond to cyber-related claims in foreign countries;
- ☐ Determine if your policy would respond to a cyber-related regulatory claim brought by a foreign power.

Section 5: Potential Coverage in Non-Cyber Insurance Policies

Coverage for “cyber”-related losses is not necessarily to be found exclusively in dedicated cyber policies. Dependent on the type of loss and the policies carried by the business, coverage may be found elsewhere. It is advisable that businesses first start from a position of believing they have no insurance for these types of losses so they can thoroughly investigate how their different policies may respond to the various loss scenarios. Commonly carried policies that may include coverage for specific losses include commercial, crime, and professional liability, employment practices, D&O, and tech E&O type policies.

Commercial Insurance Policies

While many businesses may believe that insurance coverage for data breaches – hereafter referred to as “cyber insurance” – is only found in dedicated policies, that is not necessarily the case. When businesses assess their cyber insurance needs, there are various policies that may contain coverage elements which may, or may not, respond based upon the scenario. Failure to properly assess the coverage of the business may lead to losses that would otherwise have been covered.

Before cyber insurance became well-known, businesses would often look toward their commercial insurance policy for coverage if a cyber policy was not available for coverage. Within a business’s commercial insurance policy, they will likely see three primary types of coverage:

- Coverage A – covering property damage and bodily injury;
- Coverage B* – covering personal and advertising injury;
- Coverage C – covering medical payments associated with bodily injury.⁶⁵⁷

*Coverage B is the most likely to be investigated for possible coverage following a breach.

Of note in commercial insurance, these policies are generally designed to cover property damage as a covered loss. Most policies of this type specifically exclude damage to the insured’s owned property. Rather, coverage is afforded if they damage another’s property or person.

There have been a few cases where companies successfully argued that certain data breach associated losses should be covered under their commercial insurance policies Coverage A provisions.⁶⁵⁸ However, most courts have acquiesced to hold that the loss of data is not considered tangible property and thus cannot be covered under a commercial insurance policy.⁶⁵⁹ In a case as recent as 2014, the court further limited recovery under a Coverage A dispute as hard drives contain “abstract and intangible” data, and thus a business could not argue coverage for damage to “tangible property.”⁶⁶⁰

Should a business seek to find data-breach coverage under a commercial insurance policy, they may consider Coverage B provisions. Coverage B generally indemnifies a business for personal or advertising injury. Personal injury would refer to three general categories:

- “(1) false arrest, malicious prosecution, or willful detention;
- (2) libel slander, or defamation of character, and;

(3) invasion of privacy, wrongful eviction, or wrongful entry.”⁶⁶¹

Advertising injury is generally understood to cover “publication offenses, misappropriation of ideas, and infringement of copyright or trademark offenses.”⁶⁶²

Should a business attempt data-breach coverage under Coverage B, they can expect insurers to sternly challenge such a claim. Courts have thus far been conflicting in their reasoning to uphold or dismiss such cases.

In the case of *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC*, Portal, a healthcare company, faced a class-action claim from customers following a data breach that allegedly exposed their healthcare records. In turn, Portal sought coverage for the claim under their commercial general liability policy with Travelers Indemnity Company. Portal’s policy contained coverage for “electronic publication of material that...gives unreasonable publicity to a person’s private life[.]”⁶⁶³

Travelers proceeded to bring a claim against Portal, alleging that the exposure of material did not equate to the publication of material, so no coverage should be afforded. They argued, in part, that no publication could have occurred because the insured had no intention to publish the healthcare records, and there was no indication that anyone had viewed the material. Ultimately, the district court, as well as the Fourth Circuit court, sided with Portal. Their reasoning was that the distinction held between “advertent” and “inadvertent” publication was irrelevant. Regardless of the intent, the exposure of the customer’s medical records was a publication that otherwise resulted in unreasonable publicity for their private lives.⁶⁶⁴

In stark contrast to the previous case was *Zurich American Insurance Co. v. Sony Corp.* Sony sought to recover under its commercial general liability policy following a breach of its Play Station Network, which allegedly exposed the names, addresses, and credit card data of roughly 77 million users. Within Sony’s policy was a provision that covered for the “[o]ral or written publication, in any manner, of material that violates a person’s privacy.”⁶⁶⁵

While at face value, this provision would appear to afford coverage; ultimately, the judge found in favor of Zurich. His rationale was that a publication would only occur if Sony were the ones to have published the data in question. The information had been obtained by a third-party hacker and without the permission of Sony. Thus, coverage, in this case, was denied.⁶⁶⁶

Perhaps the Sony case would lead businesses to believe that if they mistakenly, but otherwise purposefully, exposed data, this would lead to a covered loss. A common example would be placing multiple clients’ files into a client-accessible folder meant for one person. Unfortunately, coverage may still be denied.

In the case of *Creative Hospitality Ventures, Inc. v. United States Liability Company*, Creative faced a lawsuit for violating the Fair and Accurate Credit Card Transaction Act due to printing greater than the last five numbers of the consumer's credit card number on receipts. Upon facing the lawsuit, Creative Hospitality Ventures sought coverage under Coverage B of their commercial insurance policy.⁶⁶⁷

At face value, this would appear to be a covered loss as Creative Hospitality Ventures published the consumer data. However, the court did not agree. In its holding, the U.S. Court of Appeals for the Eleventh Circuit argued that coverage was denied because it did not consider receipts to fit the policy definition of "publication." Under the court's reasoning, a publication meant the "act or process of issuing copies...for general distribution to the public." Though the business printed the receipts, they were not meant for "general distribution to the public" and thus would not be considered publications. Hence, coverage was denied.⁶⁶⁸

Even if insurance companies are successful in their bid to deny coverage for data-breach-related claims brought under commercial liability policies, they would generally prefer to avoid the negative publicity and associated court costs. Thus, insurers are continually opting to refine their policy language with specific exclusions. Often, the source of these exclusions comes from the Insurance Services Office (ISO), a body which provides standardized policy language that can be altered by insurers for their own purposes.

In response to these manners of claims, ISO has offered the following specific endorsements which may already be found in a business's commercial insurance policy, though this is not a definitive list:

- ☐ CG 21 08 05 14 (Exclusion: Access Or Disclosure Of Confidential Or Personal Information (Coverage B Only)). Precludes coverage under Coverage B for disclosure or access to personal or confidential information. Specifically, this excludes coverage for notification costs, credit monitoring expenses, forensic examination and investigation expenses, expenses for public relations to handle the event, and any other related cost, loss, or expense.⁶⁶⁹
- ☐ CG 21 07 05 14 (Exclusion: Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability: Limited Bodily Injury Exception Not Included). This endorsement further excludes coverage for property damage or bodily injury that results from the disclosure or access of computer data or the loss or damage of computer data.⁶⁷⁰
- ☐ CG 21 06 05 14 (Exclusion: Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability: With Bodily Injury

Exception). Similar to the previously listed endorsement, this clarifies that bodily injury that results from the damage or loss of computer data is not to be excluded.⁶⁷¹

Recently, certain insurers offering commercial general liability policies have been offering small endorsements to their base policies. Generally, coverage has been capped at \$10,000 of coverage, which is drastically insufficient for most businesses. Additionally, the coverage elements offered lag those offered in dedicated cyber policies, so most businesses have elected to eschew such minimalist coverage.

While limited coverage may be afforded under a commercial insurance policy, definitive coverage may be unknown until the case is decided. More extensive coverage features than those found in a commercial insurance policy may be found in a dedicated cyber policy.

For most businesses, the cost to litigate nuanced insurance policy language will likely be far greater than the purchase of a dedicated cyber insurance policy. As more commercial liability insurance policies are litigated, insurance companies will continue to refine coverage elements and exclusions to specifically avoid coverage for data-breach-related claims. Thus, coverage for future claims brought in this sphere will likely be even more difficult.

Action Items:

- ☐ Determine what “cyber”-related claims may be covered under your business’s commercial insurance policy. This will likely require the assistance of a competent legal broker and/or legal counsel;
- ☐ Continuously monitor the coverage afforded under your business’s commercial insurance policy for any changes;
- ☐ Communicate this data to relevant stakeholders including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Commercial Crime Policies

Businesses often purchase a crime policy if they are handling large sums of money and are concerned about an internal misappropriation by staff. Businesses may also purchase or attempt to rely on a crime policy for specific data-breach-related funds which are often the loss of funds via fraudulent wiring instructions. Of interest to this discussion, crime policies often offer coverage for computer crime and funds transfer fraud, and possibly in amounts larger than those found in dedicated cyber insurance policies. These will be discussed in turn.

Computer Crime

Take, for example, a common policy provision found within a popular provider of crime policies for computer crime.

Computer Crime coverage:

“1. Computer Fraud: The Company will pay the Insured for the Insured’s **direct loss of, or direct loss from** damage to, Money, Securities and Other Property directly **caused by Computer Fraud.**”⁶⁷²

“Computer Fraud” is later defined in the policy as:

“The use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Financial Institution Premises:

1. to a person (other than a Messenger) outside the Premises or Financial Institution Premises, or;
2. to a place outside the Premises or Financial Institution Premises.”⁶⁷³

From the above, it can be extrapolated that coverage under a crime policy often requires the wrongful act to directly cause the damages being sought by the insured. In the context of computer-related fraud, this could mean that the losses incurred by the fraud must relate to negative acts committed on the insured’s computer. However, insurers will often question coverage for certain computer-fraud losses with arguments of causation.

To illustrate this point, consider the case of *Apache Corp. v. Great American Insurance Co.*, a case hinging on social engineering.

By way of background, the fraud began when one of Apache’s staff members received a phone call from a person purporting to be from a known and legitimate vendor of Apache. The caller requested that Apache change the bank account number of the vendor. In response, Apache notified the caller that they would need to submit

such a request on the vendor's letterhead. In response, Apache received a duplicitous email containing a counterfeit letter on the vendor's letterhead to confirm the change in banking information. To the credit of the Apache employee, they called the phone number listed on the fake letterhead to authenticate the banking details. Once confirmed, Apache wired roughly \$7 million via their computer inputs to a fraudulent account.⁶⁷⁴

Thankfully, Apache was able to recoup some of the money lost, which was likely due to an internal controls error at the bank.⁶⁷⁵ However, not all was recoverable, and in response, Apache filed a claim with their crime policy insurer, Great American Insurance Company. In response, Great American Insurance Company sought to deny coverage.⁶⁷⁶

Relevant to this claim was the policy language being relied upon by both parties like policy listed above. Specifically, the policy covered computer fraud damages for the "loss resulting directly from the use of any computer to fraudulently cause a transfer of that property" to a third party. Great American argued that the loss was not due directly to computer usage.⁶⁷⁷

The Fifth Circuit Court subsequently agreed with Great American. The court held that the loss did not arise directly from the use of a computer. The email was incidental to the Apache employee authorizing the transfer of funds. In a clear warning to all businesses holding a crime policy, the court cited a previous, similar ruling by holding that "'computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy', essentially covering losses from all forms of fraud rather than a specified risk category."⁶⁷⁸

Such rationale by the courts has been upheld in numerous other cases of similar construction.⁶⁷⁹ Thus, it is important for every business to carefully read their own policy language with competent legal counsel to clarify their own coverage. Otherwise, a business could discover that their policy does not cover what is conceived of by a plain language policy assessment.

Funds Transfer Fraud

Many crime policies purchased by businesses also offer coverage for funds-transfer fraud. As social engineering-fraud schemes become more painful and prevalent for businesses, this is a policy provision worthy serious consideration. However, businesses should not blindly believe any funds-transfer loss can be covered by this policy provision.

Take, for example, a common policy provision found within a popular provider of crime policies for funds-transfer fraud:

Funds transfer fraud coverage:

“Funds Transfer Fraud” means:

1. an electronic, telegraphic, cable, teletype or telephone instruction **fraudulently transmitted** to a Financial Institution directing such institution to debit a Transfer Account and to transfer, pay or deliver Money or Securities from the Transfer Account which instruction **purports to have been transmitted by the Insured**, but was in fact fraudulently transmitted **by someone other than the Insured without the Insured’s knowledge or consent**, or;
2. **a fraudulent written instruction**, other than one covered under [a different insuring agreement] issued to a Financial Institution directing such Financial Institution to debit a Transfer Account and to transfer, pay or deliver Money or Securities from such Transfer Account by use of an electronic funds transfer system at specified intervals or under specified conditions, which written instruction **purports to have been issued by the Insured** but was in fact fraudulently issued, Forged or altered **by someone other than the Insured without the Insured’s knowledge or consent.**⁶⁸⁰

This definition further states, “Funds Transfer Fraud does not include Social Engineering Fraud or Computer Fraud.”⁶⁸¹

Thus, coverage does not necessarily apply if an employee is duped by a hacker into transferring business or client funds. To sophisticated purchasers of insurance, such exclusions did not sit well in the age of social engineering. For this reason, crime-policy insurers began offering coverage for social engineering. This too will undoubtedly come with its own unique coverage restrictions that should be investigated by the business.

Social Engineering Fraud Coverage

Within the social engineering fraud coverage endorsement, some insurers will name a specific exclusion if the money transfer was initiated by an authorized person.

For example, take the case of *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co.* Aqua Star’s troubles began when a hacker sent a fake email to their treasury manager requesting that they change the bank account number of a known vendor. The employee then changed the account number in their internal spreadsheet used to track bank account numbers for vendors. Aqua Star was ultimately defrauded of over \$700,000 when funds were sent to the wrong address. In response, they filed a claim with their crime insurance policy provider.⁶⁸²

Travelers attempted to deny coverage due to the following exclusion for any “loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured Computer System.”⁶⁸³

The court agreed with Travelers. Specifically, the court noted in their holding, “[A]n indirect cause of the loss was the entry of Electronic Data into Aqua Star's Computer System by someone with authority to enter the system, [the named exclusion] applies. None of Aqua Star's arguments to the contrary...justify another conclusion.”⁶⁸⁴

As crime policies have evolved, some insurers have begun to eliminate the authorized person's exclusion in their social engineering fraud coverage. However, coverage sublimits in this area tend to be small – typically ranging from \$100,000 to \$250,000 – due to the unpredictability of large dollar losses.⁶⁸⁵ Should businesses elect to insure against social engineering fraud through a crime policy, they should take note of the coverage and exclusions listed in the policy with competent legal counsel.

Action Items:

- ☐ Determine what “cyber”-related claims may be covered under your business’s crime policy. This will likely require the assistance of a competent legal broker and/or legal counsel;
- ☐ Continuously monitor the coverage afforded under your crime policy for any changes;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Professional Liability Policies

In response to the onslaught of data-breach-related claims, professional liability carriers have sought to refine and limit their scope of liability. Most commonly this is done via an endorsement, which first seeks to amend the definition of a data breach in relation to a professional liability claim. Specifically, this can be accomplished by defining “privacy claims” and “client network damage” claims. Effectively, this may result in an overlap of coverage between a business’s professional liability policy and third-party coverage features found in a dedicated, cyber-liability policy. Whether this coverage overlap is detrimental will depend upon the unique circumstances of the business.

For the purposes of this chapter, it would be impossible to include examples from every profession, and every insurance carrier, which has a professional liability policy. To maintain brevity, the following examples will use policy language often found in an accountant’s professional liability policy. While the examples provided can offer guidance for other professionals, all are encouraged to seek legal counsel with any specific policy coverage questions.

Privacy Injuries

One nationwide, professional liability insurer specializing in accounting defines a privacy injury as the following:

“Privacy Injury means:

- (1) any unauthorized disclosure of, inability to access, or inaccuracy with respect to, non-public personal information in violation of:
 - (a) an *Insured’s* privacy policy, or;
 - (b) any federal, state, foreign or other law, statute or regulation governing the confidentiality, integrity or accessibility of non-public personal information, including but not limited to, the Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act, Children’s Online Privacy Protection Act, or the EU Data Protection Act.
- (2) an *Insured’s* failure to prevent unauthorized access to confidential information provided to the *Insured* by another, or created by an *Insured* for another, where such information is subject to the terms of a confidentiality agreement or equivalent obligating the *Insured* to protect such information on behalf of another.”⁶⁸⁶

Put succinctly, a privacy claim would generally mean a claim alleging a privacy injury due to a business rendering professional services. Most commonly, this element of coverage would generally provide for a business facing a private right of action suit from a client following a breach. Private rights of action, as they relate to data-breach laws, were discussed earlier in this book. In a similar vein, this could also cover a claim due to breach of a contractually obligated confidentiality agreement.

Client Network Damage

As defined by one prominent insurer, “Client Network Damage Claim means a demand for money or services received by an Insured, including service of suit or institution of arbitration proceedings, alleging Network Damage to an Insured’s client’s computer network in the rendering of an Insured’s rendering of Professional Services.”

“Network Damage means:

20. the unscheduled or unplanned inability of an authorized user to gain access to a network, or;
21. the suspension or interruption of the operation of any network, or;
22. the unauthorized access to, destruction of, addition to, deletion of, or alteration to information maintained on the network of an Insured’s client.”⁶⁸⁷

Client network damage would generally cover damage done to a client’s network if the business’s computer system sent malicious code to a client. Another scenario could include damage to a client’s network, such as downloading malware while a staff member was providing outsourced CFO or Client Accounting Services. Whether this would afford coverage to damages done to the clients of the business’s client is unknown and has yet to be tested.

Additional coverages found in such endorsements may include a small, sublimit of coverage for responding to regulatory proceedings brought by a jurisdiction for violating sections of a breach notification law. Of note, none of the endorsements assessed provided coverage for damages that could be awarded. These endorsements provide a small amount – typically around \$12,500 – for expenses related to the defense of such regulatory claims.

Misappropriation of Client Funds

Found within most professional liability policies is a sublimit for insider theft. Specifically, this would cover the business if a staff member were to misappropriate funds from a client. This would not cover the theft of the business’s funds by a staff

member. Such coverage would likely need to be obtained from a crime policy's employee theft coverage provision.

When contemplating the threat of employee theft, it is crucial that the business considers the sublimit. Many insurers offer a basic coverage of \$100,000, often included in base policy language. At the business's request, this can be increased, generally to no greater than \$2 million.⁶⁸⁸ If higher limits are needed, it may be necessary to consider a crime policy or fidelity bond.

Should a business suffer a loss greater than their policy's stated misappropriations sublimit, it is unlikely that they will be able to recover full policy limits. Such a scenario was seen in the case of *CAMICO Mutual Insurance Company v. Heffler Radetich & Saitta, LLP*.

In this case, Heffler was appointed by the court to act as a claim administrator for a \$490 million settlement. A senior accountant was assigned to assist in the administration of the settlement. Through a series of fraudulent acts, the accountant was able to work with co-conspirators to file over \$5 million in fake claims. A class-action claim was brought against Heffler for damages due to the accountant's crimes.⁶⁸⁹ In turn, Heffler submitted a claim to its professional liability carrier.

Due to the outsized nature of the claim in relation to the \$100,000 sublimit carried by Heffler, CAMICO filed suit against Heffler seeking a declaratory judgment to affirm that no coverage beyond the sublimit was obligated. In response, Heffler filed counterclaims for:

“(1) declaratory judgment that CAMICO has a duty to defend and indemnify not limited by the \$100,000 sublimit, and;

(2) bad faith.”⁶⁹⁰

Ultimately, the court held wholly in favor of CAMICO. In its holding, the court stated that “[a]s Heffler notes, CAMICO's primary reason for denying coverage was the \$100,000 sublimit for misappropriation, misuse, theft, or embezzlement. The Court has concluded that the denial of coverage on this ground was proper.”⁶⁹¹ This decision was later affirmed on appeal by the United States Court of Appeals for the Third Circuit.⁶⁹²

While CAMICO was found to have acted good faith to the policy limits offered and accepted by the firm in question, another case displays how careful businesses should be when seeking coverage for claims arising from a staff member's theft of client funds.

In the case of *Bryan Brothers, Inc. V. Continental Casualty Company*, the accounting firm had been a policyholder for multiple, continuous years. During these successive policy renewals, they employed an on-site, part-time, account clerk who was responsible for basic ledger and bookkeeping activities. Beginning in 2002, until

discovery in 2009, the clerk began to misappropriate client funds from several of the firm's clients. This was done by withdrawing from the accounts of numerous clients. To cover her tracks, the clerk made "checks drawn on client accounts payable to herself and others" while manipulating internal documents. No other employees of the firm were aware of her activities.⁶⁹³

In 2009, the owners of the firm discovered her theft, and upon admission to the clients, subsequently faced multiple claims. In response, Bryan Brothers submitted multiple claims to their professional liability insurance carrier, Continental Casualty Company.⁶⁹⁴

Continental Casualty subsequently denied coverage.⁶⁹⁵

Foremost, Continental Casualty argued that though the clerk has perpetrated fraud against multiple clients, the claims arising from multiple clients would fall under the definition of interrelated acts. Thus, sole acts committed by the clerk during the active policy period would likewise be grouped in with all acts committed prior to the policy renewal.⁶⁹⁶

If successful in arguing that all claims were interrelated, Continental Casualty was effectively limiting their own future, potential liability regarding defending against multiple claims and protecting any damages awarded from the policy.

Of utmost importance, in this case, was the policy language being relied upon for Continental Casualty's denial of coverage for all claims, "In accordance with all the terms and conditions of this policy, we will pay on your behalf all sums in excess of the deductible, up to our limits of liability, that you become legally obligated to pay as damages and claim expenses because of a claim that is both made against you and reported in writing to us during the policy period by reason of an act or omission in the performance of professional services by you or by any person for whom you are legally liable provided that: [...] 2. prior to the effective date of this Policy, none of you had a basis to believe that any such act or omission, or interrelated act or omission, might reasonably be expected to be the basis of a claim..."⁶⁹⁷

Continental argued that the clerk's knowledge of her fraud prior to the effective date of the policy would preclude coverage. In short, the clerk fell under the definition of "you" as stated in the policy and thus should have reasonably believed that her actions could bring rise to a claim. Consequently, she should have reported herself as having committed ongoing fraud.⁶⁹⁸

Continental further denied coverage that would otherwise have been afforded under the innocent insured provision of Bryan Bryans Policy. The policy stated, "If coverage under this policy would be excluded as a result of any criminal, dishonest, illegal, fraudulent or malicious acts of any of you, we agree that the insurance coverage that would otherwise be afforded under this Policy will continue to apply

to any of you who did not personally commit, have knowledge of, or participate in such criminal, dishonest, illegal, fraudulent or malicious acts or in the concealment thereof from us.”⁶⁹⁹

Continental argued that the innocent insured provision would not apply because coverage was denied on the grounds of the clerk’s knowledge of her ongoing fraud, not the fraud itself. While Bryan Brothers considered the provision ambiguous, the court was not persuaded.⁷⁰⁰

Ultimately, the court held in favor of Continental Casualty on all counts as it found the Bryan Brothers’ arguments unpersuasive. The firm appealed the decision and lost again.⁷⁰¹ The total amount of funds that Bryan Brother lost due to bringing a claim against their insurer, as well as defending and settling the multiple claims brought by their own clients, is unknown.

- ☐ Businesses who could find themselves in circumstances where staff members could pose an internal threat to client funds should consider the following:
- ☐ Investigate any misappropriations sublimit inside the professional liability policy;
- ☐ Check that the sublimit, if available, would cover a catastrophic loss due to interrelated acts;
- ☐ Understand the prior knowledge provision and its relation to policy renewal.

Professional Liability Policy Cyber Endorsements

Businesses should pay notice to the limits and sublimit within policy endorsements. Additionally, attention should be paid to the definitions of what is covered as their pertain to endorsement sublimits. These endorsements will look attractive as it appears to offer adequate limits at a reasonable price. “Buyer beware” as coverage elements vary greatly by the insurer.

Third-party cyber endorsement limits are the least likely to be used by a business following a breach.⁷⁰² As a reminder, third party claims are generally classified as private rights of action, class-action claims, and regulatory investigations. Not incidentally, those limits are often listed at the beginning of the cyber endorsement.

Take, for example, the following real-world endorsement found within a common accountant’s professional liability policy:⁷⁰³

<u>Claims for Network Damage/Extortion Demands</u>	
Limit applicable to all claims for network damage in the aggregate	\$500,000
Sublimit applicable to all extortion demands in the aggregate	\$75,000
Deductible applicable to each claim for network damage	\$5,000
Deductible applicable to each extortion demand	\$5,000
<u>Privacy Event Expenses</u>	
Limit applicable to all privacy event expenses in the aggregate	\$75,000
Deductible applicable to each privacy event	\$0

To those not familiar with the intricacies of this line of insurance, the endorsement above appears to offer a half-million-dollar cyber policy for what amounted to roughly \$560. However, it is necessary to carefully examine the definition of the bolded words to determine how this endorsement would respond to a real-life breach. Once again, the failure of the business to provide due diligence on their own endorsements could lead to catastrophic losses or critical gaps in coverage.

As it turns out, the definition of the \$500,000 sublimit of “Network Damage” generally limits coverage to claims brought by clients if they alleged that you infected their computer through the rendering of professional services.⁷⁰⁴

“Extortion Demands,” sub-limited to \$75,000 in coverage, can generally be understood to cover the extortion demands for a threatened or actual ransomware

event.⁷⁰⁵ Ransomware demands, minus a few noteworthy cases, rarely exceed \$2,000⁷⁰⁶. Considering the listed deductible for an extortion demand is \$5,000, it is difficult to see when most businesses would consider this a useful policy feature.

Finally, featured is the generically named “Privacy Event Expenses” with a total \$75,000 in coverage. When referencing the definitions section this endorsement, it covers the following:

- Notification costs to clients potentially affected by a breach;
- Costs associated with adhering to breach notification laws, including the notification of clients affected by the breach;
- Costs associated with computer forensics to determine the scope and nature of the breach;
- Attorney’s fees to assist with regulators and for compliance with breach notification laws;
- Call center costs;
- Remediation of the deficiency that led to the breach.⁷⁰⁷

While a basic listing of features, it does not appear to cover the following widely available elements often found in dedicated cyber policies. For practical purposes, these terms will be further defined later in the book.

- Business interruption costs;
- Regulatory fines, awards, and penalties;
- Crisis management and public relations;
- Contingent business interruption;
- System failure business interruption;
- Cybercrime;
- Social engineering;
- Reputation risk.

In contrast to the above endorsement, a cyber endorsement was offered to the same firm, but with different coverages and for \$480. This endorsement was a \$100,000 per event with a unique aggregate schedule based upon the number of professionals at the firm.

Coverage elements included:

- **Privacy Breach Response Costs:** This includes \$100,000 in coverage to respond to claims brought by clients following a breach alleging “breach of confidentiality, infringement, or violation of any right to privacy, including, but not limited to, a breach of your privacy policy or public disclosure of a person’s private information” Coverage also generally covers claims arising out of state breach notifications and other associated federal statutes.

- **Notification Expenses:** Included is a \$100,000 limit for attorney's fees, legal expenses, forensics, public relations, the cost to mail notifications, and any related advertising expenses.
- **Breach Support and Credit Monitoring Expenses:** This includes a \$100,000 sublimit for providing credit monitoring and identity theft education services.
- **Network Asset Protection:** This \$100,000 generally covers the loss of digital assets and/or defined special expenses. This would include the cost to return your system to the same state as before the event, as well as the costs incurred by the firm for staff to assist in returning the computer system to pre-event status. Special expenses could include the costs to mitigate further damage the firm's computer system, preservation of evidence, purchasing of licenses to restore functionality, and client notification to inform of the degradation, interruption or ceasing of the firm's system.
- **Cyber Extortion:** A \$100,000 sublimit for the ransom paid by a firm to terminate the attack. This would loosely cover both threats to the firm's system as well as ransomware events.
- **Cyber Terrorism:** This provision offers a \$100,000 sublimit if a person or group breaches your system with the intent to cause destruction or to further a belief. This could include being caught in a large-scale, state-sponsored attack which results in damage to the firm's network.

Annual Aggregate Limits	
Number of Professionals	Aggregate Limit
Up to 5	\$100,000
6 to 10	\$200,000
11 to 15	\$300,000
16 to 20	\$400,000
21 to 200	\$500,000

When assessing the total limits available for breach-related claims available via endorsement to a professional liability policy, the market lacks coherency. Combined first- and third-party limits on many endorsements range from \$50,000 to \$500,000.⁷⁰⁸ Whether one carrier’s endorsement is superior to another’s depends on the business’s needs and the sublimits offered per coverage feature.

Depending on the rating mechanism of the carrier, small- to large-sized businesses will often be able to purchase a dedicated cyber policy with higher limits and more coverage features for less than a policy endorsement. Due to their structure and rating scheme, professional liability policy cyber endorsements are often designed for sole proprietors or very small businesses with minimal staff and PII exposure.

Social Engineering and Funds Transfer Loss Coverage

Given a sizable social engineering or funds transfer loss of money owned by a client but controlled by the business, coverage might be sought under a business’s professional liability policy. The rationale for this would be that the claim arose due to a claim brought by the client against the business for professional services rendered.

Unless otherwise specifically excluded, an all-risk policy may require the insurer to respond to such a claim with defense expenses and potential damages awarded to the plaintiff. The ability for a named peril or ambiguously defined policy to respond to such an event is much more dubious. It could be subject to a court ruling whose merits are decided on a case-by-case basis.⁷⁰⁹

Regardless, businesses should seek to clarify coverage with their professional liability insurer. Should the insurer not comment on the coverage specifics of their own policy, businesses are advised to seek competent legal counsel for clarification. When in doubt, businesses should seek appropriate coverage under a dedicated cyber policy or appropriate endorsement of a professional liability policy even if they

believe that there may be duplication in coverage. Waiting until a loss occurs is no time to hurriedly search for potential coverage.

Action Items:

- ☐ Determine what “cyber”-related claims may be covered under your business’s professional liability policy. This will likely require the assistance of a competent legal broker and/or legal counsel;
- ☐ Continuously monitor the coverage afforded under your professional liability policy for any changes;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Employment Practices Liability Insurance Policies

Employment Practices Liability Insurance (EPLI) Policies generally cover wrongful employment act claims against the business. Common claims where an EPLI policy would respond include allegations of discrimination, harassment, and wrongful termination from employees. Certain policies may also cover temporary or leased workers and claims from third parties bringing claims of sexual harassment or discrimination.⁷¹⁰

While it is feasible that an employee could bring a claim following a data breach, it is unlikely that an EPLI policy would respond to such a claim. Many EPLI policies are constructed as “named peril” policies. This means that only those wrongful employment acts listed in the policy will be covered.

In theory, a Biometric Information Privacy Act (BIPA) claim could be covered under an EPLI policy. However, the authors were unable to find a relevant legal example. Businesses are encouraged to reference their own insurance policies with competent legal counsel for further clarification.

Assuredly, some enterprising plaintiff’s attorney, or business without a proper cyber policy, may find a novel claim construction alleging coverage under an EPLI Policy. However, as of publication, the authors were unable to find the record of a single case where an EPLI policy has responded to a data breach claim. It is conceivable that an EPLI policy could respond to an Americans with Disability Act (ADA) claim related to a business’s website. However, this would be highly circumstantial and dependent upon the allegations made in the claim as well as a unique wording of the policy.

Action Items:

- ☐ Determine what, if any, “cyber”-related claims may be covered under your business’s EPLI policy. This will likely require the assistance of a competent legal broker and/or legal counsel;
- ☐ Continuously monitor the coverage afforded under your EPLI policy for any changes;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Director and Officers Liability Insurance (D&O) Policies

Director and Officers Liability Insurance (D&O) policies generally cover claims against an officer or director for allegations of wrongful acts they committed while acting in their professional capacity. Companies often seek coverage under their D&O policy for claims involving a breach of fiduciary duty, theft of intellectual property, misrepresentations, or failure to adhere with workplace laws – often employment-related.

Thus, it would seem strange that companies would look toward their D&O policy to assist with at least partial insurance coverage following a data breach. Unlike most other lines of insurance, there does yet appear to be any widespread exclusions to coverage in D&O policies following a data breach. However, if D&O insurers begin finding themselves covering claims which they believe should have been covered under a cyber policy, businesses may quickly find a new exclusion on their policies.⁷¹¹

The most prominent case of possible data-breach-related coverage found in a D&O policy was shown in *Spec's Family Partners, Ltd. v. Hanover Insurance Company*.

Prior to the case, Spec's had entered in a Merchant Agreement with First Data Merchant Services to process payment cards for transactions occurring at Spec's. Subsequently, it was found that Spec's credit card network had been hacked for roughly one and a half years.⁷¹²

As a result of the breach, First Data asserted that there was “conclusive evidence of a breach of the cardholder environment at Spec's.” Further, Spec's was not in compliance with their PCI DSS requirements, and thus, First Data incurred costs related to the breach. First Data sent a demand letter to Spec's for the associated case management fee, reimbursement costs, and fines which totaled \$7,624,846.21. They also demanded documentation that Spec's prove they were now PCI DSS compliant by an attestation of compliance by a third-party qualified security assessor. Early the following year, First Data notified Spec's that the costs of the breach would increase by another \$1,978,019.49. These funds, to which Spec's believed they were entitled, were to be held in reserve accounts by First Data.⁷¹³

In turn, Spec's provided both letters from First Data to its D&O insurer, Hanover Insurance Company, as a claim. Initially, Hanover denied coverage but later agreed to provide for defense, subject to a reservation of rights letter.⁷¹⁴ To recoup the reserve account funds, Spec's filed a suit against First Data.

Initially, Hanover complied with a defense funding agreement, but eventually they decided that litigation expenses were not “defense expenses.”⁷¹⁵

Previously, Spec’s had purchased a Private Company Management Liability (D&O) policy from Hanover. The policy contained the following pertinent clauses:⁷¹⁶

Corporate Entity Liability: We will pay “Loss” which the “Insured Entity” is legally obligated to pay because of “Claims” made against the “Insured Entity” during the “Policy Period” and reported to us during the “Policy Period” for any “Wrongful Act” to which this insurance applies.”

“Claim” means:

23. Any written demand presented for monetary “Damages” or non-monetary relief for a “Wrongful Act,” or;
24. Any complaint or similar pleading initiating a judicial, civil, administrative, regulatory, alternative dispute or arbitration proceeding, including any appeal result from it, to which an “Insured” is provided notice and which subjects an “Insured” to a binding adjudication of liability for monetary or non-monetary relief for a “Wrongful Act.”

“Loss” means the amount the “Insured” is legally obligated to pay for “Damages” and “Defense Expenses” for a covered “Claim” under this Coverage Part. “Loss” does not include:

25. Any amounts which an “Insured” is obligated to pay as a result of a “Claim” seeking relief or redress in any form other than monetary “Damages;”

The policy had included several exclusions. Central to Hanover’s attempt to deny coverage was the following:

This insurance does not apply to:

“Loss” on account of any “Claim” made against any “Insured” directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. However, this exclusion does not apply to your liability that would have attached in the absence of such contract or agreement.”⁷¹⁷

Ultimately, Hanover was successful at the district court level in arguing that the policy excluded coverage for claims that had arisen as a result of the merchant services agreement between First Data and Spec’s. Immediately following the decision, Spec’s appealed.

In June of 2018, a three-judge panel of the Fifth Circuit reversed the ruling of the district court and remanded the case back to the district court for additional proceedings.⁷¹⁸

The logic of the Fifth Circuit in remanding the case was somewhat puzzling. The court held that the policy exclusion stated previously did not necessarily apply. The demand letters by First Data referenced Spec's non-compliance with PCI DSS standards and monetary relief but was "wholly separate from the Merchant Agreement." The demands for security, as well as requests for prompt payment from First Data "implicate theories of negligence and general contract law that imply Spec's liability for the assessments separate and apart from any obligations "based upon, arising out of, or attributable to any actual or alleged liability under" the Merchant Agreement."⁷¹⁹

Ultimately, it should be noted that the circuit court was not explicitly finding the existence coverage existed for Spec's. Merely, they concluded that when assessing policy language in favor of Spec's, there is a possibility for some or all of the claim to be covered.⁷²⁰ The case is currently ongoing and is assuredly being watched closely by D&O insurers.

Perhaps most puzzling is why Spec's was attempting to find coverage for a data breach and PCI DSS expenses under their D&O Policy. Cyber policies often have contractual liability exclusions, but most have an exception that provides for PCI DSS-related costs. Many come with this coverage as a standard option. Whether Spec's neglected to purchase a cyber policy, or their policy, for whatever reason, did not contain PCI DSS coverage, is speculative. Of further speculation is what other costs Spec's incurred as a result of the breach that was not involved in the above litigation and thus is wholly borne by Specs. Regardless, they could have saved the time, effort, and litigations costs seen in this case with a simple policy coverage assessment.

Action Items:

- ☐ Determine what, if any, "cyber"-related claims may be covered under your business's D&O policy. This will likely require the assistance of a competent legal broker and/or legal counsel;
- ☐ Continuously monitor the coverage afforded under your D&O policy for any changes;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary.

Tech E&O Policies

As traditionally non-technology-oriented businesses continue to acquire or organically develop computer-related services, the probability that these services are covered by a separate insurance policy is increasing. Common offerings in this range can include software installation, client training, hardware sales, and various types of computer-related consulting services. As these practice areas fall outside the scope of traditionally insured services, businesses will often need to seek coverage from a Technology Errors and Omissions Professional Liability (Tech E&O) policy.

At its most basic, Tech E&O policies are designed to cover businesses from third-party claims. Often such claims would arise due to the failure of a product or an error or omission in the performance of the technology service offered. This could include programming errors, failure to discover a crucial flaw, and implementation problems. Common claim allegations could include failure in the consultation process, deficient services rendered under the contract, or lack of work completion.⁷²¹

More immediately useful for businesses facing a breach of PII would be any first-party coverage elements found in their Tech E&O policy. As stated elsewhere in this book, first-party costs are those costs to a business following a covered event that they would otherwise be responsible for without a dedicated cyber insurance policy. Generally, these would be found under a “Privacy Notification Costs” policy provision, or some analogously named provision.

Common first-party coverage features in these policies can include forensic, legal, notification, credit monitoring, and call center costs. However, the limits or availability for these features vary by policy and could be subject to numerous sublimits that could result in unanticipated costs.

While Tech E&O policies continue to evolve in their coverage features, their first-party coverage elements and limits are generally more limited than those found in a dedicated cyber insurance policy. They may also lack necessary third-party features such as coverage for PCI DSS fines, penalties, and assessments.

Of note for any business insured under a Tech E&O policy would be the source of the breach which might trigger coverage. Even if the parent business proper is named on the declarations page as a named insured, this does not necessarily mean that a breach of the parent firm would be covered.

These types of policies have definitions for both “Professional Services,” and “Technology Based Services” that vary by insurer.

The definition of “Professional Services” will often specifically exclude any activities offered by white-collar professionals such as accountants, architects, lawyers, and engineers.

“Technology Based Services” further limits coverage which would not include any services offered by a non-technical parent company.

Therefore, if the breach arose in the system of the technology provider and affected the clients of the technology provider, there would likely be first-party coverage. If the breach arose in the system of the technology provider and affected the clients of the provider, as well as the clients of the parent company, any costs related to the parent company’s clients, may not be covered.

Therefore, it is prudent that any business carrying a Tech E&O policy understand what entities are covered under the policy, but also contemplate how various scenarios could potentially afford or deny coverage. Likely, it would generally be simpler to have a dedicated cyber insurance policy cover both the business and the technology provider under one policy to avoid ambiguities and potential pitfalls.

Technology Services Coverage in Miscellaneous E&O Policies

Certain businesses may have technology services endorsed on a “Miscellaneous E&O” policy form. These style of Tech E&O policies vary widely in their coverages and endorsement language. They will often contain manuscript endorsements that are unique to the business and its circumstances. As such, they are beyond the scope of this book. If a business has technology services endorsed under a Miscellaneous E&O policy, they are advised to seek competent legal counsel to ascertain coverage elements.

Action Items:

- ☐ Determine what, if any, “cyber”-related claims may be covered under your business’s Tech E&O policy. This will likely require the assistance of a competent legal broker and/or legal counsel;
- ☐ Continuously monitor the coverage afforded under your Tech E&O policy for any changes;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Section 6: Dedicated Cyber Insurance Policies

While coverage for various “cyber”-related incidents and claims may be found in more traditional policies, businesses are generally better served by dedicated cyber insurance policies. However, these comparatively new types of insurance are far from standardized. Basic terms could provide radically different coverage elements depending on the insurer. Businesses must become familiar with all aspects of a dedicated cyber policy to maximize their chances of being covered when an incident occurs.

Cyber Insurance Applications

Typically, a business will need to complete a lengthy application for cyber insurance, though in special instances, conditional applications and quotes may be available.⁷²² While traditional insurance applications often fall upon a specified partner within the business to complete, placing this responsibility on one individual is inadvisable for cyber insurance.

The ability of one member of management to successfully complete a cyber application with no inputs from other parties in an acceptable fashion is likely impossible. The questions often appear pedantic in their wording and would require inputs from additional stakeholders to avoid a potential declination. Other entities that should ideally be involved include IT, legal, compliance, and HR. Each stakeholder may have different takes on the questions posed, and flaws in business processes or security can be identified and remedied before the application is submitted.

Regarding the structure of the applications, they can be broadly categorized into the following four categories. Once again, this underscores the need for a business to engage all relevant stakeholders to answer the questions as thoroughly as possible.

26. **Organizational:** This would include fundamental information about the business. Questions could include industry type, employee count, disclosures of revenue, assets, and even audited financial statements.

Included in this category would be questions concerning the type and amount of first-party and third-party sensitive information held or processed by the business such as PHI or PII. Depending on the insurer, they may ask for exact record counts or will settle for a range count, i.e. 50,000 – 100,000 records.

The application will also ask how the business manages its relationship and security with outsourced service providers. Questions may focus on whether the business outsources its IT security functions to a third party or whether third parties have access to the business's network. Be aware that certain insurers may request the breach history of these third parties as well as any contracts in force between the business and these providers.⁷²³

Finally, insurers are obviously interested in the loss history of the applicant as it pertains to data breaches. Businesses who have been breached in the past may need to fill out lengthy questionnaires to satisfy the interests of the underwriter.

27. **Technical:** This section is mainly on the technical controls implemented by the business to address their cybersecurity as well as their network architecture. While the information collected is relatively basic, the idea is to help the underwriter determine a basic risk rating.

Additionally, questions may delve deeper into the type of controls implemented by the business – for example: “Does the business operate an intrusion detection system?” or, “Does the business utilize two-factor authentication for all applications storing sensitive information?”.

Other questions may focus on access to data, both physical and digital. Such questions could focus on physical access to the building and server room, or whether the business has procedures to revoke access following employee termination.⁷²⁴

28. **Policies and Procedures:** This section generally deals with data and information management within the business. Questions often focus on the information that the business would process or sell to third parties. Other common questions would include the data retention and data destruction policy within the business. For a business with an updated data retention policy, this should be easily describable, but every business should check to see whether their internal policy is being strictly followed and whether their policy requires updating.⁷²⁵

Additionally, this section will inquire into the business’s network use and security policies. While insurers are unlikely to ask for a copy of such documents, it is still good practice to have these policies and procedures documented and updated regularly after being approved by the business’s leadership and assessed by legal counsel. Businesses may also be further asked about penetration testing, vulnerability scanning, and incident response plans.⁷²⁶

29. **Legal and Compliance:** This section within the application will ask the business about their adherence to various laws, regulations, and standards. This could include questions on PCI/DSS and GLBA compliance – hence, their inclusion in this book.⁷²⁷

When completing the application, businesses should be aware that additional controls, such as encryption and penetration/vulnerability scanning, may lower the yearly premium paid. Also, some insurers will require certain controls be implemented and maintained as a prerequisite to coverage. However, the implementation of such controls may outweigh the reduced premium or be unnecessary depending on the business size and structure.

As a practical matter, applications may only provide space for a yes or no answer, while others will ask for lengthy explanations. If the business is ever in doubt as to the answer or there is not a definitive answer to the question posed, consider an addendum of explanation(s) provided to the underwriter. There is no need to be bashful and risk a potential denial of coverage.

Furthermore, businesses should understand how different insurers define different terms on their application. For example, two different applications from different insurers may ask about “Cyber Crime.” Understand that this term could have three different meanings. Cybercrime coverage may generally only cover the loss of client funds; or, it may only cover the loss of business funds, and thirdly, it could cover both. As such, businesses should seek clarification of any terms they deem ambiguous so they can properly fill out their application and minimize uninsured exposures or material misrepresentations.

Each question posed by an insurer deserves to be heavily scrutinized and investigated. Cyber applications are not like a professional liability application that can be readily completed by a single partner the day before renewal. To complete the application with the lowest possibility of a material oversight, all stakeholders should be involved, including IT, HR, legal, fellow partners, and anyone else who may provide greater insight. Do not take this task lightly.

As a further word of warning concerning the application, businesses should understand that they are making representations that form the basis of a contract – the insurance policy. These representations may be held against them by the insurer following a breach. Such was the case of *Columbia Casualty Co. v. Cottage Health System*.

Cottage Health System, an operator of hospitals across southern California, purchased a “NetProtect360” cyber insurance policy from Columbia Casualty Company, a surplus lines insurer owned by CNA, a common insurer for accounting firms.⁷²⁸

While applying for coverage, Cottage was required to complete a “Risk Control Self-Assessment.” As part of the application process, Cottage made the following representations in their risk assessment which will likely sound familiar to businesses applying for their own cyber insurance:⁷²⁹

- standards (e.g. conduct security/privacy audits or review findings of independent security/privacy auditors) ● Yes
- c. Audit all such 3rd parties at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? ● Yes
- d. Require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality. ● Yes
13. Do you have a way to detect unauthorized access or attempts to access sensitive information? ● Yes
23. Do you control and track all changes to your network to ensure it remains secure? ● Yes
- a. contractually require all such 3rd parties to protect this information with safeguards at least as good as your own ● Yes
- b. perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your

Ultimately, these questions would provide the foundation of Columbia's assertions that coverage should be denied on Cottage's cyber insurance policy.

Prior to Columbia filing suit, Cottage had become the defendant in a class-action lawsuit. The plaintiffs alleged that 32,000 patients had their records disclosed on the Internet.⁷³⁰ In response, Cottage's insurer, Columbia Casualty Co., had paid for the defense as well as the \$4.1 million settlement. Through the process, it had reserved all rights to later deny coverage and recover all amounts that it paid on the claim. Ultimately this came to fruition as Columbia attempted to deny their claim based on the following factors.⁷³¹

1. Columbia's policy had contained an exclusion for the "Failure to Follow Minimum Required Practices." Such a failure would exclude coverage for **"any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application** for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing."⁷³²

Columbia asserted that Cottage had failed to replace factory default setting in its servers. This failure resulted in the FTP settings on their server to allow for anonymous users accessing protected user data via an Internet search engine. Such allegations directly contradicted Cottage's representations to questions 5, 6, 13, and 23 listed in their application.⁷³³

2. Within the application completed by Cottage, Columbia had noted that the policy would be “**null and void if the Application contains any misrepresentation or omission:** a. made with the intent to deceive, or b. which materially affects either the acceptance of the risk or the hazard assumed by the Insurer under the Policy.”⁷³⁴

Furthermore, Columbia’s policy contained a condition requiring, “Minimum Required Practices” to be followed as a “condition precedent to coverage.” As such, Cottage was required to “**maintain all risk controls identified in the Insured’s Application** and any supplemental information provided by the Insured in conjunction with Insured’s Application for this Policy.”⁷³⁵

Columbia asserted that by allowing the breach to happen, Cottage’s application had contained “misrepresentations and/or omissions of material fact that were made negligently or with intent to deceive concerning Cottage’s data-breach risk controls.”⁷³⁶

For these reasons, Columbia asserted that they were entitled to be reimbursed by Cottage for the full \$4.125 million settlement paid for the class-action claim. Furthermore, they demanded reimbursement for all related expenses, attorney’s fees, and defense costs from the class-action claim.⁷³⁷

As an additional warning for businesses to understand the definitions in their policy, Cottage was also denied coverage for an associated claim brought by the California Department of Justice. The California DOJ was investigating concerns from HIPAA violations stemming from the breach.⁷³⁸

Cottage’s NetProtect360 policy provided coverage for “Damages and Claim Expenses resulting from any Privacy Regulation Proceeding.” However, within their policy, the term “Damages” was defined as “**civil awards, settlements and judgments... which the Insureds are legally obligated to pay as a result of a covered Claim.**” But such payments did not include “criminal, civil, administrative or **regulatory relief, fines or penalties.**”⁷³⁹

Ultimately, the court dismissed the case, but only to adhere to the policy terms requiring the use of alternative dispute resolution.⁷⁴⁰ How such mediation or arbitration was ultimately resolved is not public record. Even if both parties met halfway, it would still result in a +\$2 million loss for Cottage. Such a loss was likely avoidable from the outset if Cottage had been duly educated on the near-impossible terms they had agreed to with their cyber policy.

Action Items:

- ☐ Work with all necessary stakeholders to complete the business's cyber insurance application;
- ☐ Ask questions regarding the meaning of terms on the application if it is unclear;
- ☐ Continuously monitor the business to ensure compliance with the representations made on the application;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Consider seeking legal counsel to assist with the application process.
- ☐ Update the business's internal documents as necessary.

Concerning Admitted vs. Non-Admitted Policies

Upon completion of an application, businesses may be offered terms by multiple insurance companies. Often this can be done after completing only one application. Before a business starts to consider coverage options, they need to understand the differences between policies being offered by admitted and non-admitted insurance companies. In a line of insurance where catastrophic, cyber-related losses such as those seen with “NotPetya” appear to actuarially undefinable and thus unforeseeable, no business would want to file a claim to discover that no funds are available.

Admitted Carriers

For a carrier to qualify as being “admitted,” they must file an application with the state’s insurance commissioner for each state in which they want to do business in. In turn, the state’s Insurance Commission will review the insurance company’s application to ensure that they are adhering to that state’s unique insurance requirements. This will include a strict review of the company’s policy filing, forms, and rates.

Almost without exceptions, insurance companies have a greater depth of knowledge and expertise than could be expected of the average consumer. A primary benefit to consumers of purchasing an admitted policy is that the state’s stricter oversight should protect them from predatory or abusive behaviors by the insurance company, who may otherwise include tricky or deceptive policy language.

As admitted insurers sell policies, a portion of the premiums paid to them will be ceded to the state’s guaranty fund. Should an admitted company become insolvent, the handling and payment of claims are taken over by the state’s guaranty fund. In turn, the guaranty fund will specify a limit on the dollar amount allowed to be paid out for a claim, often based on policy limits carried by the business.

Given the rapidly changing coverage options offered by cyber insurance carriers, it is often difficult for new or smaller insurance carriers to file admitted cyber insurance policies. Filing for an admitted policy is expensive and lengthy. Depending on the state, the process could take years to complete. Weathering this task takes significant expertise and capital. Once this is completed, the market may have shifted into offering new coverage features not available in an admitted cyber policy form.

Non-Admitted Carriers

Insurance companies who fall into this category at the primary insurance level are often referred to as “surplus lines” carriers or companies. Non-admitted carriers are generally subject to token oversight by the state’s Surplus Lines Office. This oversight is generally limited to administrative measures such as the collection of applicable surplus lines taxes attached to policies, but these likely do not include the myriad of consumer protection measures found during an admitted filing.

Many cyber insurance policies on the market are offered by non-admitted carriers, though the exact percentage remains unknown. This is done so that cyber insurance carriers can quickly modify rates and coverage features without undergoing the lengthy and expensive process necessary for admitted filing with state insurance commissioners for oversight.⁷⁴¹

Should a non-admitted carrier become insolvent, a receiver will generally take control of the remaining assets. The receiver generally takes an accounting of all the liabilities and creditors of the company and submits a distribution plan for court approval. Within that plan would be the current claims submitted by the business. In the interim, businesses would need to fund and steer their own defenses and settlements while hoping that the estate may eventually reimburse some of those expenses.

A notable exception would be many non-admitted policies offered by various Lloyd’s syndicates under different trade names who alleged that they write approximately one-third of the world’s cyber insurance. In the early 20th century, Lloyd’s created a “chain of security” comprised of three layers to pay claims should a member become insolvent. The first layer, noted as £51 billion in 2017, is a trust held by the specific Lloyd’s syndicate. The second layer, known as the “member’s funds,” was noted at £24 billion. The third layer, known as the Central Fund, was noted at roughly £3 billion.⁷⁴²

Whether a business should choose an admitted carrier over a non-admitted carrier is circumstantial. Admitted carriers may provide more stability in the event of a catastrophic cyber loss affecting numerous businesses around the world. Further comfort may be found in the state guaranty fund. Non-admitted carriers may offer more policy features, but businesses may not have the oversight provided by the state insurance commissioner to avoid potentially questionable practices. Nor would businesses who hold a non-admitted cyber policy have the ability to access the state’s guarantee fund should the carrier experience financial difficulties following a catastrophic loss.

Action Items:

- Consult with legal counsel and a knowledgeable broker if you are ever in doubt as to the difference between admitted and non-admitted policy offerings.

Large Losses May Lead to Novel Policy Interpretations by Insurers

While the case of *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.* was an example of failing to obtain proper coverage, businesses should understand that even obtaining a suitable policy could still prove hazardous. Due to the relatively new nature of insuring for cyber risks without market-standard language, plenty of litigation is still occurring that could set unforeseen precedents leading to a declination of coverage. Such is the potential in the case of *Mondalez International, Inc. v. Zurich American Insurance Company*.

Mondalez is one of the largest snack companies in the world, manufacturing beverages and snack foods for consumers in roughly 165 countries. Zurich is primarily an insurance company with approximately 55,000 employees and \$60 billion in yearly revenue. Both parties are sophisticated entities with in-house legal counsel.⁷⁴³

Mondalez had purchased a property insurance policy from Zurich for “all risks of physical loss or damage” to Mondalez’s property. Specific to this discussion, the policy included “physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction...”⁷⁴⁴

Further coverage was provided for: “Actual Loss Sustained and extra expenses incurred by the Insured during the period of interruption directly resulting from the failure of the Insured's **electronic data processing equipment or media** to operate.”⁷⁴⁵

Trouble arose in June of 2017 when Mondalez became a victim of malware, which was later referred to as the “NotPetya” virus. Initially, the virus infected two of its servers in different geographic locations. Then, the virus then spread across the entire Mondalez network to allegedly render inoperable 1,700 servers and 24,000 laptops owned by Mondalez. According to Mondalez, this resulted in “property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins, and other covered losses” exceeding \$100,000,000.⁷⁴⁶

Mondalez alleged that they promptly filed a claim and provided Zurich will all manner of assistance to satisfy a proof of loss. Regardless, approximately a year after the malware incident, Zurich sent Mondalez a letter denying coverage.⁷⁴⁷

The basis for Zurich’s denial of coverage is not based upon a complex combination of policy elements, but rather a single exclusion in Mondalez’s policy:

“B. This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event,

whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss: ...

2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:

- (i) government or sovereign power (de jure or de facto);
- (ii) military, naval, or air force; or
- (iii) agent or authority of any party specified in i or ii above.”⁷⁴⁸

In short, Zurich asserted that the “NotPetya” virus fell under the common war exclusion clause. Mondalez sued, alleging that their grounds for exclusion was unprecedented among other common claims such as unreasonable conduct and breach of contract. They assert that it would be the first coverage declination for a cyber policy under this decades-old exclusion for anything other than cases of conventional warfare.⁷⁴⁹

Given their declination of coverage, the burden rested on Zurich to prove that the exclusion did indeed apply to this case.⁷⁵⁰ Yet, cyber-attacks are, by their very nature, difficult to attribute to any one person, organization, or country. On what grounds is Zurich likely to make their case?

While the defense of Zurich is only speculative at this point, they can refer to numerous official statements made by governments in the West, alleging that NotPetya was directed by Russia against Ukraine.

For example, in the United States, where the case is being heard, the White House Press Secretary released the following statement: “In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed NotPetya, quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin’s ongoing effort to destabilize Ukraine and demonstrated ever more clearly Russia’s involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.”⁷⁵¹

Whether such statements will be considered evidence worthy to justify a declination of coverage is yet to be seen in court. Outside of the assertions by various governments and intelligence bureaus, no definitive proof has yet been offered that explicitly and undeniable ties NotPetya to the Russian government. Any evidence of such assertions is likely highly classified and thus unavailable for scrutiny.

Ultimately, the decision may rest on the court in interpreting the nature of “hostile or warlike actions.” Reconsidering such language as vague and in need of

interpretation by the court could alter the meaning of a standard insurance clause, which has been apparent in insurance contracts for decades.

The cyber insurance industry waits anxiously for answers to these questions.

Businesses carrying large-limit policies should ready themselves for possible declinations out of an abundance of caution. When large dollar amounts are on the line, insurers may look to find novel ways to deny coverage. Even if an insurer knows that they may be ultimately unsuccessful in court, they can attempt to deny coverage for as long as possible with protracted litigation. Doing so can allow them to retain the investment gains from invested premiums that would otherwise be immediately lost.

Self-Insurance for Cyber Losses

Reviewing the declinations of coverage found in the cases previously noted, businesses should consider how such declinations would impact them, and whether worst-case scenarios include a partial or full declination of coverage. Under such scenarios, it may be prudent for a business to have funds set aside is worth consideration.

In addition, not every cost associated with a breach may be insurable under a cyber policy. For example, a policy may reimburse the firm for losses experienced due to a business interruption, but the reimbursement may come with various conditions. Employee overtime salary costs necessary to recover from interruption may not be covered and would need to be funded by the firm. This is just one example of many unforeseen costs that could befall a firm following a breach.

Support for some cash reserves was given credence by an insurer in the Cybersecurity Insurance Workshop Readout Report from the National Protection and Programs Directorate, U.S. Department of Homeland Security. Noting, “[S]elf-insurance should not be discounted as a reasonable risk management strategy... That approach, he emphasized, is not the same thing as ignoring risk.”⁷⁵²

A “rainy day” fund for full cyber losses is likely untenable for most firms due to tax implications and cash flow limitations. However, funding deemed reasonable by the firm’s partners, or shareholders can provide a modicum of interim risk-management comfort if the firm is declined coverage, or if certain costs are uninsurable.

Partner Action Items:

- ☐ Work with legal counsel and a knowledgeable insurance broker to determine if it would be advantageous to self-insure for certain amounts if a claim is partially or fully denied;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the firm’s incident response plan and other internal documents as necessary.

Understanding “Named Insured”

It is imperative that businesses take note of which entities are listed as being covered by the policy. How this achieved depends, as usual, on the policy provided by the insurance carrier. Subsidiary entities, entities acquired mid-policy period, or those other entities that the business needs to be covered under the cyber policy, are often, but not always, disclosed on the application.

Certain carriers may automatically cover such entities. For example, one insurer noted the following under “Who is an insured”: “... **insured means a named insured, subsidiary, employee, or acquired entity.**”⁷⁵³

However, there is a caveat to the coverage of an acquired entity. As the same insurer noted: “**With respect to an acquired entity whose revenues exceed 10% of the annual revenues of the named insured** at the time of its creation or acquisition, **any coverage under this policy will expire 90 days after the effective date of its creation or acquisition unless within such 90 day period: 1. the named insured provides us with written notice of such creation or acquisition; ... 4. we agree by written endorsement to provide such coverage....**”⁷⁵⁴

A different insurer was direct in stating that anyone other than the named insured under the policy would not be covered, noting: “The Company is not obligated to pay any amounts for Claims if brought or maintained by, on behalf of, or in the right of any entity which is a parent, affiliate, subsidiary, joint-venturer or co-venturer of any Insured, or other entity in which any Insured is a partner, and including any entity directly or indirectly controlled, operated or managed by such an entity... however, that this exclusion shall not apply to claims brought or maintained by or on behalf of or in the right of any Additional Insured.”⁷⁵⁵

The insurer goes on to state that if the subsidiary’s gross revenue exceeds 15% of the named insured annual revenue, then that subsidiary is only covered for 90 days. The business may provide written notice within that 90 days to request coverage under the cyber policy may be extended to the subsidiary.⁷⁵⁶

Depending on the policy, there may also be coverage, exclusions for contractors, seasonal workers, part-time employees, or similar working arrangements. If the specimen policy does not provide coverage for this type of worker, businesses may be afforded coverage with an endorsement if requested.

Businesses should perform their due diligence to check that any additional entities are properly covered by their cyber policy. Additional research should be undertaken to understand what, if any, notifications provisions are necessary to the cyber insurance carrier when dealing with new entities that the business needs

covered. Failure to understand which parts of the organization are covered could lead to partial or full declinations of coverage, depending on the scenario.

Action Items:

- ☐ Determine if the business's cyber insurance policy names the appropriate parties that require coverage;
- ☐ Continuously monitor the business's legal structure and policies for any changes;
- ☐ Communicate this data to relevant stakeholders;
- ☐ Update the business's incident response plan and other internal documents as necessary;
- ☐ Depending on ownership/legal structure, the business may require additional dedicated cyber policies, or they will need to self-insure for the losses.

Defense Arrangements

Most cyber insurance policies are written with the insurer having the duty and right to defend. In practice, this means that the insurer will provide the counsel necessary to navigate the claim. This would also mean that they have the right to control the defense strategy of any claim.⁷⁵⁷

For most insureds, this will not be an issue, and indeed, they will welcome having experienced counsel assist them. Cyber-related claims are complex, and the average attorney is unlikely to have the depth of knowledge necessary to guide an insured through the litany of laws necessary following a breach.⁷⁵⁸

For the largest businesses – generally those with full time in-house legal counsel – such a provision may not be wanted. In that case, an indemnification policy, or more specifically an endorsement to select legal counsel, may be requested. Whether the insurer will agree to this arrangement is situationally dependent. Furthermore, such an arrangement will need to be agreed to by the insurer before the policy is bound to avoid potentially costly time delays. Businesses pursuing this option must be diligent regarding their choice of counsel.

Also, businesses will generally be limited to a pre-selected series of vendors as offered by the insurer. In practice, most, if not all vendors dealing with first-party costs have been previously vetted by the insurer. This should allow for seasoned specialists in their fields to assist the business at costs lower than those that would otherwise be offered on the open market and with a greater level of expertise. The same rules for negotiating with specific vendors apply to negotiating legal counsel. If a business wishes to have specific vendors, those vendors should be vetted and agreed to in the policy before the policy is bound. These agreements are likewise situationally dependent. Once again, if businesses choose to utilize non-standard vendors, they should be diligent regarding their choices.

Action Items:

- ☐ Determine if the policy is a, “claims made and defended” policy, or an indemnification policy. Generally, only very large businesses would consider an indemnification policy;
- ☐ Consider pre-selecting vendors to minimize unnecessary time delays following a breach;
- ☐ Continuously monitor the business’s policies for any changes;

- ☐ Communicate this data to relevant stakeholders;
- ☐ Update the business's incident response plan and other internal documents as necessary.

Tail Policy Coverage

Each policy should contain a provision for an extended reporting period, also known as a “tail policy.” Given the current climate of mergers and acquisitions, it is important to understand the tail policy provisions in a policy.

Most policies contain automatic coverage for claims reported – in this case, the report of a breach or other covered scenario – for anywhere between 30 to 60 days after the policy lapses due to non-renewal. However, the recent 2018 Cost of a Data Breach Study: Global Overview by IBM and the Ponemon Institute, the mean time to identify (MTTI) a data breach was 201 days in the United States. Thus, tail policy provisions are much more relevant and necessary than most businesses understand.

Each policy should contain a provision to purchase a tail policy. Broadly speaking, this tail policy would provide coverage for a covered claim that results from an act that occurred while the policy was active. However, the length available for purchase varies by the insurance provider.

For example, one carrier only offers a 12-month tail policy for an additional 100% of the annual policy premium.⁷⁵⁹ Another carrier offered up to a three-year tail for 225% of the annual policy premium.⁷⁶⁰ Considering that it took 201 days as the mean time to detect a breach, half of all incidents took longer to detect.⁷⁶¹ Therefore, if businesses are reviewing tail policy terms, they should heavily consider the longest policy tail policy options.

Businesses should further investigate any additional exclusions that may come with the purchase of a tail policy. Specific policies may exclude coverage elements such as business interruption, or crisis management and public relations assistance as a condition of purchasing a tail policy.

Failure to purchase an appropriate tail policy can result in a declination of coverage. Not only would a business be required to pay open market rates for all services out of their own funds, but they would also be required to organize and steer the entire process themselves, which is no small undertaking. Given an M&A scenario, this could result in significant hardship on both sides of the purchase agreement.

Action Items:

- ☐ Determine what length of time is offered on the cyber insurance tail policy. The longer, the better;
- ☐ Communicate this data to relevant stakeholders.

Understanding the Difference Between 1st- And 3rd- Party Cyber Insurance Coverage

Before contemplating any cyber coverage, it is imperative that a business understands the difference between third-party coverage and first-party coverage, as found within cyber policies.

It is most helpful to broadly understand who the “parties” in any insurance policy generally refer to. “First Party” is considered the insured, in this case, the business. The “Second Party,” though a rarely used term, is the insurance company. “Third Parties” would be those who were owed a duty of care by the business, i.e., the First Party. These distinctions will assist the business in understanding how policies are structured and what limits are available in various scenarios.

First-party costs in a cyber insurance policy are those costs to a business following a covered event that they would otherwise be responsible for without a cyber insurance policy. For example, this could include business interruption costs, restoration of data, and providing breach notifications to impacted clients.

Third-party costs in a cyber insurance policy are those costs that a business would incur responding, defending, and paying for a breach-related claim. For example, this could include loss of client funds, regulatory fines, and penalties, and private rights of action brought by clients against a business.

Businesses should be aware that cyber policies generally lack any level of conformity in structure or wording. Policies from different insurers can name the same coverage component name, but in practice, they will respond in drastically different ways depending on how those terms are defined. Furthermore, some insurers offer third party only cyber-risk policies, others, first-party-only cyber-risk. Many contain a combination of the two.

When businesses are brainstorming on the needs for various coverages, they should keep in mind how the definitions of certain coverage terms could result in coverage ranging from full to none.

For example, the business wants to insure against their bookkeeper wiring money. As such, the business would need to consider at least the following three scenarios:

30. Could the bookkeeper misappropriate client funds for their own purpose?

31. Could the bookkeeper be fooled into transferring client’s funds to a hacker?

32. Could the bookkeeper be fooled into transferring business's funds to a hacker?

Depending on the scenario, coverage could be considered either a first-party loss or a third-party loss. Insurance coverage for these scenarios may be found in one policy, no policy, or multiple policies.

An illustrative example of the need to understand the difference between these two coverage types is found in the case of *Camp's Grocery, Inc. v. State Farm Fire & Cas. Co.*

Trouble began for Camp's when three credit unions brought a claim against them for an alleged breach of their computer system. The credit unions noted that the hack allegedly compromised confidential customer data, including card information. Due to the alleged breach, the credit unions suffered losses on "their cardholder accounts, including for the reissuance of cards, reimbursement of their customers for fraud losses, lost interest and transaction fees, lost customers, diminished goodwill, and administrative expenses associated with investigating, correcting, and preventing fraud."⁷⁶²

The credit unions asserted that Camp's was liable due to their failure to adequately train employees and their oversight in implementing reasonable cybersecurity controls such as intrusion detection systems and encryption.⁷⁶³

In turn, Camp's sought a declaratory judgment against State Farm for the insurer to defend and indemnify them under their general liability insurance policy for the case brought by the credit unions.⁷⁶⁴

Camp's right to coverage for the claim by the credit unions ultimately hinged upon the differences between first- and third-party coverage in an insurance policy. In its holding, the court noted: "Insurance contracts generally are assigned to one of two classes: either 'first-party coverage' or 'third-party coverage'.... 'First-party coverage' pertains to loss or damage sustained by an insured to its property; the insured receives the proceeds when the damage occurs. ... In contrast, if the insurer's duty to defend and pay runs to a third-party claimant who is paid according to a judgment or settlement against the insured, then the insurance is classified as 'third-party insurance.' ... Thus, wholly different interests are protected by first-party coverage and third-party coverage."⁷⁶⁵

Going on to note: "[T]here is no language in [the policy] whereby State Farm promises to 'defend' or 'indemnify' the insured whether in regard to claims involving computer equipment, electronic data, or anything else, for that matter."⁷⁶⁶ In short, Camp's had no coverage for third-party cyber-related claims.

Action Items:

- ☐ Understand the difference between first- and third-party coverages in cyber insurance policies;
- ☐ Run coverage scenarios with various stakeholders to assess reasonable coverage options and limits for the business's relevant insurance policies. Legal counsel and a competent broker may be able to assist with this exercise;
- ☐ Update the business's incident response plan and other internal documents as necessary to reflect the coverages found in the business's cyber policy.

Deductible/Retention Options

Unsurprisingly, increasing the deductible or retention will often lower the cost of the premium. While this makes the premium more immediately palatable, it does have potentially negative consequences.

Foremost among these is the issue of the sublimits within the policy. Excessively high deductibles or retentions could render various sublimits effectively useless within the policy. For example, if the business elects to have a \$50,000 deductible, a \$50,000 sublimit for cybercrime could be effectively useless for most businesses that are only wiring small amounts of money.

Also, consider that a business could be subjected to multiple, unrelated data-breach events covered under their cyber policy in each policy period. Thus, excessively high deductibles could result in a severe financial burden if those deductibles or retentions must be paid out for every cyber claim reported to the insurer.

Ultimately, cyber insurance is still relatively inexpensive when compared to other lines of insurance. Holding unnecessarily high deductibles or retentions could lead to a “penny wise, pound foolish” scenario. Businesses should take the above factors into consideration when weighing deductible or retention options. Practically speaking, businesses are often better served by considering deductibles or retentions that are lower than those they would find on their other insurance policies.

Action Items:

- ☐ Consider obtaining the lowest possible deductible/retention available given financial constraints;
- ☐ Understand how the deductible/retention works in the policy.
- ☐ Communicate this data to relevant stakeholders, so they understand the immediate costs of a breach.

Overlapping Coverage, Other Insurance Clauses, and Multiple Deductibles

Depending on the insurer and type of policy, a relatively small cyber insurance endorsement may be automatically included at little to no extra cost. For small businesses, this is generally not a problem as they welcome the additional coverage without the added necessity of researching and procuring a standalone cyber policy. For businesses that require a dedicated cyber policy, having overlapping coverage in both an attached endorsement and their separate cyber policy can result in unintended consequences.

Many cyber insurance policies contain an “Other Insurance” clause like the one below:

“Any payment due under this policy is specifically excess of and will not contribute with any other valid and collectible insurance unless such other insurance is specifically written as excess insurance over the limit of liability of this policy. However, with respect to **breach costs** only, this policy will be primary.”⁷⁶⁷

Likewise, a professional liability policy may contain a similar, “Other Insurance” clauses such as:

“This Policy will apply only as excess over any other valid and collectible insurance, whether primary, contributory, excess, contingent or otherwise, unless such other insurance is written only as specific excess insurance over the Limit of Liability provided by this Policy. This Policy will also be specifically excess over any other valid and collectible insurance pursuant to which any other insurer has a duty to defend a claim for which this Policy may be obligated to pay loss.”⁷⁶⁸

The original rationale behind these clauses was to avoid moral hazards in the overpayment to the insured, control the contribution to the loss, and prevent fraudulent claim recoveries.⁷⁶⁹ Yet when reading the above, it would appear that both policies would be considered excess to the other. Thus, each insurer would attempt to escape its duty to provide coverage for a claim. This would leave the policyholder with no coverage due to the infighting between two insurers.⁷⁷⁰

Thankfully, the courts have recognized that this would be unfair to those who purchased the insurance and have attempted to hold insurance companies responsible for providing coverage. Generally, where other insurance clauses are conflicting, the

clauses can be deemed to be mutually repugnant, and each will prorate their payments for the loss. When the other insurance clauses do not conflict, the other insurance clauses are enforceable in their prioritization.⁷⁷¹

While businesses are generally elated to know that they will not be left uninsured due to the often-unforeseen policy language complications, they are typically not so elated to pay their deductible. If more than one insurer was attached to the claim, a business may end up paying part, or the entirety, of multiple deductibles. To the insured business, it would seem fair that only one deductible should be paid; and often the smaller of those in question. After all, only one claim occurred. From the eyes of the insurers paying out losses, they each accepted the risk at a specified premium, with the understanding that a deductible would be paid to them in the event of a claim.

Naturally, this leads to a quagmire of possibilities such as the following:

- Should one of the insurers receive no deductible payment?
- Should the insured pay only one deductible, and if so, which one and why?
- Should the insured be required to pay each deductible, thereby increasing their in-house exposure for a larger figure than they had bargained for when procuring the insurance?
- Perhaps the insurers should determine what percentage of the claim each paid and then apply that percentage the insured's deductible?

Courts have long struggled with how to remedy this intractable problem of fairness. Each party can extend reasonably weighted arguments as to why their position should be supported. Unfortunately for the inquisitive business owner attempting to plan for a scenario where multiple insurance companies could be involved with a data breach claim, there does not appear to be a definitive answer. Courts have come to wildly different conclusions for seemingly sound reasons. Whether the court would look favorably upon the insured or the insurers is likely only discoverable through litigation.⁷⁷²

For these reasons, businesses should be reasonably prepared for the possibility of paying multiple deductibles if more than one insurer is involved in a data-breach-related claim. In addition, businesses should not take on unreasonably large deductibles across multiple policies, that when combined, could result in severe financial difficulties if they need to be paid simultaneously.

As an aside, the above policy language examples included two “excess” other insurance clauses. Depending on the policy, other types of other insurance clauses exist, such as pro-rata, and escape clauses.⁷⁷³ Combinations of these clauses will

result in unique arrangements not covered in this section. Businesses should work with their legal counsel to determine how other insurance clauses will affect their situation.

Action Items:

- ☐ Work with legal counsel or a knowledgeable broker to determine what policy coverage overlaps may result in multiple deductible payments;
- ☐ Speak with stakeholders about this issue and consider if your money reserves are enough to withstand multiple deductibles being paid simultaneously.

Sublimits, Policy Structure, and Appropriate Limits

Due to the general lack of expertise in the market concerning placing appropriate cyber insurance, businesses will need to investigate all sublimits within their policy. Often these sublimits may cover aspects that would be crucial to the business given an internal breach or a breach at a crucial vendor. Policies offered across the market vary greatly in their structure, available sublimits, and policy language. Certain sublimits may not have a deductible, or the sublimit applies after the deductible is met.

Should businesses fail to fully investigate a cyber insurance policy considering their own unique circumstances, they could find themselves woefully underinsured, or not insured at all, for the presented risk. Even insurance brokers, or wholesalers, that market themselves as “cyber insurance experts” may not have the technical knowledge or inherent knowledge of the business’s risks to place an appropriate policy.

Consider the following allegations made by Hotel Monteleone in the case of *New Hotel Monteleone, LLC. v. Certain Underwriters at Lloyd’s of London and Eustis Insurance, Inc.*

In 2013, Monteleone experienced a breach that resulted in the loss of payment card numbers. Following the breach, Monteleone was assessed \$471,000 and \$377,000 by Mastercard and Visa for initial fraud recovery and operational reimbursement costs. At the time, they had no insurance policy in place that would cover these losses.⁷⁷⁴

Following the breach, Hotel Monteleone reached out to Eustis Insurance, Inc., an independent insurance agency. The hotel requested a cyber insurance policy that would provide coverage for similar expenses should a breach occur in the future.⁷⁷⁵

As stated by Hotel Monteleone in the court documents, Eustis had no expertise in procuring or placing cyber insurance policies. As such, Eustis reached out to R-T Specialty, a wholesale insurance broker to assist in the placement.⁷⁷⁶

At the time, R-T Specialty’s website included a paragraph on their cyber insurance expertise by stating the following:

“It’s particularly important for insurance professionals to help their clients identify potential cyber exposures and to select the appropriate cyber liability product to fit their client’s needs. ... [W]e understand the importance of cyber liability products for our clients, and have assembled a cyber “team” of brokers whose primary focus is Cyber Liability and Technology Errors & Omissions coverage.

Members of our cyber team are constantly evaluating new cyber insurance products and will work together with retail partners to find the best fit for each client.”⁷⁷⁷

Ultimately, Hotel Monteleone purchased an Ascent CyberPro Insurance Policy with \$3 million limits for approximately \$20,277. Within their policy, Ascent had added an endorsement titled, “Payment Card Industry Fines, or Penalties Endorsement.” Crucial to that endorsement was the following language:⁷⁷⁸

27. The 2014 CyberPro Insurance Policy provides:

We shall pay on your behalf Payment Card Industry fines or penalties in excess of your deductible as stated within item 4 of the Declarations, which you become legally obligated to pay as a result of any **claim** first made against you and notified by you to us in writing, in accordance with Section XI of this policy, during the **policy period** or any **extended reporting period**, if applicable, arising solely from a **privacy event**, or **security event**.

It is agreed that Section **VII. DEFINITIONS**, is amended to include the following additional definitions:

Payment Card Industry fines or penalties means a written demand received by you by a **credit card association** for a monetary fine or penalty because of your non-compliance with **Payment Card Industry Data Security Standards**.

Credit card association means Visa, MasterCard, American Express, Discover, or JCB.

Payment Card Industry Data Security Standards means published and generally accepted security standards for the Payment Card Industry.

Unfortunately for the hotel, they would suffer another security breach shortly thereafter that allegedly compromised payment card numbers.⁷⁷⁹

Within the policy, the suit alleges that the endorsement only provided \$200,000 in total coverage. This amount was insufficient to cover the total losses anticipated by the hotel with their new breach. Furthermore, the endorsement did not apply to reimbursements, fraud recoveries, or assessments owed to the payment card processors.

As stated in their claim, these were the costs that the hotel had specifically requested be covered if another breach of their payment system occurred. According to Hotel Monteleone, Eustis had “told [them] that the 2014 CyberPro Insurance

Policy would provide full coverage for losses in the form of fraud recovery, operational reimbursement, and case management fees.”⁷⁸⁰

The hotel made various claims in their suit to have coverage afforded by other elements of the policy. Whether these claims would have been successful is speculative. The court ordered that the claims made by Hotel Monteleone against Eustis were stayed while the hotel and the insurance company arbitrated their dispute.⁷⁸¹

Regardless, businesses need to be diligent regarding the investigation of their own sublimits and coverage offerings. While courts will generally construe ambiguous language in favor of the insured, a “plain language” reading of the policy terms will often favor the insurer. When hundreds of thousands, or millions, of dollars are on the line, businesses should be very wary of placing their financial wellbeing in the hands of any self-described “cyber insurance expert.”

Action Items:

- ☐ Understand how the policy is structured and what sublimits are available;
- ☐ Work with a competent broker and legal counsel to ensure that coverage is afforded for the risks facing the business. Never assume anything is covered unless you have confirmed the coverage in writing;
- ☐ Communicate this coverage data to relevant stakeholders;
- ☐ Update the business’s incident response plan and other internal documents as necessary.

Choice of Law Provisions

If a business finds itself in a dispute with their insurer, those disputes are generally governed by state law. Businesses should be aware state laws can vary greatly, with some state laws being more “friendly” to the insured than the insurer. These seemingly minor differences can ultimately mean the difference in a business being afforded or denied coverage.

For example, in Texas, an insurer is not generally required to show prejudice from a late notice involving a claims-made policy.⁷⁸² By comparison, under most jurisdictions, a late notice of a claim does not absolve the insurer of its duties unless the insurer can prove that they were somehow prejudiced as a result of that late notice.⁷⁸³

Thus, businesses should understand what state laws would apply given a coverage dispute with their insurer. Some businesses may be able to negotiate the dispute venue, but practically speaking, such policy changes will often be based on the premium available to the insurer and the risk profile of the insured. If a business is considering a change to the venue where a dispute would be litigated, they should work closely with legal counsel to determine which state is most appropriate.⁷⁸⁴

Action Items:

- ☐ Determine if the choice of law provisions and venues are appropriate for your business;
- ☐ Communicate this data to relevant stakeholders;
- ☐ If in doubt, work with legal counsel to determine an appropriate dispute venue and work with your broker to determine if the insurer will change the venue.

Damage Control

Selecting Limits

Outside of selecting the correct coverage options and policy language, the most daunting task for most businesses is deciding policy limits. The most common threats to businesses are, in order: being underinsured in total, underinsured in part, uninsured in part, or not insured at all.

Being over-insured is generally not a concern at the moment. This is because the term “over-insured” generally refers to excessive insurance limits, which are discoverable to a plaintiff when a claim occurs. As discussed previously, the threat of a third-party data-breach-related claim is rare. Therefore, businesses should generally look at understanding their total first-party costs when considering cyber insurance limits.

A passing glance at the common statistics being thrown around most websites and conferences is unhelpful. Frequently, businesses will hear the Ponemon Institute statistics stating that the average cost of a data breach was \$3.86 million, and the average cost per lost or stolen record was \$148. Logically, this is absurd. Averages are not applicable to any half of a population set. Furthermore, those averages are based upon breaches of large, global companies across different industries that hold different types of information.⁷⁸⁵ This does not invalidate the study but is meant to suggest that such a sample set is inappropriate for all but the largest businesses.

Armed with the information presented in this book, businesses should consider the following, minimum elements when determining their insurance needs:

- Determine the number of unique records containing PII/PHI/PCI. Businesses often overlook payroll services, dependents of employees, and pass-through entities when making this calculation. Understand that a “record” in insurance parlance can roughly be translated to how many breach notification letters might go out the door following a breach. For example, if a tax preparer performed a tax return for a single individual for 10 years, and his social security and driver’s license were stolen, that could count as one record. If that same individual were to have a wife and two children, and 10 years’ worth of returns was likewise stolen, that could count as four records.
- Determine what possible third-party exposure may exist within the business. As stated previously, it is unlikely that most businesses will be subject to a private right of action or a class-action claim following a data breach, specific state allowance for these lawsuits notwithstanding. However, a business may face state and/or federal regulatory inquiries, demands arising from their

merchant services agreement (MSA) following a breach, or any other unique exposure that is business dependent.

- Determine how crucial first- and third-party exposures are limited or sub-limited in the policy. Make certain that the limits and sublimits are appropriate for the exposures the business could reasonably face.
- What is the business's network architecture?
- Are vendors contractually obligated to indemnify the business following a breach?
- What regulatory regimes do the business fall under?
- Does the business have access to client funds?
- What are the terms of the business's MSA and maximum exposure therein?
- Could the business be fooled into transferring business funds to unknown third parties?

Benchmarking insurance limits against businesses with similar revenue will not necessarily provide adequate protection as each business has its own unique exposures. For example, a \$50-million-grossing accounting firm in Washington D.C. that specializes in individual tax returns for high net worth clients has a very different exposure when compared to a \$50-million-grossing bank in Kansas that focuses heavily agricultural lending.

When calculating appropriate limits, the D.C. firm is more likely to consider breach notification and client loss to be a leading driver of limit adequacy, followed by state/federal regulatory inquiries. The Kansas bank is more likely to consider regulatory inquiries and wire fraud to be the leading driver of limit adequacy.

The cost of a breach varies greatly, and often for reasons that are entirely outside the control of the business. In addition, new exposures may arise that are outside the purview of businesses not keeping the pulse of the ever-changing cybersecurity law and insurance landscape. For these reasons, businesses are advised to work with a knowledgeable broker, if available, and competent legal counsel to adequately insure for their exposures.

Action Items:

- ☐ Determine what information the business is responsible for given a breach; PII/PHI/PCI, intellectual property, etc.;

- ☐ Estimate the unique number of records that could be breached for each category;
- ☐ Work with a knowledgeable broker and competent legal counsel to review necessary limits and sublimits;
- ☐ Reference numerous sources that benchmark data-breach costs including, but not limited to, NetDiligence, The Ponemon Institute, and Verizon studies;
- ☐ Communicate this data to relevant stakeholders;
- ☐ Update the business's incident response plan and other internal documents as necessary;
- ☐ Stay abreast of any new exposures that may arise as the legal landscape changes;
- ☐ Review the business's cyber insurance offerings each year to determine if it still adequately covers the risks identified by the business to the dollar amount necessary;
- ☐ When in doubt, consider selecting higher limits and sublimits.

Common Coverage Options

First-Party Coverage Options

As mentioned previously, first-party costs would be those costs that a business would otherwise directly incur as a result of a covered event. Businesses should note that the following is a list of features that are commonly found across multiple, cyber insurance policies. Not all cyber policies will carry every feature listed below, nor are they all necessarily relevant for each business. Furthermore, policy nomenclature will vary – similar coverages across different policies may be referred to by different names. Even policies utilizing similar nomenclature may provide radically different coverages. Businesses will also need to check any exclusions, carve-backs, or other policy language elements to make a reasonable internal coverage assessment.

Business Interruption: This category of coverage is generally meant to cover the income loss and extra expenses incurred by the business during a breach of their computer system. Income losses are generally understood to mean the net losses that would not have occurred but for the event. Extra expenses are generally understood to mean the additional costs a business would incur to utilize alternative sources to meet contractual obligations as well as the additional cost of employee labor during the event.

Policies will often contain several exclusions related to the business interruption, and those exclusions vary greatly by policy. Additionally, most policies will contain a waiting period, a loss-of-use threshold, and a retention/deductible before the business interruption sublimit reimbursement clause will become effective.

For example, a policy may state that the \$500,000 business interruption sublimit will not be available until the business has greater than 25% of its computer systems inoperable for more than eight hours. After this, the \$500,000 business interruption sublimit will be made available subject to the \$5,000 retention to be paid by the business. Often a policy will specify how many days a business can be reimbursed.

Most policies covering business interruption reimbursement will stipulate that the waiting period will begin when the matter is first reported to the insurance company. Certain policies may contain an appraisal clause allowing for an independent, third-party appraiser to provide a reasonable loss estimate to both parties. Seasonal work may or may not be considered for reimbursement.

Cryptojacking: This coverage comes into play when a business has had their computer systems accessed by a third party to mine for digital currency. As a result

of this intrusion, the business may experience additional costs from its electricity, natural gas, oil, or Internet providers. If a cryptojacking event were to befall a business, this sublimit would reimburse for those additional billing costs.

Coverage for cryptojacking claims will likely need to be specifically named in the policy for coverage for apply, though coverage may circumstantially be found in a utility-fraud-type coverage.

Push Payment Fraud: Such as coverage would allow the business to be reimbursed for the various costs surrounding push payments. This could include the cost of advising clients of the fraud, reimbursing clients for the financial losses incurred, or income losses sustained by the business because of the fraud.

Dependent Business Interruption: This coverage would generally reimburse a business for lost revenue if one of their service providers experiences a breach event or service interruption event. A service interruption is often defined as an unplanned outage due to a software or hardware error. Typically, service providers are limited to “cloud providers,” IT-service providers, or supporting operations such as a fulfillment center. On many policies, these entities must be specifically named for coverage to apply.

Generally, insurance companies are unaware of the security or business practices of these third parties. Thus, dependent business interruption coverage often comes with smaller sublimits that are subject to a deductible or retention. There may also be a long list of exclusions that apply to this coverage.

System Failure Business Interruption: Whereas the previous coverage dealt with service providers, this coverage deals with a system failure within the business proper. Generally, this coverage would provide coverage for an unintentional interruption of the business’s computer systems due to an internal error. It does not cover the business interruption costs due to a breach-like event.

Despite the best intentions of software vendors, their updates and patches do not always integrate seamlessly. There is a possibility with any changes to a functioning system that the system will be negatively impacted in a way that was totally unforeseen. This could also happen after otherwise well-meaning internal tech staff alter settings that crash the network and make recovery time-consuming.

Utility Fraud: This policy element would allow the business to be insured against the increased expenses for various utility payments. Generally, these increased expenses must come as a result of some unauthorized access to the business’s computer system to include cryptojacking and telephone-toll fraud.

Legal Costs: This allows for the payment of the assigned attorney to perform most or all the necessary functions when responding to a breach. Such functions could include providing advice regarding the breach investigation, assisting with notifications of regulators and affected individuals, as well as pursuing indemnification rights under a written agreement with a third party. The legal costs to advise the business in compliance with a PCI DSS-related matter may also be covered.

Computer Forensics Costs: This assists in paying for the computer forensic contractor to determine the scope and nature of the breach. It may also cover the costs to stop the further propagation of malware. The forensics report will often be necessary for determining what individuals require breach notification letters, as well as for reports to local, state, and federal law enforcement, if necessary. Generally, this coverage is limited to a breach of the business's system, so would not necessarily be activated if, for example, a staff member fell victim to a social engineering scheme and wired money due a fraudulent phone call.

Customers' Accounts / Invoice Manipulation Coverage: This type of coverage would be afforded if the business's computer system was intentionally used by an unauthorized third party to deceive a client or vendor into transferring money intended for the business to a different entity.

Notification Costs: This pays for the breach notification letter to be drafted and sent to the affected parties as required by the various breach notification laws previously discussed. It should also cover the costs for alternative notification methods such as a notice on a website or via news outlets to be utilized if warranted. Certain policies will also allow for voluntary notification under certain circumstances, such as the business displaying that such action would mitigate a significant risk to those affected.

Identity Protection Services: Generally, this provides up to one year of credit- or identity-monitoring programs to those affected by the breach. Certain states may require greater than one year of services to be provided, so businesses will want to check the policy for this possibility. Additionally, this coverage may also provide for clients to access identity protection training services.

Businesses should be aware that offering identity protection or remediation services such as credit monitoring, fraud assistance, and identity theft insurance is not without risks.

In the case of *Remijas v. Neiman Marcus Group, LLC*, the US Court of Appeals for the Seventh Circuit noted that the offer of free credit monitoring following a

breach was an admission of possible harm to the plaintiffs. Thus, it supported the plaintiff's standing in their lawsuit.⁷⁸⁶

Conversely, the US Court of Appeals for the Fourth Circuit refused to follow the Seventh Circuit's holding in the case of *Beck v. McDonald*. This court held that adopting a standard where the offer of free credit monitoring inferred a substantial risk of future harm would unduly discourage companies from offering credit monitoring services in the future.⁷⁸⁷

The consensus following a breach is to provide credit monitoring as a gesture of goodwill on behalf of the breached business, but make sure you consult with legal counsel first.

Crisis Management Services: Crisis managers would assist with the cost for consultants to assist the business following a breach. Typical duties would include reducing the likelihood of a claim, reestablishing the business's reputation, attempting to identify the hacker, and assistance with identifying future security improvements.

Public Relations Services: Often working alongside the crisis managers, the public relations providers assist businesses when there is a current or imminent publication of a covered event. Often this could be a report of the breach in local, regional, or national news. The public relations expert can assist the business in dealing with press releases and inquiries from the media to lessen reputational harm and potentially limit further liability.

Damage and Data Restoration: Should malware infect, corrupt, or damage your files or computer system, those items may need to be restored or corrected. Generally, this coverage allows for the reasonable costs and expenses necessary to regain access to the data, as well as the costs to replace, restore, or restore data to the state it was prior to the event. Often this will be done with backups or original sources, so businesses should check on their own backups' periodicity and security to determine whether the required backups are truly secure and available.

Call Center: Often overlooked by businesses is the need for a call center following a breach. The call center can be provided as a point of contact for clients who receive breach notification letters. Such a service can greatly assist businesses who would be unlikely to have the resources to handle thousands of clients demanding to speak with a representative of the business's management in the space of a few days.

Rogue Employees: Many cyber insurance policies will deny coverage if an extortion event was perpetrated by anyone insured under the policy. Coverage for

rogue employees can cover the business if an employee threatens to attack the business's computer system, disclose secret corporate information, or disclose PII unless a ransom is paid.

Cyber Extortion Costs: An extortion threat would most commonly be seen in a ransomware event. However, it can generally be any threat from a third party to disclose confidential client information if money is not paid to the third party. Some policies will also reimburse the business for the ransom paid to the hacker and any reasonable expenses incurred by a representative appointed by the insurance company to assist with the process. For example, a digital currency paid to the hacker with the promise that they will give you the key to unencrypt their data.

When contemplating cyber extortion, businesses should check the definition of a hacker in its relation to an extortion event. Some insurers will amend policy language to include extortion attempts from rogue employees; others will specifically exclude it. Given the damaging nature of insider threats and the vast amounts of PII at their disposal, such a threat should be considered when investigating insurance coverage.

Media Liability: This often-overlooked coverage should warrant consideration for any business operating a website or various social media accounts. Media liability coverage can roughly be understood to cover claims of libel, slander, or defamation claims that result from content published on a business's websites or social media accounts. Certain policies may also cover plagiarism, copyright infringement, trademark infringement, breach of license, and negligent publication.

Cyber Crime and Social Engineering: Of all the coverages to be assessed by a business, this coverage is the most likely to bring confusion. Depending on the policy, coverage may or may not be afforded to losses incurred by the business's own accounts, or to clients' accounts. Whether there is coverage for a social engineering scam or if the business's computer must have been compromised also varies by policy.

In certain policies, coverage may only be afforded to losses that are attributed to the staff member who was authorized to transfer funds. Other policies may include coverage only for funds lost from a business's transfer account. Some policies make no such distinctions and thus are open to interpretation by the insurer. Due to such wild variations in coverage, businesses are encouraged to read the relevant policy language in detail. Utilizing the "wargaming" scenarios found later in this book may also be useful.

Reputation Loss / Reputation Harm: Following a breach, there is a chance that the business's breach may be featured in an adverse publication. Certain policies will

reimburse the business for net losses in revenue incurred by the publication of the breach. Businesses should note that the policies offering this coverage have lengthy requirements on how the reimbursement will be calculated, as well as various waiting periods before the coverage will come into play.

Bricking: “Bricking” occurs when a piece of hardware is rendered unusable by re-writing or overwriting the firmware of the device. In effect, this makes the device inaccessible at the most fundamental levels. Such an event could result in untold monetary damage to the business. This coverage would rebuild, repair, or replace the hardware to the same level as before the event if a bricking incident were to occur. Conceivably, a hacker could brick the hardware of a business if, for example, they were using that hardware for identity theft or cryptojacking.

Coverage for bricking is currently rare but may be found as a distinct coverage or may be included under the system-failure coverage feature.

Customer Accounts and Invoice Manipulation: If the business’s computer system was used to deceive a client or vendor into transferring money to a fraudulent account, this coverage may apply. This could come into play if a business’s system was compromised, and clients were directed to pay money to a fake account purportedly owned by the business. This coverage is often strictly sub limited.

Extra Expenses: When a breach occurs, it may be necessary for the business to pay staff overtime to return to normal operation, employ contract staff, or source products or services from a different vendor to meet various contractual obligations. The extra-expenses coverage can help reimburse the business for those costs.

Voluntary Shutdown Coverage: At its core, this is a type of business interruption reimbursement coverage. When malware attacks the business, one of the suggested courses of immediate action may be to shut the system down to limit how far it can spread. In certain circumstances, law enforcement authorities may also request the business shut down its computer system to limit collateral damage. By shutting down the system, this could halt part, or all, of the business from generating revenue. This business-interruption reimbursement coverage is also often sub-limited.

1st Party Bodily Injury and Property Damage: This coverage can generally be understood to cover two elements. The first would be for losses the business incurs following a cyber event that results in bodily injury, sickness, disease, or death of a person. The second element would cover the business for losses incurred due to the damage, injury to, or destruction of actual property.

In 2015, a German steel mill had various logins stolen which gave the hackers access to the mill's control system. This resulted in parts of the mill failing and millions in damage done to the blast furnace when it was not properly shut down.⁷⁸⁸ If the German had this type of coverage, they could have covered for their property damage. If any employees had been injured as a result of the breach, this may have also been covered by a cyber insurance policy with this type of coverage.

TRIA/TRIPRA: The Terrorism Risk Insurance Act (TRIA), later reauthorized under the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA) of 2015, extends coverage for insurance related to certified acts of terror. For this coverage to apply, the act of terrorism must be certified by the Secretary of the Treasury, in concurrence with the Secretary of State and the Attorney General. Following certification, and assuming the act is covered under the policy, the government may reimburse the insurance company for losses paid to the business under a federally mandated formula. Most insurers will add this coverage automatically unless the business declines the coverage via an attached form.

As businesses investigate the various first-party coverage options, they should understand exactly what the policy language would reasonably cover, and what it would not. Depending on the insurer, some of the above coverages may overlap into single coverage elements or may not be included at all. Failure to investigate and understand coverage features can lead to an easy declination by the insurer. Be educated and prepared.

Third-Party Coverage Options

PCI DSS: Following a breach of a business's payment card system, there is a litany of mandatory fees that may apply on behalf of the business. Generally, PCI DSS coverage would pay those amounts which the business is legally obligated to pay under their merchant services agreement (MSA). This could include penalties for non-compliance, monetary expenses, and the cost of an audit to display PCI DSS compliance before payment cards can again be used.

Private Rights of Action: Many policies will also cover the defense and claim expenses if an affected individual party were to bring a claim against the business following a covered breach.

Regulatory Proceedings Fines and Penalties: This feature would cover the request for information, civil demand, or civil proceedings brought by a federal, state, or local government entity. Depending on the policy, foreign governmental entities may or may not be covered. Generally, the cyber policy will be a duty and right to defend. Many policies will also cover the fines, penalties, and assessments levied

against the business following regulatory proceedings. Readers are encouraged to reference the included chapter, which contains a greater discussion on the insurability of regulatory claims.

3rd Party Bodily Injury and Property Damage: This coverage is roughly analogous to the prior mentioned 1st Party Bodily Injury and Property Damage coverage, in that it covers losses the business incurs following a cyber event that results in bodily injury, sickness, disease, or death of a person. It can also cover the business for losses incurred due to the damage, injury to, or destruction of actual property. However, it is meant to cover the physical losses incurred by third parties that would bring a claim against a business.

For example, in 2008, a Polish teenager hacked his city's tram system. This was accomplished after he studied the city's rail lines for months and then converted an old TV remote's infrared transmitter into tripping the switches. Ultimately, he redirected numerous trains, derailed four trams, and injured roughly a dozen people.⁷⁸⁹ If the tram system had been sued by the injured passengers, this type of coverage could have responded.

GDPR: This is a relatively new coverage that deals with the European Union's General Data Privacy Regulation (2016/679). This policy provision can cover the defense costs from responding to a GDPR violation and possibly fines, penalties, and assessments that may arise as a result of such actions. If GDPR coverage is required by the business but not explicitly mentioned by the policy, businesses should consult the definitions and exclusions dealing with regulatory bodies. Often those definitions will only cover U.S.-based regulators.

CCPA: Coverage for a California Consumer Privacy Act of 2018 (CCPA) claim may be naturally included in some cyber policies as a general regulatory proceeding. However, certain businesses may request or require an affirmative declaration of CCPA coverage. In this case, policies from various insurers will either include this coverage in various definitions or will be explicitly listed as an endorsement. Whether any fines or penalties that arise from CCPA related actions are insurable is yet to be determined.

Criminal Reward Payments: Included in some policies is a small sublimit to encourage the arrest and conviction of the hacker that infiltrated the business's system. For this coverage to apply, the information leading to the arrest and conviction must not have come from information provided by the business or the business's auditors or other hired individuals.

Action Items:

- ☐ Determine what coverage options are appropriate and necessary for your business.
- ☐ Seek competent legal assistance to assist with any questions.
- ☐ Stay abreast of additional coverage features afforded in the marketplace that may prove beneficial to your business.
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary.

Common Coverage Exclusions

Exclusions serve the purpose of limiting or clarifying the coverage afforded elsewhere in the policy. Generally, exclusions listed will be those not directly related to cyber-type or data-breach losses. They can also include first-party coverages found in other insurer's policies, but not those found in the policy being reviewed. Businesses should be advised when comparing policy exclusions that doing so will be a tedious process. As one study of over 130 different cyber insurance policies noted: "parsing out the nuances in the policies can be a challenge: exclusions include exceptions that have their own exceptions buried in them."⁷⁹⁰

Intentional Misconduct: Naturally, businesses are not going to be covered for intentionally committing criminal or fraudulent acts. However, there could be a circumstance where a staff member intentionally exposes covered data for nefarious purposes. In a circumstance such as this, many policies generally allow for coverage until an adjudication of some type has concluded that the conduct was intentional. Many policies also contain an innocent-insured type provision where those who did not personally commit or know about the act would still be covered under the policy. How coverage will ultimately be decided may be settled on a case-by-case basis and dependent on policy language.⁷⁹¹

Bodily Injury or Property Damage: Unless otherwise explicitly added as a policy feature, cyber policies tend to exclude coverage based upon any allegation of bodily injury or property damage. This is logical in that those types of claims should generally fall under a general liability policy. As such an exclusion would pertain to a common trip-and-fall accident, this is understandable. However, in industries where a computer error could lead to bodily injury or property damage, such as for a manufacturer, clarification on the exclusion, as well as the need for a potential manuscript endorsement to cover such potential claims, may be warranted.

Employment-Related Claims: Generally, this exclusion would cover claims that would otherwise be covered under an employment practices liability insurance policy. Examples would include sexual harassment, failure to promote, wrongful termination, and various labor law violations.

Portable Electronic Devices: Some policies may contain an exclusion for any claim that arises as a result of a lost portable electronic device, often a laptop or tablet. Given the large amount of losses that occur from portable electronic devices, businesses should be wary of this exclusion.

Patent, Software, or Copyright Infringement: These types of claims would generally be covered under intellectual property (IP) insurance policy. The exclusion broadly covers the misuse or infringement of patented or copyrighted material. Additionally, this exclusion would bar coverage for the theft or misappropriation of ideas and trade secrets by the insured.

Failure to Follow Required Security Practices: Though becoming rarer, this exclusion denies coverage if a breach results from a failure to adhere to required security practices. Such clauses can still be found on many legacy cyber policies and should be avoided.

Failure to Follow Reasonable Security Measures: Also becoming rare, but this exclusion could eliminate coverage for a business if a loss resulted in a shortcoming in security that they should have known about. Such a broad exclusion can be extremely detrimental to a business's ability to rely on its cyber insurance policy following a breach. It would be too easy for an insurer to argue that a business should have enacted and monitored any number of security measures that could have prevented a breach. Such clauses should be avoided.

Material Misrepresentations: This is not an exclusion, per se, but rather a policy condition. If the business committed fraud or state material misrepresentations in their application, the insurer could have grounds to cancel coverage.

Violations of Specified Laws: Often, these laws will be specifically listed. Frequently included would be violations of the Securities Act of 1933, SEC Act of 1934, state or "blue sky" security laws, Employee Retirement Income Security Act of 1974, Racketeer Influenced and Corrupt Organizations Act, and other similar laws.

Payment Cards: Cyber policies generally do not cover the losses from the use of business owned credit or debit cards. If fraud occurs on a personal payment card, consumer protections may be available. Whether fraud occurring on a business credit card is covered may be situationally and policy dependent. Therefore, it should be investigated by the business in conjunction with their payment card provider.

Acts of God: Damages arising from fires, floods, earthquakes, volcanic eruptions, hail, wind, landslides, and similar disasters would not be covered.

Acts of War: Invasions, war, warlike hostilities, operations, rebellions, civil war, insurrections, terrorism, and the like, will not be covered. However, this exclusion can be modified to carve back coverage for general cyber-terrorism-related acts.

Pollution: Any claims dealing with the discharge of pollutants, or costs associated with the cleanup of those pollutants will not be covered.

Ultimately, businesses need to investigate the exclusions within their own current or proposed policy(s). The lists of exclusion – often with their own internal exclusion – can frequently run for a dozen pages or more. While the above were general exclusions found in many policies, each insurer has its own unique policy language that can further be affected by various endorsements to the policy.

Action Items:

- ☐ Understand what policy exclusions are present and how they may impact the business decisions and internal controls of the business;
- ☐ If in doubt, work with competent legal counsel to make reasonable determinations of policy language;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan and other internal documents as necessary.

Simplifying Coverage Assessments with Wargaming

Due to the non-standard nature of cyber policy coverage, it may be best for a business to “wargame” scenarios when assessing coverage. When doing so, it is best that all stakeholders, including partners, shareholders, brokers/agents, IT, legal, and HR are present. This would better allow the business to make a reasonable assessment of coverage before the policy is needed. Below are examples that can aid as a starting point for discussing coverage. Businesses should create their own series of questions tailored to their own needs taking note of all relevant policy coverages and exclusions. As discussed in previous chapters, depending on the scenario, coverage may be found in multiple policies, single policies, or is uninsured or uninsurable.

General Questions

- What the retroactive date of this policy?
- Does the policy cover the necessary-named insureds, including seasonal workers, temporary employees, and subcontractors, if necessary?
- Is the policy admitted or surplus lines?
- How adept is my broker in assisting with my cyber-related questions?
- How adept in the insurer in dealing with cyber-related claims?
- Who are the vendors that must be used following a covered event, and how experienced are they in dealing with covered events?
- Has the business assessed and confirmed the contracts of vendors before a breach has occurred?
- Are there any breach mitigation services being offered by the insurance company?
- Are those breach-mitigation services being used by the appropriate parties?

Ransomware Scenarios

- Does the policy cover cyber extortion attempts?
- Who will pay the ransom?
- What if a current or former employee perpetrated the ransom?

- What are the business interruption reimbursement provisions such as sublimit, waiting period, and retention?
- Will the policy provide for a computer forensics expert to determine the scope and nature of the breach as well as assist in removing the offending malware?
- How will the policy respond if the computer system is damaged by malware?
- Will the policy provide legal counsel well-versed in cyber-related matters to assist in navigating the process as well as notifying relevant authorities?
- If some of the business's clients leave following a publication of the breach leading to a loss of revenue, how will the policy respond?
- Does the policy provide for crisis management and public relations personnel, if necessary?
- How do I demonstrate duress, i.e., evidence of a ransomware event to the insurer?

Breach Scenarios

- Does the policy coverage a breach of my computer system?
- Will the policy provide legal counsel well-versed in cyber-related matters to assist in navigating the process?
- Will the policy provide for a computer forensics expert to determine the scope and nature of the breach as well as assist in removing the offending malware?
- Will the policy assist in notifying relevant authorities?
- Will the policy cover the cost of drafting and mailing breach notification letters to those affected?
- Will the policy provide credit monitoring to those affected? For how long?
- Does the policy provide any other services, such as financial counseling, to those affected?
- How to the policy consider voluntary notifications?
- Does the policy provide for crisis management and public relations personnel, if necessary?
- Will the policy cover the cost of a call center to handle client inquiries following a breach, if necessary?

- How would the policy respond to my network being damaged as a result of the breach?
- If some of the business's clients leave following a publication of the breach leading to a loss of revenue, how will the policy respond?
- Does the policy provide for crisis-management and public-relations personnel, if necessary?
- If the business is investigated and fined by regulatory bodies following the breach, how will the policy respond?
- If the business faces legal action brought by clients following a breach, how will the policy respond?
- Does the policy exclude claims arising from portable electronic devices?

PCI DSS Scenarios

- Does the policy offer coverage for PCI DSS claims?
- Would the policy pay the costs legally obligated by the business's merchant services agreement (MSA)?
- Would the policy cover contractual fines or penalties for PCI DSS non-compliance?
- Will the policy pay for any mandatory audit following a payment card breach to prove PCI DSS compliance?
- Are PCI DSS monetary assessments, operational expenses, card-reissuance fees, fraud-recovery fees, and case-management fees covered?
- Does the policy provide for credit monitoring to those affected by a payment card breach?
- What limits are afforded by the policy regarding the above, and will those reasonably cover the business?

Theft Scenarios

- If an employee is duped into transferring client funds, is that covered?
- If an employee is duped into transferring business funds, is that covered?
- If a rogue employee steals client funds, would the policy cover such a scenario?

- What sublimits and deductibles/retentions are associated with these types of claims?
- Does the policy limit coverage to only those who are authorized in writing to wire funds?
- If an employee uses a company credit card to pay a fraudulent request, how is that considered under the policy?

Regulatory Scenarios

- Which regulatory bodies are most likely to investigate the business?
- Does the policy cover regulatory defense expenses?
- Is the policy a “right and duty to defend” policy?
- Does the policy cover regulatory fines, penalties, and assessments?
- What regulatory bodies does the business fall under?
- What regulatory bodies are covered?
- What regulatory bodies are excluded?
- Does the policy explicitly mention GDPR or CPPA? Does it provide or exclude coverage?
- Would the GDPR or CPPA coverage indemnify the business for fines, penalties, and assessments related to a GDPR regulatory action?

Other Scenarios

- If my cloud provider suffers a breach, will the policy reimburse the business for lost revenue? If so, what are the policy provisions and sublimits?
- If my network goes down due to an error, but it is not a breach, how will the policy respond?
- Does the policy cover GDPR-related actions?
- If my computer system is used for cryptojacking, telephone fraud, or other types of utility fraud, is there coverage under this policy?
- How does the policy respond to bodily injury or property damage arising from a breach?

- If libelous, slanderous, defamatory, or copyrighted/trademarked information is published on my website or social media account, how will the policy respond?
- Does the policy provide for pre-claim or potential-claim assistance?
- How would the policy respond to a professional ethics complaint against the business following a breach?
- How does the policy respond to regulatory proceedings unique to my business's circumstances? (FTC, SEC, GDPR, state-level financial regulators, etc.)
- Does the policy contain coverage for certified acts of terrorism (TRIA)?

Action Items:

- ☐ Conduct tabletop wargaming scenarios with all relevant stakeholders, including IT, legal, HR, and partners;
- ☐ Use this as an opportunity to understand the business's unique insurance needs;
- ☐ Compare these scenarios to the coverage afforded under the business's cyber policy;
- ☐ If gaps in coverage are found, work with the broker to determine if coverage is available at renewal or policy inception;
- ☐ Update the business's incident response plan and other internal documents as necessary.

The Insurability of Fines and Penalties

Federal regulators are increasingly bringing cybersecurity and privacy law actions against businesses. States are enacting privacy and cyber regulations with specific safeguard requirements and remedies for violations. For these reasons, companies are rightfully becoming more sensitive to the multitude of fines and penalties that could be levied against them. Generally, a business will look for coverage akin to “Regulatory Fines and Penalties” as well as defense costs and investigatory expenses to cover these losses in whole, or in part, even if the proceeding is groundless, false, or fraudulent.

First, it is necessary to understand punitive damages. Punitive damages, roughly synonymous with the idea of “fines and penalties” for this discussion, can be generally seen as being awarded to punish the defendant for their wrongdoing. Many cyber insurance policies with coverage for regulatory fines and penalties will include coverage for punitive damages and well as the costs of defense and investigatory expenses. Others may also affirmatively provide coverage for compensatory damages.⁷⁹² Compensatory damages can generally be understood to be money awarded to the plaintiff to compensate them for their loss, such as in a consumer redress fund.

Businesses should be aware that regulatory fines and penalties can arise from various violations. Certain policies may only contain coverage for those claims that arise following a covered breach event. Other policies may also provide coverage for noncompliance with various data security and privacy laws. Often, this coverage is found within policy definitions:

“We will also pay up to the coverage part limit for damages and claim expenses in excess of the retention if the performance of your business operations by you or anyone on your behalf (including your subcontractors, outsourcers, or independent contractors) on or after the retroactive date results in a covered claim against you for any actual or alleged:

1. network security breach;
2. **privacy liability**;

...

Privacy liability means:

1. violation of any privacy law or consumer data protection law protecting against disclosure of personally identifiable information or confidential corporate information; or

2. breach of a common law duty relating to personally identifiable information or confidential corporate information.”⁷⁹³

When considering whether regulatory fines and penalties would be covered, insureds should look first at specific policy language found in a cyber insurance policy. A policy may provide for fines and penalties to be covered “*unless uninsurable*” under the law of the jurisdiction in which the case is heard.

More flexible policy language could include the following language:

“Damages includes punitive damages to the full extent they are *insurable under the law of any applicable jurisdiction that most favors coverage*.”⁷⁹⁴

This latter definition appears to provide greater flexibility for insureds when picking a venue for a case to be heard. However, none of the above would necessarily cover the costs of various injunctive reliefs that a regulator may be empowered to take that would compel a business to take specific actions in order to meet regulatory compliance. Coverage for the additional costs incurred to comply with an injunctive relief is likely to be explicitly excluded from coverage in a cyber insurance policy, though their costs could be sizeable. Businesses should consult legal counsel and work with their insurance broker to procure the most favorable policy language for their circumstances.

Where there is no ambiguity regarding coverages, businesses should consider how potential ruling jurisdictions view the insurability of fines and penalties. Generally, within the United States, coverage for punitive damages is insurable under business and professional type policies of which a cyber insurance policy is presumably included.⁷⁹⁵ More specifically, approximately two-thirds of states consider punitive damages insurable, with various exceptions.⁷⁹⁶ For most jurisdictions, there appears to be no public policy concern with insurance providing for claims-related expenses such as defense costs.⁷⁹⁷

Conversely, the insurability of regulatory fines and penalties may be deemed to be prohibited/uninsurable due to considerations of public policy by the state.⁷⁹⁸ Even if the business’ home state allows for coverage, there are various legal mechanisms by which a business could find itself in a courtroom defending a claim where the law applied is not the law of the state where the business physically resides.⁷⁹⁹

To illustrate this point, consider the following findings held in various courts across the country:

New York

As stated in the case of *Drexel Burnham Lambert Group, Inc. v. Vigilant Insurance Company*: “There is no basis for a finding that a fidelity insurer must indemnify an insured which has incurred criminal fines and civil penalties. That is why, generally, punitive damages are not covered by insurance. “Since punitive damages in New York are awarded as punishment against a defendant and as a warning to others, it is self-evident that it would defeat New York's expressed public policy to permit an insured to avoid the effect of the imposition of punitive damages by passing the burden of payment on to an insurance company.” ... “The sting of criminal penalties is not to be soothed by permitting its payment out of an insurance pool rather than directly by the wrongdoer.”⁸⁰⁰

Texas

The authors were unable to find an instance in Texas law that has opined on the insurability of civil fines following a data breach. However, the Texas Supreme Court may provide guidance as seen in the case of *Fairfield Insurance Company v. Stephens Martin Paving*. In this case, Fairfield brought action against Stephens for a declaratory judgment stating that it owed no duty to indemnify Stephens for exemplary damages stemming from an employee's death. The court held that it was not against public policy for an insurance company to cover punitive damages.⁸⁰¹ More specifically, they stated, “the purpose of exemplary damages may not be achieved by penalizing those who obtain the insurance required by law for the wrongful acts of those who do not.”⁸⁰² However, the court did caution that, “Extreme circumstances may prompt a different analysis. The touchstone is freedom of contract, but strong public policies may compel a serious analysis into whether a court may legitimately bar contracts of insurance for extreme and avoidable conduct that causes injury.”⁸⁰³

Delaware

In the case of *Wilson v. Chem-Solv, Inc.*, Delaware regulators brought action against Chem-Solv for civil penalties. These penalties stemmed from alleged violations of Delaware hazardous waste and anti-pollution laws caused by a fire and explosion.⁸⁰⁴ Here, the court simply stated that “public policy in [Delaware] does not prohibit an insurance policy from covering the civil penalties assessed here.”⁸⁰⁵

California

In the case of *Bullock v. Maryland Casualty Company*, the Court of Appeal for the First District of California articulated a different understanding of insurability and public policy. The court stated, “We do not believe a [business] purchases liability

insurance in the expectation that his or her insurer will pay for the costs of resisting enforcement of such conditions—let alone of complying with them. To impose such an obligation would not only exceed the bounds of an insured's reasonable expectations but would offend public policy by encouraging [businesses] and others to defy regulations in the expectation that the costs of litigation, if not of compliance, can be shifted, ultimately, to other policyholders.”⁸⁰⁶

Generally, it appears that every state will have a different understanding of how an insurance policy may respond to fines and penalties levied against a business. In certain states, there is an apparent *de facto* ban on allowing these costs to be insurable. In the states where such costs are allowable, this may be only to the extent that management and other key decision-makers were unaware of its employee's wrongful acts. Where a company's upper echelons is engaging in intentional misconduct, such as failing to fix known vulnerabilities, outright disregarding reasonable cybersecurity measures, or blatantly failing to make a reasonable attempt at complying with a state's mandatory cybersecurity or privacy laws, it is highly likely that insuring against such actions could be deemed to be against public policy. As such, businesses are advised to seek legal counsel regarding how choice of law and choice of forum may apply to them. While all this may seem ambiguous, it does lead to one particularly salient point: Businesses cannot, and should not, assume that a cyber insurance policy will always take the place of reasonably constructed cybersecurity defenses and adherence to applicable state laws that govern the protection of sensitive consumer information.

Beyond Fines and Penalties

Surely, any business that continuously loses customer data without taking appropriate post-breach remedial actions will have difficulties obtaining cyber insurance. No insurance company is in the business of losing money. When an insurer is assessing a risk, which has shown a track record of numerous breaches, they may offer renewal terms at increasingly unpalatable levels, if any coverage is offered at all. Any insurer facing the prospect of covering sizeable fines and penalties of a habitually breached company will certainly scrutinize the application, policy language, and other documents to determine if they have grounds to deny coverage.

Likewise, the states, and various federal agencies, may start investigating any business with a track record of acting irresponsibly. Even in a policy providing coverage for fines and penalties, it is not unquestionably assured that fines and penalties will necessarily be paid on behalf of the business. Regardless, the costs of comply with injunctive orders to become compliant are likely to be excluded from coverage.

While consumers are increasingly faced with “breach fatigue,”⁸⁰⁷ it is entirely plausible that each additional breach notification letters from the same company will drive them towards competing businesses. Local or national news sources may also take note of particularly egregious on-going security practices, further exacerbating the issue.

Given a sizeable breach, or a series of breaches, a plaintiff’s attorneys could start taking notice as the number of affected individuals increases. This could multiply not only the probability of a class action data breach claim but could also provide additional ammunition to the class’s ability to have at least part of their action considered reasonable. Should the case go in front of a judge or a jury, it is unlikely that they will look favorably upon a business that was breached multiple times and failed to appropriately and proactively safeguard customer information.

A final complication may be found for those companies which could find themselves subject to fines and penalties under GDPR, or other international laws. Insurability will likely vary dependent upon the host country in which the action is brought. In a review of 30 European countries, only two provide likely insurable coverage for GDPR fines and penalties. Twenty would deny coverage, and eight countries were unclear.⁸⁰⁸

All the above possibilities could result in significant, multi-faceted, long-lasting, financial difficulties by a business that are likely avoidable with responsible data security practices.

None of this is to say that coverage for fines and penalties are not insurable. Rather, businesses should understand that the applicability of such clauses is not as simple as it would naturally appear to the uninitiated. They should endeavor to avoid testing the limits of their luck and insurance policy provisions by taking proactive data security measures; costly as it may appear at the onset. Proactive measures likely include inputs from legal counsel and cybersecurity consultants, prior to – and certainly following – a breach.

Action Items:

- ☐ Businesses should read and understand their available coverage features;
- ☐ Work with legal counsel and a knowledgeable broker when in doubt;
- ☐ Communicate coverage features to relevant stakeholders, including IT and staff;
- ☐ Update the business’s incident response plan and other internal documents as necessary to reflect policy features.

Excess Insurance Considerations

Due to current market conditions, it is reasonable to assume that most businesses will have no problem obtaining adequate cyber insurance limits within one primary policy. However, very large businesses may require higher limits than those offered by any one insurer. In the future, as the number of insurers offering cyber insurance decreases, and the available limits per insurer falls in line with more traditional insurance products, it is possible that medium-sized organizations will need to look towards excess insurance.

Excess insurance can seem very attractive, perhaps too attractive to those not familiar with its risks. While this is not to say that excess insurance does not have its place, it does mean that any business contemplating this coverage in the context of a cyber claim should be duly familiar with its inherent risks and benefits.

General Structure:

In a broad sense, the term “excess insurance” is quite apt at describing its general function. Excess insurance acts to provide insurance that is in excess of the primary insurer’s limits. As a broad term, it can encompass many forms of insurance that overlay the primary insurer. A true excess policy will increase, but not broaden, the underlying coverage.⁸⁰⁹

While many types of excess insurance forms are available, they can be broadly construed to fall into two categories. “Follow form” policies incorporate the terms, exclusions, and conditions of the primary policy by reference. “Standalone” policies incorporate their own terms, which can be unique from the underlying primary policy.⁸¹⁰ In very rare circumstances, businesses may be able to purchase an excess policy which will give them the following features:

Potential Benefits

1. Generally, excess insurance is less expensive per coverage dollar than that found in a primary insurance policy. This is because excess insurers are generally shielded from many of the costs associated with being a primary insurer, such as maintaining a loss prevention department, increased interactions with policyholders, and additional regulatory costs.⁸¹¹
2. For a very large business that could face catastrophic losses, excess insurance policies may provide an additional layer of financial security.

3. Certain businesses may be able to negotiate the terms of their excess policy due to the less stringent standards placed upon the excess market by regulators.

Potential Risks

1. Foremost, excess insurance policies do not generally cover sublimits found in the underlying policy. Here is an example from an excess insurance policy: “The Policy does not provide excess insurance above any sub-limit of liability available under any Underlying Insurance unless the Insurer has agreed to provide such excess coverage by separate endorsement to this Policy. However, where payment of amounts subject to a sublimit erodes or reduces the limits of liability of the Underlying Insurance, this Policy shall recognize such erosion or reduction of the limits of liability of the Underlying Insurance.”⁸¹²

At least in the above example, any sublimit found in a cyber insurance policy will not be covered. It would not be until the entirety of the policy is exhausted that the excess insurer would provide for additional expenses. Depending on how the cyber policy is structured – and they are all different – a business may find itself with an excess policy that is not required to respond to large costs which the business is contractually or legally obligated to pay.

In very rare circumstances, a business may be able to purchase an excess policy which also covers sub-limits. As stated before, these are very rare and little legal literature is currently available on this topic. Therefore, they will not be included in this discussion.

1. Assuming that coverage is fully provided for by the primary insurer, this is not a guarantee that an excess insurer is bound to provide coverage. Even in a standard follow form excess policy, the excess insurer is bound by the terms of the primary policy, not necessarily the interpretations of the primary insurer. 813 Considering that coverage terms and limits are still very much subject to litigation in this area of insurance, any additional questions of coverage are likely unpalatable to many businesses.
2. When a loss occurs that could implicate the limits of the excess insurer, they may have the option to participate in the defense and settlement of the claim. For example, one excess insurance policy form stated: “The Insurer may elect to effectively associate in the investigation, settlement or defense of any claim reasonably likely to be covered under this

Policy.”⁸¹⁴ This could serve to further complicate the defense of the claim, as well as any settlement negotiations.

A note on other unique insurance arrangements

Cyber insurance is a new product that is, comparatively speaking, a very affordable method of risk transference. However, this book should adequately show the various methods by which insurers, policyholders, and the court system, are still struggling to define the scope and limits of seemingly basic terms. For this reason, unique insuring agreements are likely very ill-advised as a method of saving money on the front-end of a transaction.

Simply put, the more parties that are subject to paying out a claim, and thus interpreting the terms of an insuring agreement, the more likely that a business will face a declination of coverage. This increases the number of parties that a business may need to fight in litigation when seeking resolution. In turn, this will increase the complexity of any legal battle, which increases the ultimate costs of a dispute, which may not result in a favorable outcome by the business seeking coverage dollars.

Businesses should not be lured by the apparent intellectual complexity offered by a broker who is offering insurance terms. Such complexity can often be used as a sales tactic to save a business money – and thereby gain business. However, little, if anything, is ever mentioned regarding the drawbacks associated with these insuring arrangements. Should a denial of coverage take place above the primary level of insurance, any savings can quickly become eroded by the costs of litigation. For the foreseeable future, simplicity of structure and policy definitions will remain the benchmark by which cyber insurance policies should be judged for all but the largest and most sophisticated businesses.

Action Items:

- ☐ Businesses should understand the inherent risks and rewards found in excess cyber insurance policies;
- ☐ Businesses in need of excess cyber insurance policies are advised to seek legal counsel;

General Guidelines on Purchasing Cyber Insurance

In totality, there are guidelines that all businesses reviewing a new or existing cyber policy should consider:

- Work with a knowledgeable cyber insurance broker and a reputable insurance company. Though you may have a relationship with an existing broker who is not knowledgeable in this area, consider if that relationship is worth the potential cost of an insurance declination or uncovered loss;
- Work diligently with a knowledgeable broker as your business “wargames” your coverage requirements. Understand what risks are unique to your business, and how to insure – if possible – for those risks.
- Businesses should purchase the largest reasonable limits that are available in consideration of funding restrictions. While there are certainly “average” breach costs, they are just that – averages. The cost of a breach varies wildly, often based upon factors that are out of the control of the business. Most businesses should attempt to maximize first-party coverage limits.
- Businesses should purchase the broadest policy that has the most coverage features. As new attack vectors and vulnerabilities are created and exploited, businesses may find themselves responding to a method of breach that they had either not considered or otherwise deemed impossible. The legal interpretation of policy language in this field is still very much in its infancy and is rapidly evolving. Any small savings in premium can be grossly outweighed by otherwise unnecessary uncovered costs.
- If a business wants to customize coverage found in their cyber policy, they should do so carefully and in conjunction with qualified legal counsel. Cyber policies can be exceedingly complex. Even well-intentioned unique endorsements may have unforeseen negative consequences in other portions of the policy.

Section 7: After the Policy is Bound

Cyber Insurance, like cybersecurity, is a year-round endeavor. As such, businesses should be aware of the myriad of choices, decisions, and responsibilities that await them after their cyber insurance policy is bound. Failure to understand these obligations can lead to late reporting of claims, potential declinations of coverage, and increased regulatory actions.

Damage Control

Policy Benefits

Certain insurers may offer additional security services as a benefit to the policy. These can include employee training through fake phishing emails and webinars, or continuous network scanning and penetration testing.

While these tools can provide convenience, businesses should be cautious about investigating the depth of such services. These broadly termed benefits can range from rudimentary to quite sophisticated. Businesses should not necessarily consider these services as meeting the requirements of any state or federal law without first consulting legal counsel.

Businesses must weigh the convenience of automated services to the potential for additional legal liability. For example, a business may purchase a cyber insurance policy that also comes with vulnerability scanning. While the report *might* prove useful – depending on the insurer and the report delivered – businesses are being notified of actual or potential vulnerabilities in their systems.

Referencing *In re Equifax Inc., Customer Data Security Breach Litigation*, businesses can look to guidance provided by the courts on how they will view known vulnerabilities leading to data breaches. As the court stated, “The Court concludes that, under the facts alleged in the Complaint, Equifax owed the Plaintiffs a duty of care to safeguard the personal information in its custody. This duty of care arises from the allegations that the Defendants knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.... And, as this Court noted in *Home Depot*, to hold otherwise would create perverse incentives for businesses who profit off of the use of consumers' personal data to turn a blind eye and ignore known security risks.”⁸¹⁵

Therefore, businesses should consider any potential legal ramifications of receiving information about potential security vulnerabilities. Should a business elect to purchase a cyber policy that offers this service, they should be prepared to act immediately on any negative findings contained therein. Additional care should also be taken to ensure that the relevant stakeholders also receive this information in a timely and defined manner.

Finally, a crucial component to the time from breach to client notification is pre-selecting vendors. Businesses should consider researching available vendors and their contracts if provided by their insurer. This will likely require legal counsel who is well-versed in privacy and contract law to advise the business on contract suitability should the business have unique requirements.

Action Items:

- ☐ Understand what policy benefits are afforded by the insurer;
- ☐ Before assuming that these benefits fulfill legal requirements, work with legal counsel;
- ☐ If your business's cyber insurer delivers reports with known or potential security vulnerabilities, make certain that this information is delivered to the correct stakeholders and acted upon in a timely fashion;
- ☐ If necessary, work with legal counsel to pre-select vendors and negotiate vendor contracts;
- ☐ Communicate this data to relevant stakeholders, including IT staff;
- ☐ Update the business's cybersecurity framework and other internal documents as necessary.

Potential Claim Reporting

One of the most overlooked components of a cyber insurance policy is the requirement to report potential claims. As technology becomes more pervasive, complex, and distributed, it is much more likely that information held may be breached. Generally, data breaches requiring potential claim reporting fall within two categories: those breaches that occurred within the business – internal breaches, and those breaches that occurred at a third-party vendor holding the business’s information – external breaches.

Consider how one prominent cyber insurer defines the policy obligation of the insured to notify the insurer of any potential claim: “You have the option of notifying us of potential claims that may lead to a covered claim against you. In order to do so, you must give written notice to us **as soon as possible and within the policy period**, and the notice must, to the greatest extent possible, identify the details of the potential claim, including identifying the potential claimant(s), the likely basis for liability, the likely demand for relief, and any additional information about the potential claim we may reasonably request.

The benefit to you of notifying us of a potential claim is that if an actual claim arises from the same circumstances as the properly notified potential claim, then we will treat that claim as if it had first been made against you on the date you properly notified us of it as a potential claim, even if that claim is first made against you after the policy period has expired.

All potential claim notifications **must be in writing** and submitted to us via the designated email address or mailing address identified in Item 6 of the Declarations.”⁸¹⁶

As later defined in the same policy, a potential claim means “any acts, errors, or omissions of an insured or other circumstance reasonably likely to lead to a claim covered under this policy.”⁸¹⁷

Put more simply, insureds need to notify their cyber insurer of any potential claims that occur within the policy period. This is to benefit the insured in case a claim is made against the insured after the policy period has expired. Failure to do so could result in a declination of coverage. Even when the nature and extent of the potential claim are unknown, businesses should take serious consideration as to whether they need to notify their insurer.

In relation to an internal breach, businesses may unknowingly run afoul of their policy requirements. Although they may give notice that a cyber event has occurred, well-meaning but often unqualified internal IT staff may tell business owners that

nothing appears to have been stolen. Or, the business may simply decide not to report the issue for fear of an increase in the policy premium. If it was later determined that covered client information was stolen, coverage may be declined if the timing of that determination fell outside policy-reporting requirements. Further, failure to report potential claims could result in all manner of expensive uncovered risks.

Potential claim reporting of external breaches tends to become more onerous for the business. As mentioned previously, service providers are generally not responsible for the client's information stored by the business on their system. To illustrate the potential dangers that could befall a business for failing to report a potential external breach of client data, consider the recent Wolters Kluwer CCH debacle.

On May 6th, 2019, CCH – a prominent provider of software for accounting firms – experienced “network and service interruptions” that affected some of their platforms and applications. This effectively shut down or severely restricted the business operations of many accounting firms across the country for a significant period of time.

As later reported in a May 23rd update on the company’s website, their IT team had detected a zero-day exploit. For this reason, they had shut down many of their systems to avoid the spread of the malware.⁸¹⁸

Of greater importance to this discussion was the company’s notification: “To date, we have found no evidence that customer data or systems were compromised.” However, they also stated that “Our investigation of the incident is on-going.”⁸¹⁹

While the outcome of this event remains unknown at the time of publication, what would happen if CCH were to later notify businesses that their client’s information had been stolen?

Likely, it would depend on how the business initially responded, if at all. For businesses that had notified their insurer of the CCH breach as a potential claim before their policy renewed, they would most likely be afforded coverage under their policy. For businesses whose cyber policy renewed before the hypothetical CCH breach notification – and had not given their cyber insurer a potential claim notice – it would be all too easy for the insurer to deny coverage. This would leave the business scrambling to find and review appropriate vendors, manage the entire process, research and adhere to all applicable laws, and pay for the entire claim out of pocket.

Businesses who feel that their cyber insurer acted in bad faith by declining coverage could attempt to litigate the issue. Regardless of the outcome, a timely potential claim notification would be exponentially cheaper and less painful.

Action Items:

- ☐ Understand what requirements your policy contains regarding the reporting of potential claims;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan other internal documents as necessary;
- ☐ Conduct regular training for staff, so they are aware of their obligations to report a potential cyber claim.

Damage Control

Claim Reporting

Many businesses rightfully believe that a claim is a breach of their computer system by an unauthorized third party, but a cyber insurer may have an expanded definition. Consider the following definition from a well-known cyber insurer:

A “Claim” means:

1. a written assertion of liability or any written demand for financial compensation or injunctive relief;
2. a regulatory proceeding;
3. unintentional breach of a written contract asserted by a client;
4. contractual indemnity – breach costs, or;
5. contractual indemnity – third-party.⁸²⁰

In this example, the insurer is considering the traditional understanding of a computer system breach to be only one of five claim scenarios that would need to be reported. Regardless of what a business’s leadership believes, they should have a clear understanding of what the insurer defines as a claim. In turn, leadership should relay that information to all other relevant parties, including staff and IT professionals. These understandings should be encapsulated in the business’s incident response plan and information security policy.

Businesses should understand that each insurance provider will have different definitions of what a “claim” will entail. Furthermore, different cyber policies from the same carrier may have different definitions, even for the same word or phrase. As such, it is up to the business to keep abreast of any changes to their policy and incorporate those changes accordingly. Because business owners are unlikely to fully immerse themselves in network architecture and sub-vendors of their primary vendors, they should ensure that their IT professionals are well-versed in understanding what constitutes a claim or potential claim.

At worst, the failure to report a claim within the policy period can lead to an otherwise unnecessary full declination of coverage. At best, a late report of a claim will make the business ineligible for a relatively minor recoupment of funds, often from a sublimit such as one applying to a dependent-business interruption. Nonetheless, a business should not test the limits of their policy.

When in doubt, consider reporting the matter and let the system sort it out.

Action Items:

- ☐ Understand how your policy defines a claim;
- ☐ Communicate this data to relevant stakeholders, including IT and staff;
- ☐ Update the business's incident response plan other internal documents as necessary;
- ☐ Conduct regular training for staff so they are aware of their obligations to report a cyber claim, and how to do so.

Giving Notice to the Insurer

Different policies will have different policy language requirements regarding how soon claims or potential claims should be reported to the insurer.

In regard to a claim, one insurer was succinct in their policy language: “You must notify us of claims as soon as practicable once such claim is known to any board member, trustee, director, officer, in-house counsel, risk manager, chief technology officer, chief information officer, or chief privacy officer of the insured organization, but in any event no later than: (i) the end of the policy period; or (ii) 30 days after the end of the policy period for claims made against you in the last 30 days of the policy period. Proper notification of claims must be sent in accordance with the notification details in Item 7 of the Declarations.”⁸²¹

How the term “as soon as practicable” should be interpreted could vary based upon the controlling case law and venue where the coverage dispute is litigated.⁸²²

A different insurer appears to be slightly more lenient regarding the treatment of potential claims in their policy language, stating: “What you must do in the event of a circumstance which could give rise to a claim: In respect of INSURING CLAUSES 5 and 6, should a senior executive officer become aware of: a. a situation during the period of the policy that could give rise to a claim, or b. an allegation or complaint made or intimated against you during the period of the policy; then you have the option of whether to report this circumstance to us or not. However, if you choose not to report this circumstance, we will not be liable for that portion of any claim that is greater than it would have been had you reported this circumstance.

If you choose to report this circumstance you must do so no later than the end of any applicable extended reporting period for it to be considered under this Policy and we will require you to provide full details of the circumstance...”⁸²³

Action Items:

- ☐ Understand how to give notice to your insurer;
- ☐ Communicate this data to relevant stakeholders, including IT staff;
- ☐ Update the business’s incident response plan other internal documents as necessary.

Damage Control

Material Changes

Cyber insurers will often include state-specific amendatory endorsements like those found in more traditional insurance policies. While often overlooked, there are specific cancellation provisions that require vigilance on behalf of all businesses.

Take the following clause found in a cyber policy endorsement: “[W]e may cancel this policy only for one or more of the following reasons: ...

- d. Increased hazard or material change in the risk assumed which we could not have reasonably contemplated at the time of assumption of the risk;
- e. Substantial breaches of contractual duties, conditions or warranties that materially affect the nature and/or insurability of the risk;”⁸²⁴

Encapsulated within the above policy language are several issues that businesses should address.

Foremost, any material changes concerning the risk to the business should likely be reported to the insurer. Changes could include the business falling under new regulatory schemes not disclosed in the application, or material changes to network security and control regimes.

Second, the business should ensure that it is staying true to the representations that it made on the application. Often the application or the policy will include a warranty statement. This statement is essentially a promise that the statements made by the business are true, and the validity of the insurance policy depends upon the business fulfilling those promises. Failure to do so can result in a declination of coverage.⁸²⁵ This was one of the allegations used by the insurer to deny coverage in the previously discussed case of *Columbia Casualty Co. v. Cottage Health System*.

Generally, for an insurer to mount a misrepresentation defense, they will rely upon the following elements:

1. The representation made by the applicant was misleading or untrue;
2. The representation was material to the risk presented before them;
3. The insurer relied upon the representation to issue the policy at a definite premium.⁸²⁶

Notice that none of the above necessarily relied upon the applicant to consciously create a material misrepresentation to “trick” and insurance company. As held in most jurisdictions, no finding of intent is required for an insurer to claim that the applicant included a material misrepresentation, and thus the policy is voided.

Indeed, a cyber application may include language analogous to the following:

“APPLICATION DISCLOSURES: If there is any material change in the answers to the questions in this Application before the proposed policy inception date, you must notify us in writing. In such case, **we have the right to cancel, withdraw, or modify any outstanding quote for insurance coverage or any policy that may have been issued....**

The undersigned, as your authorized representative or agent, declares to the best of their knowledge and belief and after reasonable inquiry, that the statements made in this Application are true, accurate, and complete. The undersigned agrees that we will rely on this Application in issuing any insurance policy providing the requested coverage, and that this Application will form the basis of any such insurance policy.”⁸²⁷

How the various courts will determine the materiality of a misrepresentation based upon statutory codes and the specific facts pattern of any one case is well beyond the scope of this text. However, businesses should take the above with the understanding that they must take reasonable care when completing their cyber insurance application. For many applicants, the additional cost of legal assistance may be warranted in comparison to a potential declination in coverage. If an insurance company put the question on an application, it is likely that the question – and answer – is material to the risk and could be the basis for a declination.⁸²⁸

Action Items:

- ☐ Understand when material changes must be reported to the insurer;
- ☐ Communicate this data to relevant stakeholders, including IT staff;
- ☐ Make sure your business has a defined procedure for reporting material changes to your insurer;
- ☐ When in doubt, work with legal counsel to ensure policy compliance.

Section 8: Interesting Extras

The following are additional tools, resources, and publications from the authors that a business can use to better strengthen their cybersecurity posture. In turn, this can lower premiums, minimize the potential of a breach, and lessen the possibility of an insurance declination due to oversights.

Examples of Real Business Breaches

Below are examples of recent and real breaches experienced by various businesses across the country. Although these breaches are public knowledge, the authors have removed identifying information. The goal is not to embarrass these companies of note but to allow other businesses to learn from their ordeals.

Example 1: Firm 1 was performing a routine test on their data restoration procedures. The data was held by a third-party cloud provider in an offsite, separate location. While performing this routine test, the firm was notified that the data had been subject to a ransomware attack. An investigation by the firm's outside IT expert determined that there was no evidence that any information had been downloaded or copied.

Early the following year, the state's Department of Taxation and Finance notified the firm that approximately 50 tax returns were filed under the firm's electronic filing ID number for existing clients. The firm contacted the IRS, which confirmed similar activity. Subsequently, the firm suspended the filing of any electronic tax returns.

In response, the firm engaged a forensics expert to provide an assessment of the network and security. At the time of notice, the forensics expert had found no indication of any vulnerability or of any previous compromise on the firm's network. Additional forensics were performed on the firm's off-site data location to determine if any prior breach had occurred at that location.

The firm conducted a full review of their security practices and systems. Credit monitoring and identity theft and resolution services were provided to affected clients.

Example 2: Business 2 was attempting to resolve an email failure with its email-hosting service. During this action, the partner was directed to a website that instructed him to call a phone number for immediate assistance. After the phone call was placed, the technician requested to access the partner's computer to understand their email problem.

The partner on the call installed the software necessary to allow remote access. The technician began to access various IP addresses on the partner's computer and notified him that this was the reason behind the email issue. To fix the issue, the technician insisted that they allow him to install a program on the office's network server. The partner resisted and told the technician that his local IT provider would contact him to resolve the issue. At this point, the technician on the phone stated that

only a Microsoft technician could solve the issue. At this point, the partner realized that he was not speaking with his email-hosting service and disconnected his computer from the network and uninstalled the remote-access software. The interaction was stated as lasting less than eight minutes.

The partner contacted his IT provider and was notified that he had fallen victim to a scam. The remote-access software was meant to copy information on the local computer. On the partner's desktop was a "My Documents" folder that kept items that had been emailed in the past and included tax returns and other documents. Also, on his computer were previous years of their tax program that were not encrypted.

Upon examination, it was discovered that the computer was infected with a virus that was immune to "normal" virus-protection software. Virus scans were performed on all computers, and the virus software was upgraded. Physical controls were updated to ensure that all client data was stored in an encrypted form.

Example 3: Business 3 fell victim to a social engineering scam that allowed an unauthorized party to gain access to a staff member's email account. Upon discovery of the intrusion, email access was shut down for all accounts.

Clients of the business were warned that unwanted email requests looking like the business's normal emails might be made, but those requests should be immediately disregarded. Clients were encouraged to continue using the client portal provided by the business to transfer any sensitive documents.

Business 3 indicated that they engaged their IT experts to conduct a review of their email security practices and systems to ensure that appropriate security measures were in place moving forward. It was not reported how many clients received notification letters and credit monitoring.

Example 4: Business 4 became aware of a breach when they were notified that their clients' accounts were experiencing attempts to have funds withdrawn. Their clients also experienced multiple attempts to have fraudulent credit cards opened in their names.

Upon learning of the breach, Business 4 retained a computer forensics firm to determine the scope and nature of the breach. The forensics team discovered that one computer was compromised and had been accessed over a period of two days. The unauthorized party may have accessed clients' personal information, names, home addresses, social security numbers, tax returns, and financial account numbers.

Business 4 contacted the IRS and the FBI to conduct investigations and corrected the vulnerability in their computer system. Additionally, they reviewed their internal policies on data management protocols and implemented further security measures.

Ultimately 1,856 of the business's clients received notification letters and credit monitoring services.

Example 5: A large northeastern city fell victim to a ransomware attack. This attack allegedly infected nearly ten thousand government computers. While the hackers demanded a bitcoin ransom, the city refused to pay. Due to the refusal of the city to pay the ransom, houses couldn't be sold, and utility bills couldn't be paid. It took weeks before the city would regain any semblance of normalcy in daily operations. In response, the city has spent an enormous sum of money to update security and hosting systems.

Example 6: A logistics company discovered that an employee's Office 365 account was accessed by an unknown user. It was estimated that over 1,500 current and former employees may have had their names, social security numbers, bank account numbers, passport numbers, tax ID numbers, and drivers' license numbers exposed. To mitigate the possibility of future incidents, the company invested in additional protective measures. Affected parties were given notification and credit monitoring services.

Action Items:

- ☐ A continuously updated list of breaches can be found at www.databreaches.net.
- ☐ Consider using similar industry breaches as training aids and warnings for staff.
- ☐ Every breached business indicated that they performed some sort of update to security systems and/or their computer-use policies. Take this as a warning and become proactive, not reactive.

Tips on Passwords from NIST

Nearly all businesses nationwide adhere to the same minimum password requirements. Generally, at least eight characters long, one uppercase letter, one number, one lowercase letter, one special character, and so forth. Passwords must be changed at periodic intervals, such as every 90 days. However, such long-standing and ubiquitous practices are now being recommended for change by the National Institute of Science and Technology (NIST).

NIST is a non-regulatory federal agency within the Department of Commerce. This organization creates and develops the Federal Information Processing Standards that creates compulsory standards for all federal agencies. Through their Special Publication (SP) 800-series, they often set cybersecurity best practices across the industry.

In early 2019, NIST published revised guidance on security best practices in NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management. NIST refers to what is colloquially known as a “password,” with the fittingly a cryptic “Memorized Secret Verifiers.” While their purely technical recommendations are beyond the scope of this book, their updated password recommendations are as follows:

- When a user establishes or changes a password, that password should be screened against a list of commonly used or previously compromised passwords. Other examples of improper passwords include dictionary words, context-specific words such as the name of the business or derivatives, and repetitious or sequential characters such as “123456” or “abc123.”
- Passwords should not be changed at periodic intervals. For example, no more new passwords every 90 days. Changes should only be forced when there is evidence of compromise.
- The traditional composition rules requiring the mixture of special, uppercase, and lowercase letters, in combination with a number, known as “composition rules,” are no longer necessary.
- Passwords should be between 8 and 64 characters.
- NIST encourages users to utilize passwords managers, which they say may “increase the likelihood that users will choose stronger memorized secrets.”

Beyond this shortlist, there are numerous other recommendations that are worth consideration in conjunction with the business's IT and cybersecurity professionals. NIST's *Special Publication 800-63B; Digital Identity Guidelines: Authentication and Lifecycle Management* is available free to the public at: <https://doi.org/10.6028/NIST.SP.800-63b>.

Damage Control

Warning Signs

Below are common signs that a business is risking, or has experienced, a breach:

- ☐ Inability to login to your computer system;
- ☐ Strange computer behaviors such as popups, new toolbars, anti-virus warnings, or unexplained movement of your cursor;
- ☐ Slow computer speeds, often across multiple computers or the entire network;
- ☐ Unusual login activity reported by system administrators, often from unexpected and varied geographical locations;
- ☐ Abnormal outbound traffic detected on the network;
- ☐ Changes or additions to administrator login permissions;
- ☐ Off-cycle or unusual requests for money to be transferred to new accounts;
- ☐ Urgent requests that money be transferred to established clients or vendors using new payment methods in conflict stated business protocol and verification methods;
- ☐ Emails in the staff member's outbox that are unexplained;
- ☐ Abnormal request to change usernames or passwords, often seemingly from trusted sources;
- ☐ Lengthy and/or cryptic file extensions;
- ☐ Unsolicited emails requesting the staff member download a file or open a file and enable macros;
- ☐ Unexplained loss of client or business funds/information;
- ☐ Clients reporting emails from the business that were never sent by the business;
- ☐ Notification from state or federal agencies that a breach is likely to have occurred;
- ☐ Any other indication that the business reasonably believes may indicate a breach.

Action Items:

- ☐ Consider using the above as a basis for a continuously update business specific list that can be disseminated to all members of your business;
- ☐ Consider continuously supplementing this list with employee training at your business. Readers of this book can visit www.HailBytes.com and use coupon code CPLBROKERS for a discount on each employee's monthly training cost.

What is an Incident Response Plan?

In a recent Ponemon Cost of Data Breach Study (2017), the authors looked at the impact of 20 different factors on the cost of a breach. Most notably, the greatest reduction in the per capita cost of a breach was using an incident response team (IRT).⁸³⁰ Simply put, an IRT is responsible for creating, practicing, refining, and implementing an Incident Response Plan (IRP). Eventually, the business will be breached. With a little forethought and planning, businesses can lower the cost of a breach, lessen disruption of business activities, and avoid embarrassing or costly mistakes.

Considering this information, many businesses commit the following errors:

- They do not have a plan. When a breach occurs, this often results in several easily preventable and frustrating errors. Because responsibilities were not delineated before the event, egos often clash in the partner group. This can lead to necessary steps being skipped and redundant tasking. It also tends to prolong the response times, which are subject to various state and federal limitations. Contemplating if the business should respond to a reporter's phone call immediately after a breach is no time to make a judgment call. Have a plan.
- Businesses have a plan, but they've never rehearsed it. Often this occurs when a single member of the business is tasked with creating the plan. While the "box has been checked," it is of no use if the business has never taken the time to educate stakeholders and staff on how it is to be used. This often leads to increased breach detection times by business owners, increased time to potential client notification, and an unnecessary increase in business disruption length. In addition, this can have major insurance implications such as decreased recoupments of various sublimits or outright declination of coverage.
- Businesses have a plan, but it was saved on their now-inaccessible computer system.
- Businesses don't update their plan. Threats change. Key members of the team come and go. Before a business knows it, their plan is obsolete. Make certain the plan stays updated, and key members have been educated and rehearsed their roles. Staff should also understand how to identify a potential security incident and who should receive reports of those incidents.

Incident Response Plans can become very complex, but for most businesses, they should be relatively straightforward. Businesses should begin by understanding the basic functions of an IRT. At its most basic, an IRT should minimize the harm done to the business and respond to the incident in a calm and coordinated manner.

Businesses should begin by identifying their IRT.

The IRT should be comprised of at least one member from each of the business's functional groups. This could include A&A, Tax, HR, IT, Legal, Executive Committee, and so forth. Each group should include a staff member assigned to them so that they can take over in the event the primary member is absent. These will act as the business's subject-matter experts and decision-makers in their respective disciplines. Each incident will be unique, so their level of engagement will be dependent on the event at hand. However, there should be an incident leader for all events that can coordinate the actions of the team. Typically, but not always, this will be the managing partner.

Once an IRT is identified, they will need to be comfortable with the following minimum tasks:

- How will the business identify a network intrusion, privacy breach, denial of service attack, network interruption, or ransomware event?
- What is the communication plan when one of those events occurs?
- Who should be notified when an incident occurs?
- Who will be responsible for coordinating with law enforcement?
- How will the IRT communicate with software vendors, service providers, and the media?
- How will staff be trained to adhere to the policies enacted by the IRT?
- Who will the primary point of contact with the cyber insurance provider following the incident?
- Who is ultimately responsible for coordinating all the activities of the IRT?

As a word of warning, businesses should not make their plans overly complex, nor should they be inflexible by hinging on a single person. Aim for the middle ground that has enough detail to enable intelligent decisions, but not so detailed that any deviation will implode the plan and result in gridlock. It would be infeasible to create a plan for every possible scenario that could befall a business. Greater results can be derived from having members of the IRT who understand why steps are taken, as opposed to warming a chair while following a predetermined plan.

Finally, insurers are increasingly asking for businesses to disclose the fundamentals of their IRP. At a minimum, the failure to have a written IRP could result in a higher premium paid by the business. At the maximum, the failure to have a written IRP could result in terms not being offered, declination of coverage, or necessary coverage elements not being included in the policy.

Action Items:

- ☐ SP 800-61 Rev. 2, Computer Security Incident Handling Guide can be found for free at:
- ☐ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>;
- ☐ Create an incident response plan for your own business;
- ☐ Work with relevant stakeholders to continuously refine this plan and new threats emerge;
- ☐ Ensure that relevant stakeholders and staff are aware of this plan and understand their responsibilities contained therein.

What is a Cybersecurity Framework?

There is no shortage of cybersecurity vendors that promise to solve all the security woes your business is experiencing. Conversely, it is common for your IT department always to be asking for a larger budget, new tools, and they often use terms that are alien to anyone outside their field. Meanwhile, there is the threat of hackers penetrating the computer system, and regulators playing “Monday-morning quarterback” after an event. How should your business balance all these competing interests without information overload?

Thankfully, there is a solution to these problems, and it is called a cybersecurity framework. If you don’t have one, get one. If you have one, use it. When you use it, keep it current.

A cybersecurity framework can best be described as a guide to managing your cybersecurity responsibilities and technology choices. Naturally, these are crucial metrics for anyone overseeing a cybersecurity program. By their very nature, a framework needs to be comprehensive enough to be used by multiple industries, adaptable enough that various business types can use it, and simple enough that all elements of a business can implement it.

Like any technology ecosystem, there are several different frameworks to choose from. A shortlist of frameworks includes PCI/DSS, COSO, ITIL, BiSL, COBIT, TOGAF, PBMOK, and NIST CSF. Some frameworks may be situationally mandatory, such as PCI/DSS. Others are designed for niche industries with very specific needs. Regardless of the number of frameworks available, the best fit for most businesses will likely be NIST CSF.

Why Choose NIST CSF?

Not only is it free, but NIST CSF can help management level the playing field with security vendors and in-house IT personnel to ensure that they are steered towards what will inevitably become an essential business function in the years to come.

The Recent Trends in Security Framework Adoption Survey showed that 70% of US IT and security professionals viewed NSIT CSF as a security best practice.⁸³¹ Given this finding, it is common sense to adopt a framework that the professionals view as superior. Furthermore, as a business grows or the regulatory environment becomes more burdensome, it is more likely that they will need to hire cybersecurity personnel. Having personnel that are familiar with the framework from the outset will make personnel integration faster and costly mistakes less likely.

Regulatory oversight of data security has become a hot topic as of late. Increasingly, the language seen in these oversight/regulatory actions and data security laws hinges on the notion of “reasonable” cybersecurity measures. Of concern to many businesses are their requirements under various regulatory frameworks such as those enforced by the FTC. In its enforcement actions, the FTC has connected consent decrees for the offending business with specific parts of the NIST CSF despite the framework still being considered voluntary.⁸³² Indeed, the FTC has come out with a video on their webpage, which details how the NIST CSF aligns with their work on information and data security.⁸³³ Should a U.S. regulatory body ever seek interest in a business, NSIT CSF framework provides a relatively seamless method of communication that may avoid, or help lessen, fines and penalties.

For businesses holding vast quantities of PII/PHI/PCI, or any business that could be subject to a claim related to a breach of their computer system, good news is on the horizon at the state level. Ohio Senate Bill 220 provides a safe harbor to businesses that have maintained and abided by a cybersecurity program. This would allow qualifying entities an affirmative defense to tort claims if they have met the following eligibility requirements:⁸³⁴

- The business reasonably conforms to an industry-recognized cybersecurity framework, in particular, the NIST frameworks.⁸³⁵
- The cybersecurity program was designed to protect confidential client information against threats that could result in a material danger of identity theft or fraud. In this case, the NIST CSF will provide guidance via the current and target profiles in conjunction with the remainder of the framework.⁸³⁶

Granted, this is not a perfect solution for businesses inside of Ohio, nor would it effectively cover most businesses outside of Ohio. However, it does suggest a trend of state-level legislatures attempting to entice businesses to adopt better cybersecurity hygiene with provided tort defense. Although the relative cost of compliance may not outweigh the cost of litigation for those with a cyber insurance policy, the ability for a business to avoid or minimize bad publicity at the local and national level is priceless.

President Trump recently issued his Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Effectively, this Executive Order directed all federal agencies to adopt the NIST CSF.⁸³⁷ While few, if any, businesses fall under this guideline, it does point to the fact that NIST CSF will continue to be updated with industry best practices and federal support for the foreseeable future. This will enable a business to take advantage of any updates to

the framework as time and threats progress without worrying that their framework of choice may someday become antiquated.

NIST CSF is voluntary, neutral to technology, and flexible enough to scale based upon business growth or retraction. Whether a business is cloud-based, has a dedicated server in-house, or have a hybrid of the two, the framework can be adapted to their needs. Thus, every business will be able to identify their own “best” cybersecurity solutions based upon their own characteristics and circumstances, saving valuable time and money. As a business grows or contracts, the framework can be updated to best suit their current needs.

While undeniably enticing to business leadership, a common retort to adopting a framework is the belief that it is simply too complex a task to be undertaken. It should be noted that NIST CSF is relatively straightforward if taken one piece at a time. Broadly speaking, NIST CSF is comprised of three main parts: Framework Implementation Tiers, Framework Core, and Framework Profile. Each provides a particularly useful piece of the puzzle that allows a business to quickly assess and improve their cybersecurity posture at the most cost-effective level.

Implementation Tiers

First, a business can utilize the Framework Implementation Tiers to “provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.”⁸³⁸ Notably, implementation tiers create a high-level overview for other stakeholders that may allocate funding but do not have an understanding of the specific cybersecurity program in place. While business management may believe they are meeting industry best practices for security, once confronted with the objective criteria in the Implementation Tiers, they often fall to the lowest tier.

Four tier levels exist within the NIST CSF. They exhibit the following general criteria:

Tier 1 (Partial): Risk management practices are not formalized. Implementation of risk management for cyber threats is not objectively measured and recorded. Processes to facilitate sharing of cybersecurity information within the business are limited. The business does not fully appreciate its standing within the cybersecurity hierarchy in relation to its dependents and dependencies, nor does it receive or share threat information with the broader market.⁸³⁹

Due to the novel and complicated nature of cybersecurity, most small- to medium-sized businesses without a formalized cybersecurity framework will fall within this tier.

Tier 2 (Risk Informed): Management has approved risk management practices, but this may not lead to a policy at the organizational level. While there is an awareness at the organizational level of cybersecurity risks, these risks are shared at an informal level. Information on risks may not be shared with others.⁸⁴⁰

While this may sound like low-hanging fruit, it will be a worthwhile goal for most local and mid-sized businesses.

Tier 3 (Repeatable): Risk management practices are formally enshrined in an organization-wide policy that is continuously updated. The organization has both cybersecurity and non-cybersecurity executives that frequently communicate on risks. Continuous monitoring of key organizational assets exists. External participation with the broader community exists as a priority and frequently occurs.⁸⁴¹

Regional businesses may be able to reach this level with prolonged commitment from upper management. It will likely take a dedicated IT department and robust planning with oversight.

Tier 4 (Adaptive): The organization uses predictive indicators and updates policies with any lessons learned. As threats and technology changes, the organization purposefully adapts to the changing threats quickly. The interplay between organizational objectives and cyber-associated risks are considered when decisions are made. Contemplations of cybersecurity risks are ingrained within the culture of the organization. External participation occurs in near real-time with the broader community.⁸⁴²

Due to the time and cost-intensive nature of this tier, most will lack the financial resources to reach this level. Reaching such a tier will likely require full-time IT and cybersecurity staff that are supported and prioritized by both management and staff.

Framework Core

Per NIST, “The Framework Core” is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by using simplistic and non-technical language.”⁸⁴³ The Core is broken down into three component parts; functions, categories, and informative references for further guidance. With 23 categories split across five functions, the Framework Core encompasses the totality of cybersecurity goals for a business.

While this may appear abstract at first glance, these functions and categories serve an immediately useful purpose. When a business looks to understand the cornucopia of cybersecurity products available for purchase, each product should address at least one of the business’s necessary Core Functions and categories.

The five listed functions of the Framework Core are Identify, Protect, Detect, Respond, and Recover. Each is a crucial competence to maximize the probabilities of cybersecurity success. Each function is described below:

Identify: This function can be understood as the asset management, business environment, and risk management strategies necessary for a business to operate in their current environment. Steps ranging from identifying key devices and systems required to meet business objectives and to understanding regulatory and legal requirements are addressed. For businesses, this could include understanding their obligations under various regulatory requirements to enforcing a computer use policy.

Protect: Included within this function are awareness and training, data security, protective technology, maintenance, and protection policies or procedures.⁸⁴⁴ It is convenient to think of this function as a method of implementing appropriate safeguards to protect your defined assets. This can include monthly employee training on best practices, firewalls, intrusion prevention systems, and document retention policy.

Detect: This function helps a business identify anomalous events, anticipate cyber events, and utilize continuous network monitoring and threat hunting to both analyze and minimize breaches. Common detective controls include antivirus, antimalware, and intrusion detection systems.

Respond: This is the immediate function which comes into play when the previous functions have failed. It covers response planning, communications with internal and external resources such as law enforcement, analysis, mitigation techniques, and incorporation of future responses with the lessons learned.⁸⁴⁵ A common example that would cover this key function is a breach/incident response plan that is well-rehearsed and understood by all participants.

Recover: When a business's operations have been halted, this function will help develop and implement a recovery plan to minimize disruptions and return to normal operations. This function encompasses public relations, implementation of the recovery plan, and ultimately updating recovery strategies.⁸⁴⁶ Common elements of this function include hot failover sites, hard drive or server redundancy, and reputation restoration.

Within each function are categories, subcategories, and informative references. An example is as follows:⁸⁴⁷

Function: Detect

Category: Security Continuous Monitoring (DE.CM) – “The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.”

Subcategory: (DE.CM-8) – “Vulnerability scans are performed.”

Informative Reference: CIS CSC 4, 20.

The hierarchical system provides a meaningful way for a partner to oversee the business’s cybersecurity without necessitating a broad mastery of the entire spectrum of knowledge comprising cybersecurity and information technology. This format links common vernacular, via the Function and Category, with the specific action, via the Subcategory to the informative reference.

Furthermore, this structure allows a busy partner who is tasked with the oversight of the business’s cybersecurity to devote various levels of effort and study into higher risk areas while also allowing them to briefly cover areas where they feel more comfortable or knowledgeable. Any specific questions can be immediately addressed with informative references.

If a question is beyond the ability of in-house personnel, the category, subcategory, and informative reference can provide a meaningful point of discussion with contracted, outside experts. Ideally, this would enable the business to avoid incurring the undue cost of asking for blanket cybersecurity assistance. Given the ubiquitous nature of the NIST CSF framework, most outside cybersecurity experts should be able to quickly assist the business as they will already share a common knowledge base.

Framework Profile

Once a business has detailed its current needs, requirements, and resources with the Framework Tiers and Framework Cores, they can create their Framework Profile. This initial Framework Profile can be compared with a business’s Target Framework Profile to display gaps in cybersecurity. These gaps can be rank ordered in terms of size, corrective cost, and implementation priority. As a living document, this will allow a business to make an educated decision each year on their cybersecurity status and budgetary needs.

As addressed specifically within NIST CSF: “Once a product or service is purchased, the Profile can be used to track and address residual cybersecurity risk. For example, if the service or product purchased did not meet all the objectives described in the Target Profile, the organization can address the residual risk through

other management actions. The Profile also provides the organization a method for assessing if the product meets cybersecurity outcomes through periodic review and testing mechanisms.”⁸⁴⁸

In total, the above may appear to be a monumental undertaking. However, when taken one step at a time, it can be implemented effectively. The framework will ultimately best position a business to adhere to regulatory requirements, track necessary cybersecurity controls, and most effectively utilize their budget. If a business falls under multiple regulatory regimes such as PCI DSS, HIPAA, DFARS, and so on, there are numerous “crosswalks,” which allows a business to map how NIST will demonstrate reasonable cybersecurity measures needed in those other regimes. Failure to do so could later result in unnecessary breaches of client data and the potential for unwelcome regulatory scrutiny.

Action Items:

- The NIST Cybersecurity framework can be found for free at: <https://www.nist.gov/cyberframework>.
- Smaller businesses should also consider: <https://www.nist.gov/itl/smallbusinesscyber/planning-guides>;
- Small Business should also reference NISTIR 7621 Rev. 1, *Small Business Information Security: The Fundamentals* found for free at: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>
- Consider adopting a cybersecurity framework. Doing so will likely require assistance from outside experts;
- Work with legal counsel to determine your unique requirements. In certain instances, other frameworks may be more beneficial, or mandatory;
- Small Business should reference NISTIR 7621 Rev. 1, *Small Business Information Security: The Fundamentals*

Assessing the Security of Cloud Providers

For practical purposes, businesses will continue to look towards the cloud to host data and applications. For many, this will be an act of necessity as internal IT and cybersecurity staff become too rare and expensive to hire. For others, it will be a practical decision based on convenience, geographic dispersion, cost, or any number of other factors. Some may elect to maintain a hybrid system where certain information is stored on-site in a server while other information is stored in the cloud. Many companies will be forced into some cloud service as locally hosted applications become impossible.

Regardless, here is the most important consideration: There is no cloud. It's just someone else's computer. It should be unsurprising that a recent report listed 11% of breaches originating from vendors.⁸⁴⁹ As such, businesses will want to assess the security of their cloud provider. This could be for practical reasons, such as regulatory requirements listed earlier in this book, or for insurance reasons. Businesses may be able to transfer the responsibility to keep the data available and secure, but they will not be able to transfer legal accountability. Ideally, earlier examples provided in this book prove the point.

Yet, with thousands of potential cloud providers available, how can a business reasonably assess the security of a cloud provider? Unfortunately, it is not as easy as going with the largest provider or the one with the largest marketing budget.

Consider recent allegations in the class-action case of *Howard v. Citrix Systems*.

Lindsey Howard ("Howard") was a former employee of Citrix Systems, Inc. ("Citrix") bringing a class-action claim against her former employer. Citrix is an American multi-billion-dollar grossing, multinational software company that employs over 8,000 people worldwide.⁸⁵⁰ They provide, among other offerings, software as a service and cloud services. Many accounting firms rely on Citrix ShareFile to allow secure communications between the firm and its clients.

In late April of 2019, Citrix sent out a breach notification letter to numerous parties. According to Citrix, in early March of that year, the FBI informed Citrix they had reason to believe that international hackers had gained access to Citrix's internal network. Citrix believes that the hackers had intermittent access from roughly mid-October until two days following the FBI's notification.⁸⁵¹

Information that may have been potentially stolen included information on current and former employees, and potentially the information of their beneficiaries and/or dependents. This may have included names, social security numbers, and certain financial information.⁸⁵²

According to the claim, this breach occurred when the hackers attacked using “password spraying,” a well-known breach method.⁸⁵³ By way of background, password spraying is a well-known attack that attempts to access large numbers of accounts by using a few commonly used passwords such as “Password,” “Password123,” and the like. This technique is used across many accounts in succession to avoid any one account from being locked-out and notifying the user.⁸⁵⁴

Howard alleges that this type of attack is well known and could have been prevented. She further alleges that “the deficiencies in Citrix’s data security were so significant that the intrusion by the hackers remained undetected for months and was only revealed to Citrix when it was informed by the FBI.” Ultimately the hacker absconded with six terabytes of information.⁸⁵⁵ To put that in perspective, it would take roughly 9,000 CDs to hold that much information.

While those allegations are bad enough, Howard further alleges that Citrix had faced previous breaches but failed to react appropriately to the threats presented.

According to the claim, in 2016, a Russian hacker known as “w0rm” published a blog post where he claimed that he was able to gain access to Citrix’s content-management system with an unsecured password.⁸⁵⁶

Cyberint, an Israeli cybersecurity intelligence company, claimed that it had identified the breach in October of 2015. Cyberint allegedly made multiple efforts to notify Citrix of the incident but never received a response. That same month, “w0rm” supposedly tweeted a link of his blog post detailing the breach to Citrix but received no response.⁸⁵⁷

In 2016, Citrix’s popular remote-desktop-software company, GoToMyPC, forced all users to reset their passwords after they were “targeted by a very sophisticated password attack.”⁸⁵⁸

In December of 2018, Citrix forced password resets to protect against “credential stuffing.” This is where credentials such as usernames and passwords from other hacks are used to gain access to unaffiliated systems.⁸⁵⁹

In response to the 2019 breach, Citrix’s chief digital risk officer stated, “Certainly the incident that happened, if anything, made us more focused on the topic, and made us look even deeper at everything what we do[.]”

Regardless of the outcome of the lawsuit, businesses would do well to remember that according to the various state-level breach notification laws, they are responsible for their clients’ information held by third-party providers. In addition, businesses may be required by regulatory requirements or their cyber insurer, to assess the security of their service providers.

With that in mind, how should a business look to assess the cybersecurity of their cloud provider?

While there are several different methods that could be used, perhaps the most readily available, understandable, and pertinent choice for most businesses would be the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

CSA is a multinational organization with the stated goal of “defining and raising awareness of best practices to help ensure a secure cloud-computing environment.”⁸⁶⁰ Notably, the CCM is designed to create a shared matrix that is useful for both cloud vendors and prospective cloud customers.⁸⁶¹ Much like the NIST CSF discussed prior, the CCM provides a framework for businesses to conduct its due diligence in understanding the controls that various cloud providers put in place to secure their data.

While not mandated as an industry standard, CCM can be used as a standardized metric within an RFP to maximize a business’s security in a cloud environment. In addition, the CCM is mapped to various other standards that a business may be obligated to follow or are familiar with, such as HIPAA, PCI DSS, AICPA SOC, and NIST CSF. This will enable a business to maximize the probability that its client’s data will remain as secure as possible while also staying compliant within various other regulatory or contractual mandates.

CCM is categorized into the following 16 domains:

- Application and Interface Security (AIS)
- Audit Assurance and Compliance (AAC)
- Business Continuity Management and Operational Resilience (BCR)
- Change Control and Configuration Management (CCC)
- Data Security and Information Lifecycle Management (DSI)
- Datacenter Security (DCS)
- Encryption and Key Management (EKM)
- Governance and Risk Management (GRM)
- Human Resources (HRS)
- Identity and Access Management (IAM)
- Infrastructure and Virtualization Security (IVS)
- Interoperability and Portability (IPY)
- Mobile Security (MOS)
- Security Incident Management, E-Discovery, and Cloud Forensics (SEF)

- Supply Chain Management, Transparency, and Accountability (STA)
- Threat and Vulnerability Management (TVM)⁸⁶²

Within those primary domains listed above, there are roughly 130 different total controls to be considered. Thus, using a standardized metric for cloud-provider security could provide a robust method of maximizing security per dollar spent as well as maintaining compliance with various regulatory schemes.

While obviously, it is a good idea for a business to perform due diligence in keeping client information secure, it may also be mandatory. Consider the allegations and warnings of *In the Matter of GMR Transcription Services, Inc.*

GMR is a company that takes audio recordings from customers and has them transcribed into text format. The audio and transcript files can include names, dates of birth, social security numbers, driver's license numbers, tax information, and medical information.⁸⁶³

The FTC noted the following practices, which, they alleged, did not protect the information stored by GMR.

- GMR failed to require transcriptionists to adopt and implement reasonable security measures such as installing an anti-virus application.
- GMR failed to adequately assess the security of their contractor, Fedtrans.
- GMR failed to require that Fedtrans implement appropriate security measures to safeguard GMR client information.⁸⁶⁴

Due to these failures, the FTC alleged that Fedtrans' internal application stored client data in a readable text that was accessible to anyone and without authentication. Furthermore, a quick Internet search found the Fedtrans application and indexed thousands of sensitive client documents in their control.⁸⁶⁵

Under the terms of their settlement with the FTC, GMR agreed to a 20-year consent order. This includes having their information security program evaluated every two years by a certified third party. Also, GMR must establish a comprehensive information security program that ensures the information security of GMR as well as that of their service providers.⁸⁶⁶

The main takeaway for businesses is the understanding that they may be held responsible for the security of their vendors.

For any business with service providers that host client data, there are insurance considerations.

On the cyber insurance application, the business may be asked if they require vendors to demonstrate various information security protections. Or, they could be asked whether the business is auditing vendors to ensure they are meeting various

security standards. If a business answers in the affirmative but fails to perform the required due diligence on their vendors – and their cloud service provider – it could later result in a declination of coverage.

Action Items:

- ☐ Assess the security of all vendors to ensure they are meeting the same security requirements of the business;
- ☐ The Security Guidance for Critical Areas of Focus in Cloud Computing V.30 can be found for free at:
<https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>;
- ☐ The latest version of the CSA CCM can be found for free at:
https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview.

What are Written Information Security Programs & Policies?

Written Information security Program (WISP) and Information security Policies (ISPs), set the groundwork for what measures a business will utilize to protect sensitive information. Some businesses will create these documents as required by various laws such as Massachusetts' 201 CMR 17. Others will adopt them as part of demonstrating "reasonable" cybersecurity measures for various Safeguards Rule, HIPAA, or other federal-level requirements. Even without any legal requirements to do so, WISPs and ISPs are foundational for ensuring that the business and staff understand their cybersecurity obligations.

Broadly speaking, a WISP attempts to provide overarching guidance in the following areas:

- The purpose and scope of the program. This can include how the business defines personal information that requires specific safeguarding;
- Designation of an Information security Coordinator to implement the WISP, train users, and maintain records;
- Standardization of Risk Assessment frequency as well as actions to be taken following those assessments;
- The creation of information security policies and procedures that will be used by the business;
- An accounting of the minimum safeguards necessary to adhere to required laws and ensure the security of personal information;
- A requirement to oversee the security of various service providers;
- The monitoring and evaluation of the program to maintain security and address any shortcomings in security;
- The establishment of an Incident Response Plan (IRP);
- Enforcement for infractions of the WISP;
- A minimum yearly review of the WISP to address any material changes.⁸⁶⁷

As tempting as it would be for businesses to share a common WISP template, each business's WISP should be unique. Truly, the policies prescribed to a small business with an in-house server exposed to vast quantities of PHI will differ greatly from a large business which is entirely cloud-based and focused on the agricultural

industry. Standard templates can provide a useful starting point for developing a unique WISP, but a template is unlikely to satisfy unique business requirements in the eyes of regulators.

Furthermore, a business's WISP should be considered a living document. As required by the findings of ongoing risk assessments, security audits, and other internal or external findings, the WISP should be updated. Often, this can be accomplished by an IT compliance business, or a law firm specializing in privacy law.

Concurrent with development and implementation of a WISP is the development and implementation of the business's Information security Policy (ISP). While there will be a natural overlap between the two – an ISP is generally part of the WISP – the WISP can be thought of as a high-level document referenced by management, while the ISP is more of a document to be used by staff members.

At the heart of any ISP is the acknowledgment that technology is useful, but people will always be the weakest link. Staff may inadvertently break rules, fall victim to phishing attacks, or purposefully circumvent established controls. An ISP attempts to minimize these risks by clearly communicating business expectations to staff.⁸⁶⁸

Generally, ISPs should cover the minimum following areas:

- An introduction to staff which legitimizes the necessity of the document and the rules contained therein. This can include guiding principles, scope of the policy, resources for additional questions, notes on workplace privacy and monitoring, and regulatory compliance issues;
- A section on responsibilities in the workplace.

WISPs and ISPs can either be directly or indirectly referred to on a cyber insurance application. In the direct sense, an insurance provider may ask if the business has implemented and enforces an information security program or policy. More indirectly, the insurer may allude to such policies and programs by using alternative nomenclature, or implying compliance, typically, in questions referring to regulatory compliance. If the business is ever in doubt, they should seek guidance from legal counsel and query the underwriter for clarification. Failure to do so could lead to a declination of coverage.

For example, an insurer may pose the following question on an application: "Does the business comply with local, state, federal and international security and privacy laws affecting the business?" If the business had a Massachusetts resident as a client but had failed to develop a WISP in accordance with 201 CMR 17, any part of the claim involving that law, or the entire claim, could be denied by the insurer.

Action Items:

- ☐ Determine if your business is obligated to maintain a WISP.
- ☐ Work with legal counsel to meet any legal or technical requirements.
- ☐ Update the business's incident response plan and other internal documents as necessary.

The Golden Rules of Cyber

- **Rule #1:** If it's drastically cheaper than the other guy, it's probably run out of someone's basement.
- **Rule #2:** Big words do not equal big results. If they can't explain it to you in common terms, they don't understand it. When in doubt, ask them to draw a picture explaining where it works and how it fits into your system – see Rule #3.
- **Rule #3:** Einstein couldn't drive a car, so don't be afraid to look dumb. Ask probing questions and educate yourself on the topic. We all started from scratch with technology. The Internet is your friend.
- **Rule #4:** You can outsource responsibility, but not accountability.
- **Rule #5:** Talking about geographically isolated redundant backups stored in a nuclear blast-resistant underground facility is fun. Quality employee training and free coffee will probably keep you safer.
- **Rule #6:** The cloud is someone else's computer. Act accordingly.
- **Rule #7:** Everyone will get hacked. Have a breach response plan.
- **Rule #8:** If your breach response plan is only available on the computer that just got hit with ransomware, you don't have a breach response plan.
- **Rule #9:** There are no magic bullets. Defense-in-depth is your friend – an expensive but necessary friend.
- **Rule #10:** Should you buy that new fancy cybersecurity product? Consult your cybersecurity framework.
- **Rule #11:** If you don't have a cybersecurity framework, you probably shouldn't buy it.
- **Rule #12:** If you drive a \$100,000 car to work and complain about the cost of cybersecurity, you're missing the point.
- **Rule #13:** For anything cyber-related, beware of the self-labeled "experts." You probably want to talk with the guy who considers himself "pretty-damn-good." The first guy will probably screw you over; the second guy will let you know when there is a legitimate problem that he can't fix.

- **Rule #14:** IT makes information easy to get to. Cybersecurity makes information harder to get to. The two require constant balance.
- **Rule #15:** “Cyber-Secure” is a journey, not a destination.

Attorneys and Cybersecurity

An often-overlooked ally for a business needing assistance navigating the morass that is cyber insurance and cybersecurity law is a qualified attorney. As alluded to numerous times in this book, an attorney can provide invaluable assistance before, during, and after a breach.

Most cyber insurance policies should provide an attorney to assist with basic data-breach legal functions. This can include:

- Assisting in overall business response to a ransomware or data-breach incident;
- Coordinating breach notification responses;
- Coordinating vendor responses;
- Assisting businesses with computer forensic needs following a breach;
- Working with state and federal law enforcement entities;
- Short advice calls – generally, for up to one hour;
- Providing defense following government, regulatory investigations as well as for class action, or private litigation from data breaches.

There are numerous other cyber-related functions that a qualified attorney can provide a business that are not as apparent but just as crucial as those listed above. These may include the following services that are generally not provided by cyber insurance carriers, or their assigned legal counsel:

- Ongoing assessments of regulatory compliance issues in the international, federal, state, local, and industry-specific areas;
- Facilitating cybersecurity compliance, privacy, and network security audits;
- Counseling executives and the board of directors regarding risk-management strategies;
- Proactive liaising with government and state law enforcement as appropriate;
- Providing guidance regarding the cybersecurity risk of agreements, such as mergers and acquisitions, or corporate transactions;
- Providing contract review or negotiations of contracts as they pertain to data risks and disclosures;

- Enforcing contractual obligations against third parties;
- Assisting with cyber insurance applications to avoid material misrepresentations;
- Providing guidance regarding the policy language of various cyber insurance policies to provide the best coverage for each business's unique exposures;
- Guiding the business through potentially conflicting privacy or cybersecurity law issues;
- Assisting with conflicting data destruction and data retention policies;
- Providing further guidance on various privacy or cybersecurity law requirements not covered in this book.

While non-legal professionals may be able to provide some of the services listed above, perhaps the greatest benefit provided by an attorney is that of attorney-client privilege. This allows a company to likely keep information provided by the attorney from being disclosed to third parties such as regulators or government investigators. For this reason, many companies will retain an attorney to hire third-party cybersecurity assessors to perform their services. The findings of these assessments often disclose security flaws that may evidence a lack of compliance. For businesses who believe that they could face legal issues for these flaws, keeping the findings of assessments confidential is crucial.

As laws vary by state, businesses should check with local counsel to determine how attorney-client privilege applies to their unique needs and circumstances.

Finding Qualified Legal Counsel:

Boutique cybersecurity-law-focused firms or larger multi-disciplinary law firms may have the expertise to assist a business with these additional functions as they often have a dedicated privacy and cybersecurity law practice area. Given that these topics are such a multi-faceted, complex, and ever-changing area of the law, general counsel is unlikely to possess the resources or skills necessary to fully advise a business on their evolving exposures. In many instances, even businesses possessing in-house legal counsel may outsource their cybersecurity-law needs to a specialist. It is not advisable to rely on in-house or contracted IT staff to give legal recommendations. Insurance brokers are certainly ill-suited for this task.

When a business is looking to engage a cybersecurity attorney, they should heavily scrutinize their credentials and experience. Like any other specialty law area, the partner overseeing these engagements will often possess additional qualifications

specific to the field of cybersecurity law. This could include a master's degree in Cybersecurity Law, various IT or privacy law certifications, extensive practical experience – often in a government capacity, certified ABA Privacy Law Specialist, or something similar.

Regardless, due diligence should be a serious consideration for every business when retaining a privacy- and cybersecurity-law-focused attorney.

Action Items:

- ☐ If your business has not already done so, consider starting a relationship with qualified legal counsel to assist in the myriad of cybersecurity requirements your business is currently, or will shortly, face.

The Interesting Role of CPAs in Cybersecurity

A business speaking with their accountant about cybersecurity may seem like an odd scenario. Yet, businesses across the country are now engaging their accounting firm to provide cybersecurity-related services. Historically, CPAs have been required to evaluate the internal controls in financial statement audits since the early 1970s.⁸⁶⁹ This skillset evolved over nearly 50 years to the point that many businesses are now commonly speaking with their CPA firm about cybersecurity.

Mainly, these conversations and engagements appear to be driven by the board of directors, executives, and senior management. These groups are facing mounting pressure to oversee their business' cybersecurity risk management programs. Concurrently, they are being required to provide assurances to current and potential clients, investors, business partners, and regulators. For senior management – busy with the daily success of their business – it often makes sense to bring in outside expertise to provide third-party assurances. This is where accounting firms are increasingly providing valuable services.

Generally, cybersecurity engagements with accounting firms can be classified into three areas: traditional services that prove valuable for cybersecurity purposes; cybersecurity services proper – such as penetration testing, vulnerability scanning, and PCI Security; and System and Organization Controls (SOC) reports. Each will be discussed in turn.

Traditional Accounting Services

Not every accounting firm will have a practice area devoted to cybersecurity. Nor will every business necessarily have access to a local firm that could provide these services. This does not mean the “traditional” accounting firm does not have a role to play.

Consider the increasing threat of cybercrime and social engineering in light of the allegations found in *American Tooling Center v. Travelers Casualty & Surety Co.*

In this case, American Tooling Center (ATC) outsourced some of their manufacturing work to companies overseas. One of these companies was YiFeng Automotive Die Manufacturing company.⁸⁷⁰

ATC alleged that they paid vendors in four distinct payments. These payments were based on the progress of the order at the time. To facilitate these payments, the vendor would email ATC invoices. In turn, ATC would validate these payments through a multi-step process before money would be wired.⁸⁷¹

Per the court case, ATC alleges that employees would verify that the vendor completed the required elements for the payment schedule. The vice-president and treasurer of ATC would review a physical spreadsheet of the outstanding vendor payments and initiate a wire transfer. This wire transfer would need to be validated by ATC's assistant comptroller before the wire would be ultimately approved.⁸⁷²

Trouble arose when ATC's vice-president emailed his contact at YiFeng to request all outstanding invoices. Unbeknownst to ATC, a third party had intercepted this email and began impersonating Yi-Feng in their communications.⁸⁷³ ATC alleged that they had received an email from the "yifeng-rnould" domain, which was easily confused for the true domain of, "yifeng-mould." Note: the first domain contained an "r-n" combination to simulate the "m" in mould.⁸⁷⁴

Through the course of their communications, this third party was allegedly able to convince ATC that, due to an audit, a different account was to be used for all future wire payments. Prior to this communication, YiFeng had legitimately told ATC that it had changed its banking information, but ATC allegedly had no process to verify this change in information.⁸⁷⁵ This seemingly minor oversight would prove quite costly.

It wasn't until YiFeng demanded payment from ATC that the parties become aware of the scam.⁸⁷⁶ Ultimately, ATC had wired approximately \$834,000 to this unknown third party.⁸⁷⁷

When ATC submitted a claim to their insurer, Travelers, the claim was denied. ATC subsequently brought a claim against Travelers for a breach of contract that was denied on summary judgment by a district court.⁸⁷⁸ It took nearly three years from the loss until a judge at the U.S. Court of Appeals for the Sixth Circuit reversed the decision and remanded for further proceedings.⁸⁷⁹ While this is certainly good news for ATC, waiting years in litigation to recover funds of that magnitude is not an ideal situation.

As with many social engineering scams, it is often a minor oversight, or lack of internal controls, that tips the balance in favor of the malicious third party.

If a business is worried about this type of loss, and they likely should be, there are a myriad of services a traditional CPA firm could offer. So long as there is not third-party involvement, a business could simply request a consulting engagement. This would offer great flexibility with a minimum of work papers. A qualified CPA can look at how money is transferred in and out of the business and make improvements on internal controls. The goal is to mitigate the possible financial risks from social engineering such as those found in the previous case.

Technical Cybersecurity Services, Assessments, and Consulting

Many accounting firms are now offering technical cybersecurity services in addition to cybersecurity compliance and consulting services. Far from being comprised only of CPAs, these accounting firms, or their associated technology branch, come with a serious stable of credentials that are highly sought after in purely cybersecurity focused companies.

Below is a list of the technical cybersecurity services offered by selected CPA firms:

- Application penetration testing;
- Network penetrations testing;
- Social engineering testing;
- Implementation of cybersecurity controls;
- Cybersecurity framework implementation.

Below is a list of assessments, audits, and consulting engagements offered by selected CPA firms:

- System and Organization Controls (SOC): 1, 2, 3 & for Cybersecurity; discussed in detail later;
- PCI DSS Compliance such as PCI DSS, PA-DSS, and P2PE;
- ISO Certifications such as 27001, 9001, 22301, and 20000;
- Federal level assessments such as FedRAMP, FISMA, and NIST 800-53;
- Healthcare assessments such as HIPAA/HITECH, HITRUST CSF, and DEA EPCS audits;
- Privacy Law assessments such as GDPR, APEC, EU-US, and Swiss-US Privacy Shield, HIPAA, GLBA, COPPA, FERPA, TCPA, and 23 NYCRR 500;
- Financial assessments such as those for SWIFT, FFIEC, GLBA, NYDFS;
- Third-party risk management;
- Security of emerging technologies;
- Threat intelligence;
- IT Risk Assessments;

- Simulated CFPB Audits;
- Business Continuity and Disaster Recovery.

Beyond the convenience of working with an established and trusted partner, larger CPA firms likely have traditional accounting practice areas that focus on the industry in which a business operates. This could allow a business to benchmark their controls against those of their peers in the industry to determine “reasonability.” As described in another chapter, businesses attempting to conform with “reasonable cybersecurity” regulatory requirements must look at available technological solutions, strictly defined regulatory requirements, *as well as the common practices in their industry*.⁸⁸⁰

System and Organization Controls (SOC)

Only licensed CPAs will be able to offer firms System and Organization Controls (SOC) reports. Broadly, SOC reports are reports overseen by the AICPA, the governing body for CPA firms. There are four distinct categories – SOC 1, SOC 2, SOC 3, and SOC for Cybersecurity.

Below are some of the issues that may be addressed in SOC 1, SOC 2, or SOC 3 reports:

- Does the business have an organizational structure?
- Does the business have specific employees designated to create and implement procedures and policies?
- Does the business have background screening procedures, and do they have employee standards of conduct?
- Has the business conducted a formal risk assessment? Does that risk assessment identify potential threats, scrutinized the significance of those threats, and are they mitigation strategies for those defined risks?
- Does the business regularly assess vendor management?
- Does the business annually review policies and procedures?
- Does the business have a document retention policy?
- Has the business created and tested their incident response plan?
- Does the business have physical controls in place to limit access to sensitive data?

- Does the business update their hardware, software, and infrastructure as necessary?
- Does the business have an adequate backup and recovery policy for critical data?

SOC 1 Reports

A SOC 1 report focuses on an organization's controls that could be relevant to an audit of their customer's financial statements. In other words, a business is holding financial information that could affect their client's financial reporting.⁸⁸¹ For this reason, many SOC 1 reports are requested by current or potential customers of the service organization. Common businesses that may require a SOC 1 report could include payroll providers or Insurance Plan TPAs.

According to the attestation standards issued by the Auditing Standard Board, the purpose of a SOC 1 auditor is to:⁸⁸²

- .07a. obtain reasonable assurance about whether, in all material respects, based on the criteria
- i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period (or in the case of a type 1 report, as of a specified date)
 - ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the specified period (or in the case of a type 1 report, as of a specified date).
 - iii. when included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved throughout the specified period.
- b. express an opinion in a written report about the matters in paragraph .07a.

A common confusion regarding SOC 1 reports pertains to the difference between a SOC 1 – Type 1 report and a SOC 1 – Type 2 report. A SOC 1 – Type 1 report is a description of the controls of an organization for a specific date. Consequently, a control must be in place as of the date of the Type 1 report.⁸⁸³

A SOC 1 – Type 2 report comprises the same elements as a Type 1 report but with two key differences. The Type 2 report determines the suitability of controls over a specified period as opposed to a specific date. Thus, the controls should be in place and operating effectively over the period detailed in the engagement. Also, the

Type 2 report includes “a description of the tests of controls and the results thereof,” which is not found in the Type 1 report.⁸⁸⁴

For businesses considering this service, it may be advisable to first start with a SOC 1 – Type 1 report to establish a baseline. From that point forward, the SOC 1 – Type 2 report may be more beneficial to measure controls over a period of time.

Due to the detailed nature of SOC 1 reports, generally, only the management and auditors of the client’s business are allowed access.

SOC 2 Reports

SOC 2 reports are meant to test the security, availability, processing integrity, and confidentiality or privacy controls of service organizations. They are designed to give users assurance that the non-financial controls at service businesses are appropriately protecting client data.⁸⁸⁵ In other words, a client may ask, “How do I know my information is secure and available when necessary as promised by the vendor?” SOC 2 reports attempt to provide a third-party assurance to that question. Common business types that may require a SOC 2 include data centers, software developers, and MSPs.

Recall that SOC 1 reports may be required when a business is holding financial information that could affect their client’s financial reporting.⁸⁸⁶ By comparison, SOC 2 reports are generally required when a business is either hosting or processing client information that would not affect their financial reporting. A good example of a business type that might be required to perform a SOC 2 report would be a technology service organization that stores a client’s information in the cloud, such as a cloud-based on-demand software.

According to the AICPA Assurance Services Executive Committee (ASEC), SOC 2 reports can cover the following breadths of a business’ “information and systems [that are] (a) across an entire entity; (b) at a subsidiary, division, or operating unit level; (c) within a function relevant to the entity’s operational, reporting, or compliance objectives; or (d) for a particular type of information used by the entity.”⁸⁸⁷ The SOC 2 report will test whether management is “meeting its commitments to customers and system requirements.”⁸⁸⁸

Fundamentally, the SOC 2 report is based upon one or more of the AICPA’s Trust Services Criteria (TSC). The five SOC 2 TSCs are Security, Confidentiality, Processing Integrity, Availability, and Privacy.⁸⁸⁹

These criteria are generally described as the following:

Security: “Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could

compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.”⁸⁹⁰

Confidentiality: “Information designated as confidential is protected to meet the entity's objectives.”⁸⁹¹

Processing Integrity: “System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.”⁸⁹²

Availability: “Information and systems are available for operation and use to meet the entity's objectives.”⁸⁹³

Privacy: “Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.”⁸⁹⁴

Of note, these are general descriptions. Each of the criteria listed above contains a more in-depth explanation which can be found in the AICPA’s Trust Services Criteria document found at: <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf>

Much like SOC 1 reports, SOC 2 reports come in two varieties: SOC 2 – Type 1 and SOC 2 – Type 2. Both address the same relevant subject matter but contain key differences. SOC 2 – Type 1 reports are designed to cover the suitability of the design of the controls at the service organization.⁸⁹⁵ In comparison, a SOC 2 – Type 2 is designed to report on the same elements found in the Type 1 report, but also on their effectiveness.⁸⁹⁶

SOC 3 Reports

A SOC 3 report is essentially a SOC 2 report, but can be used for general distribution, such as being openly available on a website. The SOC 3 uses the same principles and guiding factors as the SOC 2 report, but contains limited descriptions.⁸⁹⁷ For this reason, many entities will add-on a SOC 3 report at the conclusion of their SOC 2 findings.

In totality, the necessity for a SOC 1, 2, or 3 report of either Type 1 or Type 2, can be a necessary but daunting decision. Businesses should seek guidance from a qualified CPA to determine their specific needs.

SOC for Cybersecurity

Management, directors of boards, business partners, and investors are increasingly briefed on the cybersecurity measures in their organization. Without being technologically savvy and able to get into the daily cybersecurity operations, how

would decision-makers know if everything is truly being accomplished as demonstrated? How does management know that their vendors are adhering to necessary cybersecurity requirements? Better yet, how do those responsible for the daily cybersecurity effectiveness of the business ensure that they aren't unknowingly overlooking crucial trends or details? This is where SOC for Cybersecurity comes into play. It may be just as common for decisions makers to request a SOC for Cybersecurity engagement as for those tasked with data security. Regardless of who requests the engagement, fresh eyes can provide crucial information for all involved.

Previously, the SOC reports described were for service organizations. Because other non-service organizations of differing sizes would benefit from a cybersecurity audit, the AICPA created SOC for Cybersecurity.

Fundamentally, SOC for Cybersecurity is an examination of the effectiveness of the organization's cybersecurity risk management program. This provides a useful benchmark for boards of directors, regulators, business partners, investors, and other interested parties to determine if they are meeting the needs required by the business.⁸⁹⁸

A SOC for Cybersecurity examination contains three main factors:⁸⁹⁹

1. A description by management of the business' cybersecurity risk-management program. In general, this is a prepared narrative that describes several features including how the entity identifies information assets, how they manage cybersecurity threats, policies, and procedures;
2. An assertion by management of their business' cybersecurity risk program at a specified point, or over a period of time;
3. The practitioner's report which states management's description of their risk management program was effective in meeting the entity's cybersecurity objectives.

For those entities holding PII, PHI, or PCI, it could be easily argued that a SOC for Cybersecurity engagement should be considered a mandatory yearly expense. Even a business holding no information considered protected under the various privacy and breach notification laws should still consider these engagements a mandatory expense. This is because every business has trade secrets, competitive advantages, and client lists that they would not want published online following a data breach; to say nothing of the potentially devastating effects of falling victim to ransomware.

Overall Applicability to Data Security in Vendor Agreements

As the world becomes more interconnected and businesses become more aware of their regulatory responsibilities, SOC reports will continue to become more common among the business community. Below are regulations that could require one or more of the various SOC reports to aid in compliance.

FTC general data security requirements should be kept in mind. Recall *In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekanth Srivastava, individually and as officers of GMR Transcription Services, Inc.* earlier in this book. In this matter, the FTC signaled that they will hold businesses responsible for the data security of vendors who receive sensitive information.⁹⁰⁰

Financial Institutions subject to GLBA should recall that GLBA could extend to any financial institution's vendor if the vendor could be deemed a service provider. Per the GLBA Safeguard's Rule, a covered entity must, "Oversee service providers, by (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards."⁹⁰¹

Covered entities subject to HIPAA must obviously implement appropriate safeguards. However, the covered entity must also contractually require the business associate to use appropriate safeguards that prevent use or disclosure of PHI other than permitted by the contract.⁹⁰² Moreover, the Security Standards require that the business associate, "implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronically protected health information that it creates, receives, maintains, or transmits..."⁹⁰³

Education institutions and their service providers subject to FERPA should recall how third parties should be supervised if they handle education records. Per FERPA, "A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions, may be considered a school official under this paragraph provided that the outside part... is under the direct control of the agency or institution with respect to the use and maintenance of education records."⁹⁰⁴

GDPR requires that data controller organizations using vendors that process personal data must ensure that the vendor is implementing appropriate technical and organizational safeguards to protect data.⁹⁰⁵

As noted previously, several states require business that maintain their resident's sensitive information create and implement a written information security plan. That plan will likely require oversight of service provider controls. Recall the previously

mentioned Massachusetts' 201 CMR 17 which states the following: "Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers..."⁹⁰⁶

The following states generally require reasonable safeguards which could include vendor safeguards oversight: Alabama,⁹⁰⁷ Arkansas,⁹⁰⁸ California,⁹⁰⁹ Colorado,⁹¹⁰ Connecticut,⁹¹¹ Delaware,⁹¹² Florida,⁹¹³ Illinois,⁹¹⁴ Indiana,⁹¹⁵ Kansas,⁹¹⁶ Louisiana,⁹¹⁷ Maryland,⁹¹⁸ Nebraska,⁹¹⁹ Nevada,⁹²⁰ New Mexico,⁹²¹ New York,⁹²² Oregon,⁹²³ Rhode Island,⁹²⁴ Texas,⁹²⁵ and Utah.⁹²⁶

Sector-specific laws such as the previously noted 23 NYCRR 500 may require that a covered entity ensure that third-party providers adequately protect sensitive information. Per 23 NYCRR 500.3: "Each Covered Entity shall implement and maintain a written policy or policies... setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: ... vendor and Third Party Service Provider management[.]"⁹²⁷

In total, there are a myriad of requirements by which a business could be obligated to assess and mandate appropriate safeguards from vendors. As more businesses take notice of this reality, the more likely that SOC reports – in their various iterations – will become commonplace.

Action Items:

- ☐ Businesses should consider speaking their accountant about a consulting engagement to assess internal controls that could limit the probability of wire fraud and social engineering.
- ☐ Speak with your accountant to determine if they offer any additional cybersecurity services which could add value to your business.
- ☐ If your business is considering a SOC engagement, consult with your accountant to determine which type(s) would be most appropriate.
- ☐ Speak with the board of directors concerning an SOC for Cybersecurity engagement to determine if this would assist them in their oversight capacity.
- ☐ As always, work with competent legal counsel to determine which cybersecurity and privacy laws may require you to assess and mandate cybersecurity requirements for vendors.

Section 9: Other Useful Publications from the Authors

Within this section are other useful publications from the authors. While the immediate audience was accounting firms across the nation, the fundamentals of each article can be applied to many other types of businesses. Understanding the knowledge contained within these articles can assist a business in creating a more holistic understanding of the cybersecurity threats they face.

Tips on Minimizing Wire Fraud

Many businesses have experienced losses that could have been avoided with basic countermeasures. Losses in this arena can range from small dollar amounts to millions, and the ability to recoup those funds is often circumstantial. Rather than worry about fund recovery after a breach, it is much simpler to avoid the problem altogether. As humans will always be the weakest link in any security program, it is vital that not only the appropriate internal controls are implemented, but that those controls are explained and strictly adhered to by staff and clients.

Thoroughly consider the measures below and discuss with your partners if and how they can help protect your practice. While the below list is no means a foolproof way to avoid all fraud, even basic checks can save you a lot of heartache. Remember, it's much easier for a criminal to use psychology and guile than to implement a complex and highly technical heist.

- Make an established policy to never approve the release of funds without speaking with your client over the phone. Consider using a pre-approved phone number. Having a client that is “too busy” to speak with you can also be a red flag to other problems that should warrant your interest.
- Avoid sending pre-filled wiring instructions. If, by circumstance, this is unavoidable, encrypt the email and send it to your client while you are already on the phone. This can help quickly confirm that they are in receipt of your instructions, and there is no ambiguity.⁹²⁸
- Use encryption for any personally identifiable information (PII). Failure to do so is not only bad practice; it may leave regulators knocking on your door.⁹²⁹ Consider this for tablets, company phones, laptops, and any other devices which can store or view this information.
- Give your employees the power to raise a red flag if something doesn't “feel” right. Make sure that they are communicating with clients via phone numbers that are registered and on file with your business. Be very wary of sending funds to new accounts in foreign countries and new locations.
- Use multi-step authentication.⁹³⁰ Consider a series of authentication questions to confirm the identity of your client. Common measures include a PIN number, codeword, and special authentication question. Pay special note to use information that cannot be readily found on a social media profile.

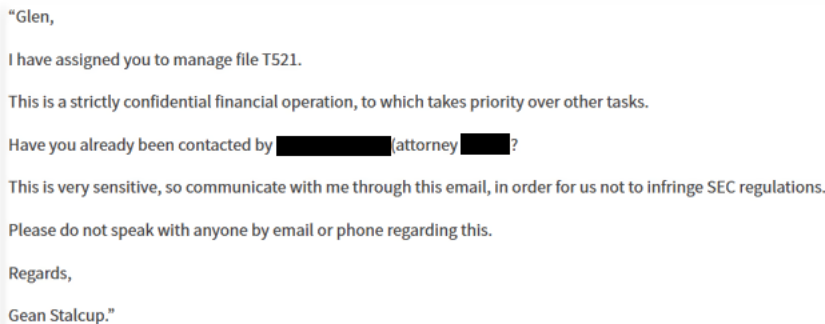
- Advise your clients to increase their security as well.⁹³¹ Complex passwords and two-step authentication to access email and sensitive information are a great start.

Remember that new technology can appear foolproof, but we are in a digital arms race with criminals where there is no clear advantage. As such, the human element will always be the most susceptible to fraud. Pay special heed to reinforce best practices with your employees and hold them accountable to abiding by your policies. Also, describe your security measures to new and existing clients immediately upon implementation. While no one wants to unnecessarily annoy a client, it's much easier to apologize for the inconvenience than to explain why their account is empty.

As a warning on how crucial a healthy degree of skepticism can save your business untold amounts of money and time, consider the allegations in the case of *Ameriforge Group Inc., d/b/a AFGlobal Corp. v. Federal Insurance Co.*

According to AFGlobal's original petition, they had originally purchased a \$3 million insurance policy from Federal Insurance Company, a division of Chubb Group.⁹³²

From May 21st, 2014 until May 27th of that same year, fraudulent emails impersonating AFGlobal's CEO, Gean Stalcup, were sent to the Director of Accounting, Glen Wurm.⁹³³

A screenshot of an email with a white background and a thin grey border. The text is in a standard sans-serif font. It begins with "Glen," followed by "I have assigned you to manage file T521." The next line is "This is a strictly confidential financial operation, to which takes priority over other tasks." This is followed by "Have you already been contacted by [REDACTED] (attorney [REDACTED])?" Then, "This is very sensitive, so communicate with me through this email, in order for us not to infringe SEC regulations." The next line is "Please do not speak with anyone by email or phone regarding this." The email ends with "Regards," and "Gean Stalcup." on separate lines.

"Glen,
I have assigned you to manage file T521.
This is a strictly confidential financial operation, to which takes priority over other tasks.
Have you already been contacted by [REDACTED] (attorney [REDACTED])?
This is very sensitive, so communicate with me through this email, in order for us not to infringe SEC regulations.
Please do not speak with anyone by email or phone regarding this.
Regards,
Gean Stalcup."

The imposter's email sent to Stalcup stated the following:⁹³⁴

Apparently, the imposter somehow knew the normal procedures of the company and knew that Wurm and Stalcup had a personal relationship. After approximately 30 minutes, Wurm was contacted by phone and email from the attorney that the due diligence fees associated with an acquisition in China in the amount of \$480,000 were required. Wurm then instructed the cash manager and treasurer of AFGlobal to transfer the funds.⁹³⁵

Nothing further was noted until May 27 when the imposter confirmed receipt of the funds, then asked for an additional \$18 million. It was then Wurm became suspicious and alerted his supervisors.⁹³⁶

Officers of AFGlobal attempted to retrieve the lost funds and attempted to recall the wire transfer from Bank of America. In addition, they alerted all the banks involved and their security departments of the perpetrated fraud. Finally, they filed a police report. Later, they were informed that the bank account which had received the money had been zeroed out and closed.⁹³⁷

Concurrently, AFGlobal had to make their brokerage firm, Aon Risk Services, aware of the loss. By June 2, the company had filed a formal proof-of-loss to their insurance carrier.⁹³⁸ They were seeking coverage under the Computer Fraud and Funds Transfer Fraud coverage elements of the policy.⁹³⁹

Approximately a month later, AFGlobal's insurer declined their claim. While their reasoning for declination is lengthy, it mainly centers around the policy definitions of "Computer Fraud" and "Funds Transfer Fraud" not being met as Wurm had knowingly authorized the transfer.⁹⁴⁰

Regardless of the outcome of the case, numerous points of failure are apparent. Foremost, AFGlobal should have enforced internal controls on wire transfers. A quick phone call or a face-to-face meeting could have saved AFGlobal \$480,000 plus legal costs. Assuming that no internal control is fool-proof, the risk manager should have "war-gamed" the scenario seen above and compared that to the insurance coverage offered.

Action Items:

- Review internal control procedures regarding the transfer of business or client funds;
- Review the business's cyber insurance policy and compare to different wargame scenarios to determine if there is a reasonable belief of coverage;
- Communicate this data to relevant stakeholders.

Russian Hackers Specifically Targeting Accounting Firms

(As seen in *CPA Practice Advisor* – June 2018)

Much to the ire of businesses worldwide, hackers have ceaselessly attempted to penetrate their computer systems and abscond with valuable information. While seemingly no business sector is beyond the reach of opportunistic hackers, the financial services industry has been particularly sensitive to these intrusions due to the vast quantities of personal information stored therein. Yet, like all systems found in the business world, specialization of skills is a natural outgrowth.

Unfortunately for accounting firms nationwide, this specialization has resulted in an alarming new finding. Hackers are now specifically targeting your firm. With most firms using relatively similar software and service providers, a flaw found in one system can be easily replicated in countless others. The game of cybersecurity cat-and-mouse is quickly accelerating against your firm.

“Authors: You’re most famous in the cybersecurity world for discovering some of the most high-profile breaches in history such as those at JPMorgan, Adobe, and Lexis Nexis. How did you discover that there is a gang of cybercriminals focusing on CPA firms?”

Alex Holden: We monitor a number of Dark Web forums and information exchanges. In this particular case, one of the lesser-known forums was used for this type of data exchange. Fortunately for us, hackers disclosed more information than they wanted to, allowing this glimpse into their activities.

Authors: Do you have any indication where these criminals are located geographically?

Alex: We have no clear indication of where they are from geographically. We can only assert that one of them spoke Russian natively but communicated in broken English.

Authors: Why would this group be focusing on accounting firms specifically?

Alex: I believe that the main direction is tax fraud. Accounting firms were targeted, but also other sources of W2 information and other financial data were on the targets list.

Authors: Is there a specific avenue of attack, such as keyloggers or ransomware, that these criminals prefer?

Alex: The CPA's computer had some kind of virus that allowed data-logging along with screenshots and keyboard inputs from the victim. This was non-disruptive, seamless, for the victim as likely the infection and operation of his computer.

Authors: Once the criminals have stolen data from these firms, how are they distributing the data?

Alex: The stolen data is not as useful as the hackers' ability to generate profits. This crime model deals more with tax refunds than any other abuse vector. It is unclear how if actual data was exfiltrated or was the victim's computer was used as a conduit to commit tax fraud.

Authors: In your experience, what size accounting firm are they targeting, and why?

Alex: Accounting firms are targeted not based on size but on opportunity. While larger firms may have dedicated IT and data security staff, they are also significantly attractive targets for potential profits. Yet smaller firms that operate on a one-on-one basis are easier targets because of a lack of data security measures. At the end of the day, you are likely to do business with a smaller firm because of personal touch and trust, but this personal touch may come with an expensive price tag of missing a lot of critical data security safeguards.

Authors: For a small accounting firm, with a very limited cybersecurity budget, if any, what are some cost-effective ways that can lessen their odds of being compromised that are often overlooked?

Alex: Smaller firms invest in commercial-grade accounting software, yet the data security side is far below the commercial-grade or may be missing. Basics: patch your system regularly, don't miss any updates; buy anti-virus and anti-malware software and keep it up-to-date; do not use your work computer for any other purpose than work; and lastly, become more educated about email scams, viruses, hoaxes – don't get victimized yourself and endanger your clients.

Authors: For large accounting firms with a dedicated cybersecurity budget, what is one area they continually overlook, but should pay much greater attention to?

Alex: Larger firms may not have a challenge with commercial-grade security software, yet the employees are still often tasked with the upkeep of their devices as they travel and do not always connect to the corporate networks. Stricter data security policies are definitely

needed. But what is usually lacking is a deeper understanding of security threats and poor password policies. End-user education around data security must be a paramount concern for larger firms, and re-using or assigning weaker passwords should not be tolerated.

Authors: What is Deep Web monitoring, and why would an accounting firm need such a service? Could they include this service for their own clients?

Alex: This tax season, we saw tax data of tens of thousands of victims traded on the Deep and Dark Web by hackers. At the same time, the exploitation of accounting firms is visibly on the rise, and this particular incident is not a unique occurrence. To see what hackers are targeting and if you are on a list of targets or victims is sometimes a quick check that may save you not only money but reputational loss. And knowing if your clients have already been compromised, in many cases, may allow you to help them proactively as recovery from tax fraud is not an easy task at all.

Authors: Understanding that no computer system is ever 100% secure, how important is a breach response plan, and when should a company start seeking assistance in crafting and implementing such a plan?

Alex: Breach or incident response planning is essential for a company of any size. Pretty much like dealing with any kind of incident (car accident, fire, etc.), it is much better to put some or a lot of thought into your response than trying to ad-lib during a crisis. Your ability to find the right partners that will help you with the recovery process cannot be hindered by the timing of a breach. Knowing whom to call, what to do, and how to respond is critical. In many cases, doing things the right way and quickly can minimize the impact of an incident.

Authors: Are there any new cybersecurity tools that you are particularly excited about that firms should be aware of?

Alex: I do not want to endorse any specific vendors but rather want to highlight technologies, many not new but enhanced. Anti-phishing solutions, ransomware protection, robust anti-virus, and anti-malware solutions, and Internet traffic filters preventing computers from going out to malicious sites.

Authors: Within the next five years, do you expect the frequency and severity of cyber breaches to increase or decrease, and why?

Alex: I believe that the overall amount of breaches is on a slow decline as security tools are getting better. However, the severity of each new breach will become more and more devastating as hackers are getting better at their evil tasks and not caring about the devastation they leave in their path.”

When asked for comment concerning the above revelations, Anthony Valach, counsel at BakerHostetler, cautioned accounting firms to consider the larger ramifications for their own clients. “It doesn’t matter what time of year it is. It’s always W-2 season. Remember, the main goal of these actors isn’t to steal someone’s identity. It’s to monetize the information as quickly as possible. If they get W-2s, they will try to file fraudulent tax returns.”

On a more optimistic note, he did add that many breaches he works on center around fundamental security measures that would have been easily rectified. “Yes, there are government-backed actors looking to cause chaos, but the run-of-the-mill hacker is trying to turn information into money as quickly as possible. If they can’t do that easily, or at least have a reasonable chance at doing so, they will move on to the next one.”

Garrett Wagner, CPA/CITP and founder of consulting firm C3 Evolution Group, emphasized the need to educate your staff. “Internally, they need to provide regular training and reminders to their staff about the various threats and email attacks currently being used.” Furthermore, he noted the often-overlooked client vulnerability saying, “Externally, they need to remind their clients of the tools they have to send secure communications. Nothing is worse than having all the tools and resources to keep data secure than to have all your clients email un-encrypted emails into the firm on a regular basis.”

No matter how secure you may think your computer systems may be, we are entering a new and dangerous phase for accounting firms worldwide. It is well worth the time and energy to commit to investigating new cybersecurity technologies and employee training programs. As with all things in life, the longer you wait, the more painful and costly the transition may become.

Cyber-Related Claims Without a Breach ... They're Coming

(Published April 2018 – *CPA Journal*)

A new series of cyber-related class-action claims against at least 15 law firms could have serious implications on how CPA firms, and many of their clients, manage their computer systems, and view data security. The most troubling aspect of the only-publicly-available complaint centers on these new claims is that there was no actual breach of confidential client information, merely the possibility of a breach (Gabe Friedman, “Class-Action Suit Targeting Law Firm Privacy Protections Could Be Unsealed,” Bloomberg Law, May 5, 2016, <http://bit.ly/2Fo0ryp>).

To make matters worse for potential defendants, claims such as these are probably uninsurable, so they could become quite costly to firms and their clients. It is no longer enough to avoid a data breach simply. Firms and clients must become proactive and deliberate about network and data security.

Shore v. Johnson & Bell

In the above-mentioned, publicly available complaint, two former clients of the law firm Johnson & Bell alleged that confidential client information had been put at risk due to inadequate data security [*Shore v. Johnson & Bell*, Case No. 16-cv-4363 (N.D. Ill. 2016), <http://bit.ly/2osxhGr>].

Namely, the complaint calls Johnson & Bell “a data breach waiting to happen” and claims that, among other computer-related issues, the “time record system could have been accessed without any username or password (or any other credentials).” The complaint further alleges that if a breach of this system were to occur, sensitive information would be easily stolen. Hackers could also obtain sensitive information from Johnson & Bell’s clients by impersonating the firm’s lawyers via email.

The four-count complaint alleges breach of contract (legal malpractice), negligence (legal malpractice), unjust enrichment, and breach of fiduciary duty. While the exact monetary damages are not stated, “the amount exceeds \$5,000,000.” In a conversation with the authors, Anthony Valach, counsel at BakerHostetler, said, “Since there was no breach, the class cannot allege out-of-pocket damages and must rely on the benefit-of-the-bargain measure of damages. Essentially, the class representatives allege that a portion of the fees paid to Johnson & Bell was to cover the administrative costs of protecting their data. Plaintiffs argue that the firm did not employ adequate measures to protect the data and are due a refund of those amounts because they did not receive the benefit of their bargain.”

When asked whether this type of claim could expand to other professions such as accounting firms, Valach stated, “Absolutely. It is easy to imagine a situation where professional services firms become the target of lawsuits for failing to employ reasonable measures to secure client data. Unfortunately, I think we are still at a point where many firms don’t think they are a target or don’t have data hackers would want. That’s a dangerous and potentially fatal attitude for a business. People don’t realize that on the Internet, we all live in a bad neighborhood. Ultimately, we may see the same effect as the Dodd-Frank Act. Small firms will be forced to choose between drastically increasing their cybersecurity budget and posture or face potential lawsuits and exposure from data breaches that can do lasting harm.”

The arbitration clause between the law firm and its former clients has, for the time being, saved the defendants from having to litigate this matter in the public eye. The court recently ruled that Johnson & Bell’s arbitration clause did not permit class-wide arbitration; only an individual action was permissible. As it currently stands, the plaintiffs will need to pursue individual arbitration, though their attorney, Jay Edelson, will likely appeal the decision (Derek Borchardt and Michael F. Buchanan, “Law Firm Sued for Alleged Lax Data Security Obtains Significant Win in District Court,” *Patterson Belknap Data Security Law Blog*, Mar. 8, 2017, <http://bit.ly/2HGjg0L>).

If Johnson & Bell wins the potential appeal, it may still need to weather two separate arbitration cases. In the meantime, the firm has filed a defamation suit against Edelson. Even if Johnson & Bell are victorious on all counts and cases, there may be irreparable reputational harm to their brand.

A quick Internet search for Johnson & Bell was telling. The first result was the firm’s website, followed by two headlines that could easily scare off existing or potential clients, resulting in unquantifiable future economic losses:

- “Chicago’s Johnson & Bell First U.S. Firm Publicly Named in Data Security Class Action”
- “Chicago Law Firm Accused of Lax Data Security in Lawsuit”

With data breaches constantly in the headlines, consumers are increasingly concerned about a company potentially mishandling their information. No matter how one views the merits of the case, no firm wants that type of publicity.

What if this was a CPA Firm?

It is only a matter of time until cases such as the above are brought against CPA firms. Do firms’ insurance policies cover such liability? Even as brokers specializing in this area for CPA firms, the authors’ research and experience leads to an uncomfortable answer: Maybe, but it is unlikely.

Professional liability and cyber-insurance carriers generally cover claims when a client demands money or services for damages due to professional services rendered. In this case, there did not seem to be any damages per se because a breach had not yet occurred. This leads to the potential for an uncovered claim where the firm may have to pay entirely out of pocket for defense and damages awarded.

The ability to perform a wholesale security scan of a firm's network is not only easy; it is free. According to Byron Patrick, managing director of the CPA Practice at Network Alliance: "Every vulnerability in this case is easily discernable from readily available online tools that are free. Port scans, vulnerability scans, penetration testing, etc., can all be conducted by a savvy 15-year-old with no formal cybersecurity training. It's unlikely the plaintiffs knocked the digital door down. All they needed to do was peek through the windows." He adds: "A disgruntled client could perform a quick Internet search, watch a few videos, and you're suddenly staring at a multimillion-dollar claim. It's terrifying for the accounting profession, and everyone should take this very seriously."

The authors reached out to the plaintiff's attorney in the case mentioned above, Jay Edelson, to gain insight into his thought process on these types of claims. When asked whether he would eventually pursue other professional services firms, such as CPAs, he replied: "We aren't specifically 'targeting' law firms, financial service firms, or any other companies. Rather, our focus is bringing cases where companies are (a) holding onto sensitive personal information, (b) likely can be the subject of cyberattacks, and (c) not using reasonable security measures. In some sense, we are going to the same places that hackers are going; our motivation is to get there first to force negligent actors to use better security measures so that a data breach never occurs. We have been very pleased with the success we have had to date and look forward to having an active role in ensuring corporate cyber-responsibility."

Taken in total, most CPA firms could easily match all three criteria mentioned. If Edelson is ultimately successful in any of his 15 class-action claims, this will embolden other attorneys to pursue similar cases against CPA firms. For partner groups that have not yet taken a proactive and sustained approach to network security, the circumstances above should give them plenty to speak about.

Action Items

- **Engagement letters.** In the Johnson & Bell case, an arbitration clause in an engagement letter proved valuable to the defendants. Firms should consider working with their professional liability insurers to review such engagement

letters and inquire about including, or updating, the arbitration or mediation clauses therein.

- **Vulnerability scanners.** These services attempt to identify susceptibilities in open ports, IP addresses, software, and operating systems. Once a system is scanned, a company specializing in this area can further assist with determining how much risk the firm is willing to tolerate in each component part of its computer system.
- **Third-party penetration testing.** This type of testing is performed by “white-hat” hackers to specifically target weaknesses and determine how vulnerable the firm is. It can be performed from both outside and inside the network, to give the firm a more robust picture of its total network security.
- **Warning clients.** As trusted advisors, CPA firms should ensure that clients are also aware of this new type of danger to their business. If the firm offers various IT services, this class-action claim should serve as a serious warning. Clients may ultimately need to reallocate resources, update software, and improve security processes, which may require significant time and resources.

There is no time like the present to take a proactive stance towards cybersecurity. Previously, merely avoiding a breach counted as a success, but this is no longer the case.

Use of Driver's License Numbers Raises Security Concerns

(Published March 2017 and July 2017 – *Journal of Accountancy*)

The IRS is now recommending that taxpayers use their driver's license number to provide another layer of security when electronically filing a federal tax return. A few states, notably New York, Ohio, and Alabama, are requiring a driver's license number, or an equivalent, for state returns. This sounds promising at first; another layer of verification to help prevent tax identity theft seems prudent. However, as with many other "good ideas," the unintended consequences can cause problems.

This new use for driver's license numbers should create concerns among CPA firms about data security and the potential for a cyber breach. Most CPA firm staff and clients have been trained to treat Social Security numbers (SSNs) with exceptional care, but the same has not been true necessarily with driver's license numbers (DLNs). While the reasons for that, explained below, are understandable. The increased relevance placed upon DLNs has made them a new high-value item for criminals and CPA firms alike.

Regulatory Requirements

Why do CPAs need to be concerned about the possibilities of a data breach involving driver's license numbers? The first reason is that while the 47 states' and territories' breach notification laws are different, they all qualify DLNs and SSNs as being equally important pieces of personally identifiable information (PII). And, while it's important to consult competent legal counsel to understand the breach laws pertaining to your firm, California's definition of personal information in its civil code regarding customer records (Cal. Civ. Code §1798.82) illustrates the point. Specifically, personal information includes but is not limited to the following:

- (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - (A) Social Security number;
 - (B) Driver's license number or California identification card number;
 - (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
 - (D) Medical information;
 - (E) Health insurance information. [Cal. Civ. Code §1798.82(h)]

As you can see, the driver's license number is given equal status with the SSN, and that's a concern because our experience indicates that a significant percentage of the population does not see DLNs as important as SSNs in the protection of personally identifiable information.

Views on Driver's License Numbers

To illustrate the types of attitudes we encounter regarding SSNs and driver's license numbers, we sent a couple of questions to 15 of our non-CPA but college-educated peers to determine how they view a lost DLN versus a lost SSN. While certainly not scientific, the answers they provided give a voice to the attitudes the authors have heard in the field.

Question #1: "What would you do if your Social Security card was lost or stolen?"

Selected answers: "Freak out," "Notify the credit agencies," "Watch my credit score like a hawk," "Purchase identity theft protection."

Question #2: "What would you do if your driver's license was lost or stolen?"

Selected answers: "Get a new one," "Ask my (spouse) if they've seen it," "Wait a week then go to the DMV," "Is that a big deal?"

The difference in answers is telling. Lost SSNs are generally understood to be a serious threat to identity theft. Lost DLNs are perceived as a mere inconvenience.

To gain insight into how CPA firms view this exposure, the authors conducted an anonymous survey with 29 respondents. Respondents came from varying levels of seniority, firm size, and geographic location. Again, the results are not scientific but are interesting:

We found that 55% of respondents said they are collecting DLNs, but 35% didn't know DLNs are considered PII. Contradictorily, nearly half were using unsecure methods of collecting DLNs from their clients.

When asked if their clients knew DLNs were PII, 72% responded either "No," or "Not sure."

The Risk

Now that driver's license numbers are being used as a form of identification verification for tax return filing, it's easy to see them becoming a high-value target for hackers and other cybercriminals. And, if accounting firms and their clients don't take care in protecting DLNs and other personally identifiable information, the results can be costly.

The Ponemon Institute's 2016 "Cost of a Data Breach" study illustrates how costly a security breach can be. The average total cost of a data breach for the nearly 400 companies studied came to \$4 million, or \$158 per each lost or stolen record. The costs were even higher in highly regulated industries, with an average cost of \$221 per stolen or lost record in the financial services section. Adding insult to injury, adverse media attention could further result lost business opportunities and revenue for years to come.

Insurance can offer some protection, but not as much as you might expect. CPA firms can find insurance for a number of items including credit monitoring for clients, forensic analysis of computer systems, removal of malware and system restoration, among others, but the Ponemon study found that insurance protection reduced the cost of a data breach by a mere \$5 per record.

CPA firms also have to be concerned that improper breach notification to a client could be a violation of rule 1.700, Confidential Information, in the AICPA Code of Professional Conduct and also lead to problems with various regulatory bodies and state attorneys general. While the penalties vary, in several states, fines can easily reach more than \$100,000, and violation of Internal Revenue Code Sec. 7216 can result in possible conviction for a misdemeanor with a fine of not more than \$1,000, and/or as much as a year in prison.

Action Items

Educating the public at large is well beyond the capability of most firms. Even the IRS Taxpayer Guide to Identify Theft and IRS Publication 4524, Security Awareness Tips for Taxpayers, fail to mention the safeguarding of a DLN at this point. Resources should be directed toward training staff to speak with clients and implementing appropriate security measures to minimize the possibility of a breach.

Train your staff: If you already have training on internal firm policies that deal with handling and storing PII, place an emphasis on DLNs. Because the costs to your firm losing an SSN and a DLN are likely the same, treat them equally. In turn, your staff should be the direct link to your clients, reinforcing the necessity for the minor inconvenience in properly handling PII.

Implement appropriate security tools: Most firms already have the tools in place to protect DLNs. Having previously implemented secure portals or encrypted email solutions to protect SSNs, it's simply a matter of educating your staff to leverage these tools they already have.

Secure portals such as Citrix ShareFile allow you to insert a request link into your email to the client. With this link, the client can send an image of their driver's license via an encrypted tunnel, protecting their DLN from nefarious characters.

Alternatively, using an encrypted email to exchange PII saves the steps required when using a portal. Solutions such as the Secure Messaging application from Mimecast allows you to send secure email messages to your client and allows them to send PII data securely.

Finally, it is easy to overlook a simple tool that has been available for years – your phone. A quick call to collect a DLN from your client is a simple and secure solution with a personal touch.

Should CPA Firms Be Worried About Data-Breach Claims?

Hurdles to Establishing Standing and Demonstrating Economic Viability

(Published March 2018 – *CPA Journal*)

Driven by unceasing news reports, CPA firms are growing increasingly concerned that data breaches are increasing in both frequency and severity. With this deluge of information, it is no surprise that partners and shareholders are increasingly concerned about the possibility of a client bringing a lawsuit following a data breach. But is this concern justified?

Although the general assumption is that one can be sued for anything, this is not necessarily true. Before a lawsuit can proceed in a federal court, and most state courts, a plaintiff must first demonstrate standing. As stated by the U.S. Supreme Court, “The question of standing is whether the litigant is entitled to have the court decide the merits of the dispute.” [*Warth v. Seldin*, 422 U.S. 490 (1975)].

Establishment of standing comprises three elements. First, the plaintiff must show that an injury occurred. Second, that injury must be traceable to the defendant’s (i.e., a CPA firm’s) unlawful conduct. Third, there must be a request for redressability for the unlawful act, usually in terms of a monetary award. In legal parlance, a plaintiff must demonstrate injury-in-fact, traceability, and redressability.

These elements are easily understood in common claims against CPA firms. For example, suppose a firm has undeniably miscalculated a tax deduction costing the client an additional \$1 million that is otherwise unrecoverable. Standing would be stated as follows:

- **Injury-in-fact:** The client suffered an injury of \$1 million due to the firm’s negligence.
- **Traceability:** The firm’s work documented the failure to provide correct calculations, resulting in overpayment.
- **Redressability:** The client wants the firm to reimburse the \$1 million, plus expenses.

When the same logic is applied to a data breach, however, how can these same principles be demonstrated? What injury could a client face? By now, it is almost certain that the information has been stolen somewhere else. Even if an individual client’s identity is stolen after the firm is breached, how could it be proven to be the

firm's fault? Even if all the above were true, what is the dollar value of, say, a Social Security number?

Injury-in-Fact

U.S. courts have not yet provided a definitive answer on what constitutes an injury-in-fact following a cyber breach. Some courts consider standing based upon the threat of future harm, but others refute this idea [Eric C. Surette, *Liability of Businesses to Governments and Consumers for Breach of Data Security for Consumers' Information*, 1 A.L.R.7th Art. 2 (2015)].

In *Krottner v. Starbucks Corp.* [628 F.3d 1139 (9th Cir. 2010)], a laptop was stolen containing the unencrypted names, addresses, and Social Security numbers of roughly 97,000 Starbucks employees. In response, Starbucks told the employees that there was “no indication that the private information has been misused.”

One plaintiff alleged that she “has been extra vigilant about watching her banking and 401(k) accounts” and has spent a “substantial amount of time doing so.” Another argued that he “has spent and continues to spend substantial amounts of time checking his 401(k) and bank accounts” and “has general anxiety and stress regarding the situation.” A third plaintiff said that someone attempted to open a bank account in his name, but the bank promptly thwarted those efforts, and he was subsequently notified. Nowhere in the pleading did any plaintiff allege that identity theft had occurred. Nevertheless, this was enough to satisfy the court that the increased risk of future identity theft was enough to establish injury-in-fact. Specifically, the court stated, “Plaintiffs-Appellants, whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing.”

While pleading the mere risk of identity theft may seem to establish injury-in-fact, not all courts are so easily persuaded. *Reilly v. Ceridian Corp.* [664 F.3d 38 (3rd Cir. 2010)] provides a useful illustration. Here, a claim was sought by the employees of a law firm after a breach at Ceridian exposed the personal and financial data of approximately 27,000 individuals at 1,900 companies. In response to the breach, Ceridian had sent letters notifying the affected parties and offered one free year of credit monitoring. Later that same year, a lawsuit was filed alleging that the plaintiffs “1) have an increased risk of identity theft, 2) incurred costs to monitor their credit activity, and 3) suffered from emotional distress.”

In this case, the court stated, “We cannot...describe how Appellants will be injured in this case without beginning our explanation with the word “if”: if the hacker read, copied, and understood the hacked information, and if the hacker attempts to use the information, and if he does so successfully, only then will Appellants have suffered an injury.” In short, the court held that the possible risk of

identity theft does not constitute an injury-in-fact without showing imminent or actual harm.

CPA firms should consider that establishing injury-in-fact is a nuanced exercise that depends on both the venue and the unique circumstances of the claim. Controlling the circumstances of a client is impossible and staying abreast of circuit court holdings is untenable. Therefore, it is advisable that firms start from the proposition that injury-in-fact will be established if even a single plaintiff alleges fraudulent activity following a breach.

Traceability

The alleged injury suffered by the plaintiffs must also be reasonably traceable to the breach suffered by the firm. While this sounds simple, the vast anonymity of the Internet provides a seemingly impossible hurdle to establishing traceability. Once again, however, the law is much more nuanced.

In *Resnick v. AvMed Inc.* [693 F.3d 1317 (11th Cir. 2012)], two laptops containing the personal information of roughly 1.2 million individuals were stolen and subsequently sold to a person known to deal in stolen property. Of note, two of the plaintiffs showed that prior to this incident, they had never previously been the victims of identity theft but became such directly following the breach.

The question before the court was whether these facts could be reasonably linked to the breach suffered by AvMed. As held by the court, “A showing that an injury is ‘fairly traceable’ requires less than a showing of ‘proximate cause.’ Plaintiffs became the victims of identity theft after the unencrypted laptops containing their sensitive information were stolen.” The judge reasoned that even though there was not incontestable proof that the identity theft resulted from the breach, there was enough of a rationally discernable link to satisfy the requirement of traceability.

Therefore, CPA firms should note that an assumption of deniability should not be considered a defense against traceability. Even an indirect link to injuries sustained by the plaintiffs may fulfill this requirement.

Redressability

Other common retorts to the impracticality of data-breach claims are the related ideas that either personal information has no value, or its value cannot be quantified. While these ideas may hold sway in casual conversation, they have no basis in the legal environment. As shown in multiple cases, the barrier to establishing standing often rests upon establishing the two prior mentioned elements, injury-in-fact and traceability.

When it comes to redressability, plaintiffs must show that a resolution in their favor will duly compensate their injuries [*Friends of the Earth Inc. v. Laidlaw Environmental Services, Inc.*, 528 U.S. 167 (2000)]. As is well known to those that have experienced a professional liability claim, plaintiffs often seek redress in terms of monetary damages. This area is no different.

Until a definitive national standard is formed, the ability of plaintiffs to establish standing in a data-breach-related case will continue to rest upon circumstances unique to the case, which are well outside the bounds of a CPA firm's control. While this sounds bleak, there is an additional factor that could provide relief: the economics of such claims.

Data-Breach Claims

Most states have specifically excluded any private right of action in their laws relating to data breaches (BakerHostetler, Data Breach Charts, July 2018, <http://bit.ly/2GJZRyL>). Those that have included such an action often limit the action to questions concerning the notification of, and not the alleged damages from, the breach. This effectively limits the potential award to the point where litigation may not be economically feasible (Paul G. Karlsgodt, "Key Issues in Consumer Data Breach Litigation," *Practical Law*, October/November 2014, <http://bit.ly/2GVYBrr>). In contrast, class-action claims are the preferred method of litigation following a data breach. Many breaches involve residents of multiple states, and class-action cases tend to focus more directly on whether a company was at fault for the data breach (Karlsgodt). This broader question allows attorneys to be more creative and expansive with the potential damages they seek.

A survey conducted by the author of 38 known class-action claims resulting from data breaches yields is encouraging for most CPA firms (see **Exhibit A – Case References** on the last page of this section). For claims where greater than 200,000 records were exposed, one anomalous defendant had \$30 million in revenue, and the rest generated multi-billion-dollar annual revenues. In cases where it was alleged that fewer than 200,000 records were exposed, each company, excepting one nonprofit medical organization and one government entity, had annual revenues exceeding \$600 million.

At present, the authors were unable to find a single case on file where the clients of accounting CPA firm have brought a claim following a data breach. Even the recent high-profile breach at Deloitte in September 2017 does not appear to have led to any legal action by the clients affected. Deloitte noted in its statement on the incident that "only very few clients were impacted" (Sept. 25, 2017, <http://bit.ly/2TaoxWB>). Though the exact number of affected clients remains

unknown, it was apparently small enough to make a class-action data-breach claim unpalatable to those involved. This further supports the idea that a business must have sizeable annual revenues and lose control over vast quantities of records to face a data-breach–related class-action claim.

This is not to say that smaller firms will forever be immune to class-action data-breach claims. It does, however, point to the current reluctance of plaintiffs' attorneys to be involved in pursuing legal action against entities if relatively few records have been exposed. Even if plaintiffs' attorneys are confident in their ability to establish standing, overcome significant legal hurdles, and win the case, the comparatively minor per capita awards make smaller class actions economically unappealing.

In short, the largest CPA firms should consider data-breach claims a possibility, remote and difficult as they may be, to end successfully for the plaintiff. For the time being, however, smaller- and mid-sized firms that do not possess vast quantities of personal information can rest a little easier.

Exhibit A - Case References

Case Reference	Alleged Records	Estimated Revenue - 2017 (Includes Parent)
Bell v. Axiom Corp., 2006 WL 2850042 (E.D. Ark. 2006)	1,600,000,000	\$880 Million
In re Yahoo! Inc. Customer Data Security Breach Litig., 2018 WL 1243332 (N.D. Cal. Mar. 9, 2018)	500,000,000	\$1.37 Billion
In re Target Corp. Data Sec. Breach Litigation, 2014 WL 7192478 (D. Minn. 2014)	110,000,000	\$71.88 Billion
In re Sony Gaming Networks and Customer Data Security Breach Litigation, 996 F. Supp. 2d 942 (S.D. Cal. 2014)	77,000,000	\$77.4 Billion
In re Adobe Systems, Inc. Privacy Litigation, 2014 WL 4379916 (N.D. Cal. 2014)	38,000,000	\$7.3 Billion
In re Anthem, Inc. Data Breach Litigation, 162 F. Supp. 3d 953 (N.D. Cal. 2016)	37,500,000	\$89.1 Billion
In re Zappos.com, Inc., Customer Data Sec. Breach Litigation, 893 F. Supp. 2d 1058, 95 A.L.R.6th 721 (D. Nev. 2012)	24,000,000	\$3.0 Billion
Hammond v. The Bank of New York Mellon Corp., 2010 WL 2643307 (S.D. N.Y. 2010)	12,500,000	\$3.9 Billion
In re Premiera Blue Cross Customer Data Security Breach Litigation	11,000,000	\$4.5 Billion
Fero v. Excellus Health Plain, Inc., 236 F. Supp. 3d 735, 753–54 (W.D.N.Y. 2017)	10,500,000	\$5.6 Billion
In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation, 45 F. Supp. 3d 14 (D.D.C. 2014)	4,700,000	\$4.5 Billion
In re: Community Health Systems, Inc., 2016 WL 4732630 (N.D. Al. 2016)	4,500,000	\$18 Billion
Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011)	4,200,000	\$18.3 Billion
In re Hannaford Bros. Co. Customer Data Security Breach Litigation, 2010 ME 93, 4 A.3d 492 (Me. 2010)	4,200,000	\$18.3 Billion
Moyer v. Michaels Stores, Inc., 2014 WL 3511500 (N.D. Ill. 2014)	3,000,000	\$5.2 Billion
Community Bank of Trenton v. Schnuck Markets, Inc. 887 F.3d 803 (7th Cir. 2018)	2,400,000	\$2.7 Billion
Key v. DSW, Inc., 454 F.Supp.2d 684 (S.D.Ohio 2006)	1,500,000	\$2.8 Billion
Chambliss v. Carefirst, Inc. 189 F. Supp. 3d 564 (D. Md. 2016)	1,100,000	\$8.8 Billion
Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014)	1,100,000	\$46 Billion
Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017)	1,100,000	\$8.8 Billion
Unchageri v. Carefirst of Maryland, Inc. 2016 WL 8255012 (C.D. Ill. 2016)	1,100,000	\$8.8 Billion
Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871 (N.D. Ill. 2014)	1,035,000	\$12.3 Billion
Amburg v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009)	700,000	\$4.5 Billion
Peters v. St. Joseph Services Corp., 74 F. Supp. 3d 847 (S.D. Tex. 2015)	405,000	\$6.5 Billion
In re Arby's Restaurant Group Inc. Litigation 2018 WL 3549783 (N.D. Ga. 2018)	350,000	\$3.5 Billion
Storm v. Paytime, Inc., 90 F.Supp. 3d 359 (M.D.Pa. 2015)	233,000	\$30 Million
Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007)	229,501	\$1.2 Billion
Shafra v. Harley-Davidson, Inc., 2008 WL 763177 (S.D. N.Y. 2008)	60,000	\$5.6 Billion
Lewert v. P. F. Chang's China Bistro, Inc., 819 F. 3d 963 (7th Cir. 2016)	60,000	\$1.2 Billion
Belle Chasse Automotive Care, Inc. v. Advanced Auto Parts, Inc., 2009 WL 799760 (E.D. La. 2009)	56,000	\$9.37 Billion
Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775 (W.D. Mich. 2006)	55,000	\$2.8 Billion
Remijas v. Neiman Marcus Group, LLC, 794 F. 3d 688 (7th Cir. 2015)	35,000	\$4.71 Billion
Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011)	27,000	\$600 Million
Khan v. Children's National Health System, 188 F.Supp.3d 524 (D. Md 2016)	18,000	Non-Profit
Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793 (M.D.La.2007)	17,000	\$53 Billion
Randolph v. ING Life Ins. and Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007)	13,000	\$20.7 Billion
Beck v. McDonald, 848 F. 3d 262 (4th Cir. 2017)	2,000	Government Entity
Smith v. Triad of Alabama, LLC, 2017 WL 1044692 (M.D. Al. 2017)	1,208	\$3.0 Billion

Section 10: Staying Current

Naturally, businesses should remain diligent in staying current with any changes in the law, or best practices. The following are a few of the many resources that businesses of all sizes may consider in this endeavor.

- The *Cybercrime Support Network* is a non-profit, public-private collaboration, created to assist businesses and individuals with preventing and responding to cybercrime. Their numerous thought leaders continuously update available to resources to provide the most pertinent information. They can be found at: <https://fraudsupport.org/>
- *Cybrary* is an IT Security education site. Most of the site is free and contains high quality courses on the topic of cybersecurity. They can be found at: <https://www.cybrary.it/>
- Brian Krebs is a world-renowned security blogger that has won countless awards for his reporting. His blog, *Krebs on Security*, is constantly updated to include the latest information on high profile breaches and threats. He can be found at: <https://krebsonsecurity.com/>
- BakerHostetler, is a nationwide law firm with a specialty in privacy and cybersecurity law. Their newsletter, the *Data Privacy Monitor* is constantly updated with the latest goings-on in the cyber specific legal arena. They can be found at: <https://www.dataprivacymonitor.com/>
- The International Association of Privacy Professionals (*IAPP*) is one of the world's leaders in certifying individuals as Privacy Professionals. Numerous resources exist to assist businesses in remaining current with the latest rulings and law changes. They can be found at: <https://iapp.org/>
- The United States Computer Emergency Readiness Team (*US-CERT*) contains a bevy of constantly updated cybersecurity warnings and information that is generally more appropriate for cybersecurity professionals. US-CERT can be found at: <https://www.us-cert.gov/>
- *InfraGard* is a partnership between the FBI and the private sector. This provides for a timely exchange of potentially sensitive information between government officials and businesses to remain current with the latest threats. Membership is required to participate. Visit <https://www.infragard.org/> for more information.

Damage Control

Author's Contact Information

Joseph E. Brunzman: joseph@cplbrokers.com

Daniel W. Hudson: dhudson@cplbrokers.com

References

-
- ¹ Caitlin Bronson, *One In Four Insurance Agents Will Be Gone By 2018* Insurance Business (2015), <https://www.insurancebusinessmag.com/us/news/marine/one-in-four-insurance-agents-will-be-gone-by-2018-17943.aspx> (last visited Apr 15, 2019).
- ² Global Cyber Security Insurance Market 2018 Size, Overview, Trends, Various Insurance Types, Applications, Key Player, REUTERS (2018), <https://www.reuters.com/brandfeatures/venture-capital/article?id=36676> (last visited Apr 15, 2019).
- ³ Facts Statistics: Industry overview, III, <https://www.iii.org/fact-statistic/facts-statistics-industry-overview> (last visited Apr 15, 2019).
- ⁴ Jeff Kosseff, *Cybersecurity Law* 92 Footnote 170 (2017)
- ⁵ Estimated using Hiscox Pro Privacy Pre-Priced Application PLPPVY A0001.
- ⁶ Laurent Heslault, *Actuaries Beware: Pricing Cyber Insurance Is A Different Ballgame*, LinkedIn (2017), <https://www.linkedin.com/pulse/actuaries-beware-pricing-cyber-insurance-different-laurent-heslault/> (last visited Apr 15, 2019).
- ⁷ *Cybersecurity Legislation 2018*, NCSL (2019), <http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx> (last visited Mar 13, 2019).
- ⁸ Lydia Dishman, *Why People In Finance And Insurance Are The Unhappiest Employees: Three factors contribute to the lack of job satisfaction, despite security and high wages* (2015), <https://www.fastcompany.com/3046257/why-finance-and-insurance-workers-among-the-unhappiest-employees> (last visited Apr 04, 2019).
- ⁹ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 224-225 (2018).
- ¹⁰ *Sarchett v. Blue Shield of California*, 43 Cal. 3d 1, 14–15, 729 P.2d 267, 276 (1987)
- ¹¹ Tyler Hale, Madeline Burke & Jeff Standridge, *THE HERITAGE COMPANY HOLDING GRAND RE-OPENING IN SHERWOOD AMP* (2019), <https://armoneyandpolitics.com/heritage-company-grand-reopening/> (last visited Mar 6, 2020).
- ¹² Shelby Rose, *SHERWOOD TELEMARKETING COMPANY TEMPORARILY SHUTS DOWN, BLAMES CYBER ATTACK RANSOM KATV* (2019), <https://katv.com/news/local/sherwood-telemarketing-company-temporarily-shuts-down-blames-cyber-attack-ransom> (last visited Mar 6, 2020).
- ¹³ *Stolen W-2 Tax Form Data Up for Grabs on the Dark Web*, DARK WEB NEWS (2017), <https://darkwebnews.com/dark-web/stolen-tax-form-up-for-grabs-on-dark-web/> (last visited Apr 15, 2019).
- ¹⁴ Andy Greenberg, *The Untold Story Of Notpetya, The Most Devastating Cyberattack In History* Wired (2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (last visited Apr 15, 2019).

-
- ¹⁵ What is hacktivism?, IT PRO (2018), <https://www.itpro.co.uk/hacking/30203/what-is-hacktivism> (last visited Apr 15, 2019).
- ¹⁶ Timeline of events associated with Anonymous, WIKIPEDIA (2019), https://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous (last visited Apr 15, 2019).
- ¹⁷ Estimating Password Cracking Times, BETTER BUYS, <https://www.betterbuys.com/estimating-password-cracking-times/> (last visited Apr 15, 2019).
- ¹⁸ Dwight B. Davis, CRYPTOJACKING FLUCTUATES ALONG WITH CRYPTOCURRENCY VALUES SYMANTEC (2019), <https://www.symantec.com/blogs/feature-stories/cryptojacking-fluctuates-along-cryptocurrency-values> (last visited Mar 6, 2020).
- ¹⁹ What is a man-in-the-middle attack?, SYMANTEC, <https://us.norton.com/Internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html> (last visited Apr 15, 2019).
- ²⁰ What is a man-in-the-middle attack?, SYMANTEC, <https://us.norton.com/Internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html> (last visited Apr 15, 2019).
- ²¹ Amanda C. Hauray, 10 Of the Most Costly Computer Viruses Of All Time Investopedia (2012), <https://www.investopedia.com/financial-edge/0512/10-of-the-most-costly-computer-viruses-of-all-time.aspx> (last visited Apr 02, 2019).
- ²² Kimberly Hutcherson, Six Days After A Ransomware Cyberattack, Atlanta Officials Are Filling Out Forms By Hand, CNN (2018), <https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html> (last visited Apr 15, 2019).
- ²³ Fred O'Connor, Fileless Malware 101: Understanding Non-Malware Attacks, Cybereason (2017), <https://www.cybereason.com/blog/fileless-malware> (last visited Apr 15, 2019).
- ²⁴ VPNFilter: New Router Malware with Destructive Capabilities, SYMANTEC (2018), <https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware> (last visited Apr 16, 2019).
- ²⁵ Alan Henry, The Difference Between Antivirus and Anti-Malware (and Which to use) (2013), <https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277>, (last visited May 15, 2019)
- ²⁶ Michael J., Chapple M., & Gibson D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 715 7th ed. (2015)
- ²⁷ Michael J., Chapple M., & Gibson D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 715 7th ed. (2015)
- ²⁸ Michael J., Chapple M., & Gibson D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 737 7th ed. (2015)
- ²⁹ Michael J., Chapple M., & Gibson D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 572 7th ed. (2015)

-
- ³⁰ Michael J., Chapple M., & Gibson D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 634 7th ed. (2015)
- ³¹ Michael J., Chapple M., & Gibson D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 642 7th ed. (2015)
- ³² <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf>
- ³³ The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932)
- ³⁴ Special Publication (SP) 800–167, Guide to Application Whitelisting, National Institute of Standards and Technology (NIST), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf>, (last visited Mar 06, 2020).
- ³⁵ In re Elli Lilly and Company, C-4047 (2002)
- ³⁶ In re RockYou, Inc. , CV-12-1487 (2012)
- ³⁷ In re Twitter, Inc., a corporation., C-4316 (2011)
- ³⁸ In re BJ’s Wholesale Club, Inc., a corporation., C-4148 (2005)
- ³⁹ In re PETCO Animal Supplies, Inc., a corporation., C-4133 (2005)
- ⁴⁰ In re Accretive Health, Inc., C-4432 (2014)
- ⁴¹ in re Reed Elsevier Inc. and Seisint, Inc., corporations., C-4226 (2008)
- ⁴² Start With Security: A Guide for Business, FEDERAL TRADE COMMISSION (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Jan 2020).
- ⁴³ Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees, DATABREACHES.NET (2010), <https://www.databreaches.net/rite-aid-settles-ftc-charges-that-it-failed-to-protect-medical-and-financial-privacy-of-customers-and-employees/> (last visited Mar 6, 2020).
- ⁴⁴ In re RITE AID Corporation, a corporation, C-4308 (2010)
- ⁴⁵ In re Goal Financial, LLC, a limited liability corporation., C-4216 (2008)
- ⁴⁶ In re Superior Mortgage Corporation, a corporation., C-4153 (2005)
- ⁴⁷ In re Fandango, LLC, a limited liability corporation., C-4481 (2014)
- ⁴⁸ UNITED STATES OF AMERICA, Plaintiff, v. VALUECLICK, INC., Hi-Speed Media, Inc., and E-Babylon, Inc., Defendants., 2008 WL 2127539 (C.D.Cal.)
- ⁴⁹ In re The TJX Companies, Inc., a corporation, (2008)
- ⁵⁰ Start with Security: A Guide for Business, FEDERAL TRADE COMMISSION (2020), <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> (last visited Mar 6, 2020).
- ⁵¹ FEDERAL TRADE COMMISSION, Plaintiff, v. Gregory NAVONE, Defendant., 2009 WL 2955963 (D.Nev.)
- ⁵² In re Franklin’s Budget Car Sales, Inc., also dba Franklin Toyota/Scion, a corporation, (2012)
- ⁵³ In re InfoTrax Systems, L.C., a limited liability company, and Mark Rawlins, C-4696 (2020)
- ⁵⁴ In re Credit Karma Inc., a corporation, C-4480 (2014)
- ⁵⁵ In re DSW Inc., a corporation C-1457 (2006)
- ⁵⁶ In re DSW Inc., a corporation C-1457 (2006)

-
- ⁵⁷ In re DSW Inc., a corporation C-1457 (2006)
- ⁵⁸ In re Dave & Buster's Inc., a corporation C-4291 (2010)
- ⁵⁹ In re Dave & Buster's Inc., a corporation C-4291 (2010)
- ⁶⁰ In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekanth Srivastava, individually and as officers of GMR Transcription Services, Inc., C-4482 (2014)
- ⁶¹ In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekanth Srivastava, individually and as officers of GMR Transcription Services, Inc., C-4482 (2014)
- ⁶² In re CardSystems Solutions, Inc., a corporation, C-4168 (2006)
- ⁶³ In re CardSystems Solutions, Inc., a corporation, C-4168 (2006)
- ⁶⁴ In re CardSystems Solutions, Inc., a corporation, C-4168 (2006)
- ⁶⁵ See generally: FTC website for decisions and orders.
- ⁶⁶ <https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/>
- ⁶⁷ <https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/>
- ⁶⁸ Dune Lawrence, A LEAK WOUNDED THIS COMPANY. FIGHTING THE FEDS FINISHED IT OFF BLOOMBERG.COM (2016), <https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/> (last visited Mar 7, 2020).
- ⁶⁹ Kevin L. Miller, What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach, Fla. B.J., September/October 2016, at 22, 24
- ⁷⁰ Fla. Stat. Ann. § 501.171 (West)
- ⁷¹ Ala. Code § 8-38-3
- ⁷² Nev. Rev. Stat. Ann. § 603A.210 (West)
- ⁷³ Or. Rev. Stat. Ann. § 646A.622 (West)
- ⁷⁴ State Data Breach Laws Substitute Notice Chart: Overview, Practical Law Practice Note Overview 6-601-7666
- ⁷⁵ Patco Const. Co. v. People's United Bank, 684 F.3d 197, 199 (1st Cir. 2012)
- ⁷⁶ Patco Const. Co. v. People's United Bank, 684 F.3d 197, 199 (1st Cir. 2012)
- ⁷⁷ Patco Const. Co. v. People's United Bank, 684 F.3d 197, 202 (1st Cir. 2012)
- ⁷⁸ Patco Const. Co. v. People's United Bank, 684 F.3d 197, 202 (1st Cir. 2012)
- ⁷⁹ Rule 1.6: Confidentiality of Information, AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/ (last visited Mar 7, 2020).
- ⁸⁰ Rule 1.6 Confidentiality of Information - Comment [18], AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/ (last visited Mar 7, 2020).
- ⁸¹ Ponemon cost of data breach studies, combined data from 2015-2019 reports. Individually available at www.ponemon.org
- ⁸² 2019 Ponemon Cost of Data Breach Study.

⁸³ 2015 Ponemon Cost of Data Breach Study.

⁸⁴ Patient Advisory, THE CENTER FOR FACIAL RESTORATION, <http://www.davisrhinoplasty.com/patient-advisory> (last visited Feb 15, 2020).

⁸⁵ Larry Dignan, RANSOMWARE ATTACKS: WHY AND WHEN IT MAKES SENSE TO PAY THE RANSOM ZDNET (2019), <https://www.zdnet.com/article/why-and-when-it-makes-sense-to-pay-the-ransom-in-ransomware-attacks/> (last visited Mar 7, 2020).

⁸⁶ Ransomware, RANSOMWARE | CISA, <https://www.us-cert.gov/Ransomware> (last visited Mar 7, 2020).

⁸⁷ Ionut Arghire, BETABOT STARTS DELIVERING CERBER RANSOMWARE SECURITYWEEK (2016), <https://www.securityweek.com/betabot-starts-delivering-cerber-ransomware> (last visited Mar 7, 2020).

⁸⁸ Dan Swinhoe, HOW HACKERS USE RANSOMWARE TO HIDE DATA BREACHES AND OTHER ATTACKS CSO ONLINE (2019), <https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html> (last visited Mar 7, 2020).

⁸⁹ UNITED STATES OF AMERICA, v. Faramarz Shahi SAVANDI and Mohammad Mehdi Shah Mansouri., 2018 WL 6798078 (D.N.J.)

⁹⁰ UNITED STATES OF AMERICA, v. Faramarz Shahi SAVANDI and Mohammad Mehdi Shah Mansouri., 2018 WL 6798078 (D.N.J.)

⁹¹ UNITED STATES OF AMERICA, v. Faramarz Shahi SAVANDI and Mohammad Mehdi Shah Mansouri., 2018 WL 6798078 (D.N.J.)

⁹² Ryuk ransomware targeting organisations globally, NCSC.GOV.UK (2019), <https://www.ncsc.gov.uk/news/ryuk-advisory> (last visited Mar 7, 2020).

⁹³ By, WHAT ARE RANSOMWARE ATTACK LOOPS AND HOW TO PREVENT THEM – ASIGRA BRIEFING NOTE STORAGESWISS.COM - THE HOME OF STORAGE SWITZERLAND (2018), <https://storageswiss.com/2018/06/29/ransomware-attack-loops-and-how-to-prevent-them-asigra/> (last visited Mar 7, 2020).

⁹⁴ JD Sherry, BYOD: BRING YOUR OWN DISASTER? BANKINFOSECURITY (2014), <http://www.bankinfosecurity.com/interviews/trend-micro-sherry-i-2352> (last visited Mar 7, 2020).

⁹⁵ More Than Half of Consumers Don't Password-Protect their Mobile Devices, SECURITY MAGAZINE RSS (2018), <https://www.securitymagazine.com/articles/89220-half-of-consumers-dont-password-protect-their-mobile-devices> (last visited Mar 7, 2020).

⁹⁶ More Than Half of Consumers Don't Password-Protect their Mobile Devices, SECURITY MAGAZINE RSS (2018), <https://www.securitymagazine.com/articles/89220-half-of-consumers-dont-password-protect-their-mobile-devices> (last visited Mar 7, 2020).

⁹⁷ Sam Bakken, INFOGRAPHIC: SURPRISING STATS EXPOSING MOBILE DATA DANGERS NOWSECURE (2019), <https://www.nowsecure.com/resource/infographic-surprising-stats-exposing-mobile-data-dangers/> (last visited Mar 7, 2020).

⁹⁸ Jai Vijayan, RANSOMWARE SITUATION GOES FROM BAD TO WORSE DARK READING (2019), <https://www.darkreading.com/attacks-breaches/ransomware-situation-goes-from-bad-to-worse/d/d-id/1336664> (last visited Mar 7, 2020).

-
- ⁹⁹ Verizon Mobile Security Index 2019, available at:
<https://enterprise.verizon.com/resources/reports/msi-2019-report.pdf>
- ¹⁰⁰ FACT SHEET: Ransomware and HIPAA, FACT SHEET: RANSOMWARE AND HIPAA, <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (last visited Mar 6, 2020).
- ¹⁰¹ 45 C.F.R. § 164.402
- ¹⁰² FACT SHEET: Ransomware and HIPAA, FACT SHEET: RANSOMWARE AND HIPAA, <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (last visited Mar 6, 2020).
- ¹⁰³ 45 C.F.R. § 164.402
- ¹⁰⁴ Conn. Gen. Stat. Ann. § 36a-701b (West)
- ¹⁰⁵ N.J. Stat. Ann. § 56:8-163 (West)
- ¹⁰⁶ 10 L.P.R.A. St § 4051 et seq.
- ¹⁰⁷ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/rules/interp/2018/33-10459.pdf> (last visited Mar 7, 2020).
- ¹⁰⁸ Alena Naiakshina & Anastasia Danilova, WORK GROUPS "IF YOU WANT, I CAN STORE THE ENCRYPTED PASSWORD." A PASSWORD-STORAGE FIELD STUDY WITH FREELANCE DEVELOPERS, https://net.cs.uni-bonn.de/fileadmin/user_upload/naiakshi/Naiakshina_Password_Study.pdf (last visited Mar 7, 2020).
- ¹⁰⁹ Toshihiko Takemura, STATISTICAL ANALYSIS ON RELATION BETWEEN WORKERS' INFORMATION SECURITY AWARENESS AND THE BEHAVIORS IN JAPAN NORTH AMERICAN BUSINESS PRESS, <http://t.www.na-businesspress.com/JMPP/TakemuraWeb.pdf> (last visited Mar 7, 2020).
- ¹¹⁰ Robert Yanus, CRITICAL SUCCESS FACTORS FOR MANAGING AN INFORMATION SECURITY AWARENESS TRAINING PROGRAM PACE UNIVERSITY (2007), <http://support.csis.pace.edu/CSISWeb/docs/techReports/techReport238.pdf> (last visited Mar 7, 2020).
- ¹¹¹ 2019 Ponemon Cost of Data Breach Study.
- ¹¹² 2019 Ponemon Cost of Data Breach Study.
- ¹¹³ Robert Half Technology, SURVEY: NEARLY A QUARTER OF WORKERS WILL PUT IN MORE TIME AT WORK THIS CYBER MONDAY (SHOPPING, THAT IS) PR NEWswire: PRESS RELEASE DISTRIBUTION, TARGETING, MONITORING AND MARKETING (2018), <https://www.prnewswire.com/news-releases/survey-nearly-a-quarter-of-workers-will-put-in-more-time-at-work-this-cyber-monday-shopping-that-is-300557101.html> (last visited Mar 7, 2020).
- ¹¹⁴ Editor, BYOD FOR BUSINESS IS ON THE RISE - ITSPMAGAZINE ITSPMAGAZINE: AT THE INTERSECTION OF TECHNOLOGY, CYBERSECURITY, AND SOCIETY. ITSPMAGAZINE (2018), <https://www.itspmagine.com/from-the-newsroom/byod-for-business-is-on-the-rise> (last visited Mar 7, 2020).
- ¹¹⁵ Ivan Dimov, SECURITY AWARENESS STATISTICS INFOSEC RESOURCES, <https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-fundamentals/security-awareness-statistics/> (last visited Mar 7, 2020).

¹¹⁶ Ross Kelly, ALMOST 90% OF CYBER ATTACKS ARE CAUSED BY HUMAN ERROR OR BEHAVIOR CHIEFEXECUTIVE.NET (2017), <https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/> (last visited Mar 7, 2020).

¹¹⁷ Survey of metrics from Ponemon 2015-2019 studies.

¹¹⁸ Andrea Arias, THE NIST CYBERSECURITY FRAMEWORK AND THE FTC FEDERAL TRADE COMMISSION (2019), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc> (last visited Mar 7, 2020).

¹¹⁹ Kevin L. Miller, What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach, Fla. B.J., September/October 2016, at 22, 24

¹²⁰ State Data Breach Laws Substitute Notice Chart: Overview, Practical Law Practice Note Overview 6-601-7666 (West)

¹²¹ Or. Rev. Stat. Ann. § 646A.622 (West)

¹²² NY S.5575B/A.5635 § 4 (effective March 21, 2020), available at: <https://legislation.nysenate.gov/pdf/bills/2019/S5575B>

¹²³ Kamala D. Harris, CALIFORNIA DATA BREACH REPORT 2016 CALIFORNIA OFFICE OF THE ATTORNEY GENERAL (2016), <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf> (last visited Mar 7, 2020).

¹²⁴ Center for Internet Security: Download the CIS Controls, CENTER FOR INTERNET SECURITY: DOWNLOAD THE CIS CONTROLS, https://learn.cisecurity.org/control-download?utm_campaign=Controls&utm_medium=email&_hsenc=p2ANqtz-_i2_5cOk0mpwfIOnmDbojyCDCI5VP3dhKqbEUh5q2RhgaXg9aCP4AiGWEihRIQfTKdvVjg7rDkbDILLpC1RPabF1XN-g&_hsmi=48404281&utm_source=hs_automation&utm_content=48404281&hsCtaTracking=9689e0d4-3a83-4169-a989-6a360e1d8a92|801e2b6a-ce35-4d2e-992e-b084680409ef (last visited Mar 7, 2020).6a360e1d8a92%7C801e2b6a-ce35-4d2e-992e-b084680409ef

¹²⁵ Cal. Civ. Code § 1798.155(b)

¹²⁶ Andrea Arias, THE NIST CYBERSECURITY FRAMEWORK AND THE FTC FEDERAL TRADE COMMISSION (2019), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc> (last visited Mar 7, 2020).

¹²⁷ Andrea Arias, THE NIST CYBERSECURITY FRAMEWORK AND THE FTC FEDERAL TRADE COMMISSION (2019), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc> (last visited Mar 7, 2020).

¹²⁸ Nicole.keller@nist.gov, FRAMEWORK DOCUMENTS NIST (2019), <https://www.nist.gov/cyberframework/framework> (last visited Mar 7, 2020).

¹²⁹ ¹²⁹ Center for Internet Security: Download the CIS Controls, CENTER FOR INTERNET SECURITY: DOWNLOAD THE CIS CONTROLS, https://learn.cisecurity.org/control-download?utm_campaign=Controls&utm_medium=email&_hsenc=p2ANqtz-_i2_5cOk0mpwfIOnmDbojyCDCI5VP3dhKqbEUh5q2RhgaXg9aCP4AiGWEihRIQfTKdvVjg7rDkbDILLpC1RPabF1XN-g&_hsmi=48404281&utm_source=hs_automation&utm_content=48404281&hsCtaTracking=9689e0d4-3a83-4169-a989-6a360e1d8a92|801e2b6a-ce35-4d2e-992e-b084680409ef

g&_hsmi=48404281&utm_source=hs_automation&utm_content=48404281&hsCtaTracking=9689e0d4-3a83-4169-a989-6a360e1d8a92|801e2b6a-ce35-4d2e-992e-b084680409ef (last visited Mar 7, 2020).6a360e1d8a92%7C801e2b6a-ce35-4d2e-992e-b084680409ef

¹³⁰ Mimecast, CYBERSECURITY BREAKDOWN: IMPROVING WORKPLACE AWARENESS MIMICAST BLOG (2018), <https://www.mimecast.com/blog/2018/12/cybersecurity-breakdown-improving-workplace-awareness/> (last visited Mar 7, 2020).

¹³¹ Curry v. Schletter Inc., No. 1:17-CV-0001-MR-DLH, 2018 WL 1472485, at *1 (W.D.N.C. Mar. 26, 2018)

¹³² Curry v. Schletter Inc., No. 1:17-CV-0001-MR-DLH, 2018 WL 1472485, at *1 (W.D.N.C. Mar. 26, 2018)

¹³³ Curry v. Schletter Inc., No. 1:17-CV-0001-MR-DLH, 2018 WL 1472485, at *1 (W.D.N.C. Mar. 26, 2018)

¹³⁴ Curry v. Schletter Inc., No. 1:17-CV-0001-MR-DLH, 2018 WL 1472485, at *2 (W.D.N.C. Mar. 26, 2018)

¹³⁵ Curry v. Schletter Inc., No. 1:17-CV-0001-MR-DLH, 2018 WL 1472485, at *2 (W.D.N.C. Mar. 26, 2018)

¹³⁶ Andy Klein, HARD DRIVE COST PER GIGABYTE BACKBLAZE BLOG | CLOUD STORAGE & CLOUD BACKUP (2019), <https://www.backblaze.com/blog/hard-drive-cost-per-gigabyte/> (last visited Mar 7, 2020).

¹³⁷ See generally *State of Washington v. Uber Technologies, Inc.*, Office of the Attorney General of Washington State (2017), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2017_11_28Complaint.pdf (last visited Feb 28, 2019).

¹³⁸ Joseph Brunsman & Daniel Hudson, SHOULD CPA FIRMS BE WORRIED ABOUT DATA BREACH CLAIMS? THE CPA JOURNAL (2019), <https://www.cpajournal.com/2019/04/19/should-cpa-firms-be-worried-about-data-breach-claims/> (last visited Mar 7, 2020).

¹³⁹ Pamela C. Williams & John D. Martin, Hoarders Beware: Defensible Data Disposal Is Good Business, ACC Docket, May 2013, at 26, 28

¹⁴⁰ Pam Greenberg, DATA DISPOSAL LAWS DATA DISPOSAL LAWS, <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx> (last visited Mar 7, 2020).

¹⁴¹ Ala. Code § 8-38-10

¹⁴² N.Y. Gen. Bus. Law § 899-bb(2) (McKinney)

¹⁴³ N.Y. Gen. Bus. Law § 899-aa(d)(2) (McKinney)

¹⁴⁴ N.Y. Gen. Bus. Law § 899-bb(2)(C) (McKinney)

¹⁴⁵ Or. Rev. Stat. Ann. § 646A.622(1) (West)

¹⁴⁶ Or. Rev. Stat. Ann. § 646A.622(C) (West)

¹⁴⁷ *In re BJ's Wholesale Club, Inc.*, a corporation., C-4148 (2005)

¹⁴⁸ *In re BJ's Wholesale Club, Inc.*, a corporation., C-4148 (2005)

¹⁴⁹ The Aftermath of a Data Breach: Consumer Sentiment, Ponemon Institute, April 2014. Available at:

<https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf>

¹⁵⁰ Khalid Saleh, CUSTOMER ACQUISITION VS.RETENTION COSTS – STATISTICS AND TRENDS THE INVEBP BLOG: CONVERSION RATE OPTIMIZATION BLOG (2019), <https://www.invespcro.com/blog/customer-acquisition-retention/> (last visited Mar 7, 2020).

¹⁵¹ Information Resellers Consumer Privacy Framework Needs To Reflect Changes In Technology And The Marketplace (2013), <https://www.gao.gov/assets/660/658151.pdf> (last visited Feb 7, 2019).

¹⁵² U.S. House Committee on Financial Services, Blaine Luetkemeyer & Carolyn B. Maloney, Data Acquisition and Technology Accountability and Security Act (Discussion Draft (115AD). Available at: https://financialservices.house.gov/uploadedfiles/03.07.2018_data_s_bill.pdf

¹⁵³ Lisa Madigan *et al*, Thoughts on The Proposed Data Acquisition And Technology Accountability And Security Act (2018), [https://buckleyfirm.com/sites/default/files/Buckley Sandler InfoBytes - State AGs Data Breach Letter to Congress 2018.03.19.pdf](https://buckleyfirm.com/sites/default/files/Buckley%20Sandler%20InfoBytes%20-%20State%20AGs%20Data%20Breach%20Letter%20to%20Congress%202018.03.19.pdf) (last visited Mar 12, 2019). Signed by 32 State Attorneys General.

¹⁵⁴ U.S. Const. art. VI, cl. 2

¹⁵⁵ Md. Code Ann., Com. Law § 14-3504 (West)

¹⁵⁶ D.C. Code Ann. § 28-3852 (West)

¹⁵⁷ Va. Code Ann. § 18.2-186.6 (West)

¹⁵⁸ Md. Code Ann., Com. Law § 14-3504 (West)

¹⁵⁹ D.C. Code Ann. § 28-3852 (West)

¹⁶⁰ Va. Code Ann. § 18.2-186.6 (West)

¹⁶¹ State Data Breach Laws Substitute Notice Chart: Overview, Practical Law Practice Note Overview 6-601-7666

¹⁶² Cal. Civ. Code § 1798.82 (West)

¹⁶³ Data Breach Charts, (2018),

[https://www.bakerlaw.com/files/uploads/documents/data breach documents/data_breach_charts.pdf](https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf) (last visited Sep 2018).

¹⁶⁴ N.C. Gen. Stat. Ann. § 75-66

¹⁶⁵ Okla. Stat. Ann. tit. 24, § 162 (West)

¹⁶⁶ Ohio Rev. Code Ann. § 1349.19 (West)

¹⁶⁷ Vt. Stat. Ann. tit. 9, § 2430 (West)

¹⁶⁸ Data Breach Charts, (2018),

[https://www.bakerlaw.com/files/uploads/documents/data breach documents/data_breach_charts.pdf](https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf) (last visited Sep 2018).

¹⁶⁹ N.C. Gen. Stat. Ann. § 75-65

¹⁷⁰ Wash. Rev. Code Ann. § 19.255.010 (West)

¹⁷¹ CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays \$2.25 Million to Settle Allegations of HIPAA Violations, FEDERAL TRADE COMMISSION (2015),

<https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial> (last visited Mar 20, 2019).

¹⁷² CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays \$2.25 Million to Settle Allegations of HIPAA Violations, FEDERAL TRADE COMMISSION (2015), <https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial> (last visited Mar 20, 2019).

¹⁷³ CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays \$2.25 Million to Settle Allegations of HIPAA Violations, FEDERAL TRADE COMMISSION (2015), <https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial> (last visited Mar 20, 2019).

¹⁷⁴ N.Y. Gen. Bus. Law § 899-aa (McKinney)

¹⁷⁵ N.J. Stat. Ann. § 56:8-163 (West)

¹⁷⁶ Fla. Stat. Ann. § 501.171 (West)

¹⁷⁷ Fla. Stat. Ann. § 501.171 (West)

¹⁷⁸ S.C. Code Ann. § 39-1-90

¹⁷⁹ Tenn. Code § 47-18-2107

¹⁸⁰ Mich. Comp. Laws Ann. § 445.72 (West)

¹⁸¹ Boardman Molded Products Inc., v. Involta, LLC, 2020-CV-00154.

¹⁸² Boardman Molded Products Inc., v. Involta, LLC, 2020-CV-00154.

¹⁸³ Boardman Molded Products Inc., v. Involta, LLC, 2020-CV-00154.

¹⁸⁴ Neb. Rev. Stat. 87-801 *et seq.*

¹⁸⁵ Minn. Stat. Ann. § 325E.61 (West)

¹⁸⁶ Tex. Bus. & Com. Code Ann. § 521.053 (West)

¹⁸⁷ Ga. Code Ann. § 10-1-912 (West)

¹⁸⁸ Data Breach Charts, (2018),

https://www.bakerlaw.com/files/uploads/documents/data_breach_documents/data_breach_charts.pdf (last visited Sep 2018).

¹⁸⁹ Wis. Stat. Ann. § 134.98 (West)

¹⁹⁰ Fla. Stat. Ann. § 501.171 (West)

¹⁹¹ State Data Breach Laws Substitute Notice Chart: Overview, Practical Law Practice Note Overview 6-601-7666

¹⁹² S.C. Code Ann. § 39-1-90

¹⁹³ State Data Breach Laws Substitute Notice Chart: Overview, Practical Law Practice Note Overview 6-601-7666

¹⁹⁴ State Data Breach Laws Substitute Notice Chart: Overview, Practical Law Practice Note Overview 6-601-7666

¹⁹⁵ R.I. Gen. Laws § 11-49.2-5.

¹⁹⁶ R.I. Gen. Laws § 11-49.2-5.

¹⁹⁷ Haw. Rev. Stat. Ann. § 487N-2 (West)

¹⁹⁸ Fla. Stat. Ann. § 501.171 (West)

¹⁹⁹ Wash. Rev. Code Ann. § 19.255.010 (West)

-
- ²⁰⁰ State of Washington v. Uber Technologies, Inc., Office of the Attorney General of Washington State (2017), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2017_11_28Complaint.pdf (last visited Feb 28, 2019).
- ²⁰¹ State of Washington v. Uber Technologies, Inc., Office of the Attorney General of Washington State (2017), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2017_11_28Complaint.pdf (last visited Feb 28, 2019).
- ²⁰² State of Washington v. Uber Technologies, Inc., Office of the Attorney General of Washington State (2017), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2017_11_28Complaint.pdf (last visited Feb 28, 2019).
- ²⁰³ State of Washington v. Uber Technologies, Inc., Office of the Attorney General of Washington State (2017), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2017_11_28Complaint.pdf (last visited Feb 28, 2019).
- ²⁰⁴ Key Issues in Consumer Data Breach Litigation, Practical Law Practice Note 5-582-9285
- ²⁰⁵ John M. Parker, Data Security Law- Who Can Enforce Violations of Data Security Breach Notification Statutes?-in Re Target Corp. Data Security Breach Litigation, No. 14-2522, 2014 WL 7192478 (D. Minn. Dec. 18, 2014)., 38 Am. J. Trial Advoc. 631, 633 (2015)
- ²⁰⁶ Jeff Kosseff, Cybersecurity Law 65 (2017)
- ²⁰⁷ Jeff Kosseff, Cybersecurity Law 65 (2017)
- ²⁰⁸ Jeff Kosseff, Cybersecurity Law 65 (2017)
- ²⁰⁹ California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West)
- ²¹⁰ California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West)
- ²¹¹ California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West)
- ²¹² California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West)
- ²¹³ Kamala D. Harris, CALIFORNIA DATA BREACH REPORT 2016 CALIFORNIA OFFICE OF THE ATTORNEY GENERAL (2016), <https://oag.ca.gov/sites/all/files/agweb/pdfs/db/2016-data-breach-report.pdf> (last visited Mar 7, 2020).
- ²¹⁴ Janine Anthony Bowen *et al.*, Overview of the New California Consumer Privacy Law (2018), <https://www.dataprivacymonitor.com/wp-content/uploads/sites/5/2019/01/Overview-of-the-New-California-Consumer-Privacy-Law.pdf> (last visited Mar 2, 2019).
- ²¹⁵ Don Jergler, CYBER ALERT: NEW ERA IN PRIVACY LIABILITY TO BEGIN. CALIFORNIA'S DATA PRIVACY LAW COULD BE GAME-CHANGER INSURANCE

JOURNAL (2019), <https://www.insurancejournal.com/magazines/mag-features/2019/07/15/532104.htm> (last visited Mar 7, 2020).

²¹⁶ Cal. Ins. Code § 533.5 (West)

²¹⁷ Cal. Ins. Code § 533.5 (West)

²¹⁸ Alan L. Friel, *et al.*, California Assembly Privacy Committee Votes in Favor of Advancing CCPA Amendments (2019), https://www.dataprivacymonitor.com/ccpa/california-assembly-privacy-committee-votes-in-favor-of-advancing-ccpa-amendments/?utm_source=BakerHostetler+-+Data+Privacy+Monitor&utm_campaign=a370fca0d3-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_11eb73cca1-a370fca0d3-73474273 (last visited Oct 2, 2019)

²¹⁹ 201 Mass. Code Regs. 17.01

²²⁰ 201 Mass. Code Regs. 17.01 *et seq.*

²²¹ 201 Mass. Code Regs. 17.03 *et seq.*

²²² 201 Mass. Code Regs. 17.04 *et seq.*

²²³ Commonwealth of Massachusetts, Plaintiff, v. Equifax, Inc., Defendant., 2017 WL 4176743 (Mass. Super.)

²²⁴ Commonwealth of Massachusetts, Plaintiff, v. Equifax, Inc., Defendant., 2017 WL 4176743 (Mass. Super.)

²²⁵ Commonwealth of Massachusetts, Plaintiff, v. Equifax, Inc., Defendant., 2017 WL 4176743 (Mass. Super.)

²²⁶ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.0

²²⁷ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.1

²²⁸ FAQs: 23 NYCRR Part 500 – Cybersecurity, https://www.dfs.ny.gov/industry_guidance/cyber_faqs (Last visited Jul 4, 2019)

²²⁹ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.1

²³⁰ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.2

²³¹ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.3

²³² N.Y. Comp. Codes R. & Regs. tit. 23, § 500.4

²³³ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.5

²³⁴ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.6

²³⁵ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.7

²³⁶ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.8

²³⁷ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.9

²³⁸ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.10

²³⁹ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.11

²⁴⁰ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.12

²⁴¹ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13

²⁴² N.Y. Comp. Codes R. & Regs. tit. 23, § 500.14

²⁴³ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.15

²⁴⁴ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.16

²⁴⁵ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17

²⁴⁶ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.18

²⁴⁷ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.19

-
- ²⁴⁸ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.20
- ²⁴⁹ NY Cybersecurity Regulations for Financial Services Companies: Enforcement Begins Aug. 28, McGuireWoods (2017) <https://www.mcguirewoods.com/Client-Resources/Alerts/2017/8/NY-Cybersecurity-Regulations-Financial-Services-Enforcement-August.aspx> (last visited Oct 2, 2019)
- ²⁵⁰ N.Y. Gen. Bus. Law § 899-aa(2) (McKinney) (out of date)
- ²⁵¹ N.Y. Gen. Bus. Law § 899-aa(d)(2) (McKinney)
- ²⁵² N.Y. Gen. Bus. Law § 899-aa(4) (McKinney)
- ²⁵³ N.Y. Gen. Bus. Law § 899-aa(1)(b) (McKinney) (out of date)
- ²⁵⁴ N.Y. Gen. Bus. Law § 899-aa(b)(5) (McKinney)
- ²⁵⁵ N.Y. Gen. Bus. Law § 899-bb(2) (McKinney)
- ²⁵⁶ N.Y. Gen. Bus. Law § 899-bb(2)(A) (McKinney)
- ²⁵⁷ N.Y. Gen. Bus. Law § 899-bb(2)(C) (McKinney)
- ²⁵⁸ N.Y. Gen. Bus. Law § 899-bb(2)(C) (McKinney)
- ²⁵⁹ N.Y. Gen. Bus. Law § 899-bb(1) (McKinney)
- ²⁶⁰ N.Y. Gen. Bus. Law § 899-bb(1)(c), (2)(c) (McKinney)
- ²⁶¹ NY LEGIS 117 (2019), 2019 Sess. Law News of N.Y. Ch. 117 (S. 5575-B) (McKINNEY'S)
- ²⁶² NY LEGIS 117 (2019), 2019 Sess. Law News of N.Y. Ch. 117 (S. 5575-B) (McKINNEY'S)
- ²⁶³ NY LEGIS 117 (2019), 2019 Sess. Law News of N.Y. Ch. 117 (S. 5575-B) (McKINNEY'S)
- ²⁶⁴ N.Y. Gen. Bus. Law § 899-bb(4)(e) (McKinney)
- ²⁶⁵ N.Y. Gen. Bus. Law § 899-bb(4)(d) (McKinney)
- ²⁶⁶ NY LEGIS 117 (2019), 2019 Sess. Law News of N.Y. Ch. 117 (S. 5575-B) (McKINNEY'S)
- ²⁶⁷ Bureau of Internet and Technology (BIT) Resource Center, NEW YORK STATE ATTORNEY GENERAL, <https://ag.ny.gov/press-releases/12t> (last visited Mar 7, 2020).
- ²⁶⁸ PricewaterhouseCoopers, NEW YORK SHIELD ACT PWC, <https://www.pwc.com/us/en/services/consulting/cybersecurity/new-york-shield-act.html> (last visited Mar 7, 2020).
- ²⁶⁹ Spiceworks, Inc, DATA SNAPSHOT: BIOMETRICS IN THE WORKPLACE COMMONPLACE, BUT ARE THEY SECURE? THE SPICEWORKS COMMUNITY (2018), <https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure> (last visited Feb 17, 2020).
- ²⁷⁰ 740 Ill. Comp. Stat. Ann. 14/1 to 14/99
- ²⁷¹ Tex. Bus. & Com. Code Ann. § 503.001 (West)
- ²⁷² Wash. Rev. Code Ann. § 19.375.010 to 19.375.900(West)
- ²⁷³ Michael Monajemi, Privacy Regulation in the Age of Biometrics That Deal with A New World Order of Information, 25 U. Miami Int'l & Comp. L. Rev. 371, 402 (2018)
- ²⁷⁴ 740 Ill. Comp. Stat. Ann. 14/5(c)
- ²⁷⁵ 740 Ill. Comp. Stat. Ann. 14/10
- ²⁷⁶ 740 Ill. Comp. Stat. Ann. 14/1 to 14/99

-
- ²⁷⁷ 740 Ill. Comp. Stat. Ann. 14/10
²⁷⁸ 740 Ill. Comp. Stat. Ann. 14/10
²⁷⁹ 740 Ill. Comp. Stat. Ann. 14/10
²⁸⁰ 740 Ill. Comp. Stat. Ann. 14/10
²⁸¹ 740 Ill. Comp. Stat. Ann. 14/10
²⁸² 740 Ill. Comp. Stat. Ann. 14/10
²⁸³ 815 Ill. Comp. Stat. Ann. 530/5
²⁸⁴ 815 Ill. Comp. Stat. Ann. 530/10
²⁸⁵ 815 Ill. Comp. Stat. Ann. 530/45
²⁸⁶ 815 Ill. Comp. Stat. Ann. 530/45
²⁸⁷ 740 Ill. Comp. Stat. Ann. 14/15
²⁸⁸ 740 Ill. Comp. Stat. Ann. 14/10
²⁸⁹ 740 Ill. Comp. Stat. Ann. 14/15
²⁹⁰ 740 Ill. Comp. Stat. Ann. 14/15
²⁹¹ 740 Ill. Comp. Stat. Ann. 14/10
²⁹² 740 Ill. Comp. Stat. Ann. 14/15
²⁹³ 740 Ill. Comp. Stat. Ann. 14/15
²⁹⁴ 740 Ill. Comp. Stat. Ann. 14/15
²⁹⁵ 740 Ill. Comp. Stat. Ann. 14/15
²⁹⁶ 740 Ill. Comp. Stat. Ann. 14/15(a)
²⁹⁷ 740 Ill. Comp. Stat. Ann. 14/20
²⁹⁸ Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, 129 N.E.3d 1197
²⁹⁹ 740 Ill. Comp. Stat. Ann. 14/20
³⁰⁰ Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 28, 129 N.E.3d 1197, 1205
³⁰¹ Michelle ESPINOSA, on behalf of herself and all other persons similarly situated, known and unknown, Plaintiff, v. REVMD PARTNERS, LLC, Defendant., 2019 WL 2103430 (Ill.Cir.Ct.)
³⁰² Michelle ESPINOSA, on behalf of herself and all other persons similarly situated, known and unknown, Plaintiff, v. REVMD PARTNERS, LLC, Defendant., 2019 WL 2103430 (Ill.Cir.Ct.)
³⁰³ 740 Ill. Comp. Stat. Ann. 14/1 to 14/99
³⁰⁴ In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1158–59 (N.D. Cal. 2016)
³⁰⁵ 740 Ill. Comp. Stat. Ann. 14/10
³⁰⁶ In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal. 2016)
³⁰⁷ In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016)
³⁰⁸ Liu v. Four Seasons Hotel, Ltd., 2019 IL App (1st) 182645, 138 N.E.3d 201
³⁰⁹ Liu v. Four Seasons Hotel, Ltd., 2019 IL App (1st) 182645, ¶ 1, 138 N.E.3d 201, 203
³¹⁰ Liu v. Four Seasons Hotel, Ltd., 2019 IL App (1st) 182645, ¶ 18, 138 N.E.3d 201, 205

-
- ³¹¹ Liu v. Four Seasons Hotel, Ltd., 2019 IL App (1st) 182645, ¶ 27, 138 N.E.3d 201, 207
- ³¹² ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, INSURANCE JOURNAL (2014), <https://www.insurancejournal.com/news/east/2014/07/18/332655.htm> (last visited Apr 7, 2019).
- ³¹³ 815 Ill. Comp. Stat. Ann. 530/10
- ³¹⁴ 15 U.S.C.A. § 45 (West)
- ³¹⁵ FTC Policy Statement on Unfairness, FEDERAL TRADE COMMISSION (1980), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> (last visited Mar 12, 2019).
- ³¹⁶ FTC Policy Statement on Unfairness, Federal Trade Commission (1980), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> (last visited Mar 12, 2019).
- ³¹⁷ FTC Policy Statement on Unfairness, Federal Trade Commission (1980), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> (last visited Mar 12, 2019).
- ³¹⁸ FTC Policy Statement on Deception, Federal Trade Commission (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (last visited MAR 25, 2019)
- ³¹⁹ Jeff Kosseff, Cybersecurity Law 5-6 (2017)
- ³²⁰ Internet Privacy and Data Security: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility, 4–5 (2019). Testimony Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate
- ³²¹ F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 608 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015)
- ³²² F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015)
- ³²³ F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 611 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015)
- ³²⁴ F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 611–12 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015)
- ³²⁵ F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015)
- ³²⁶ F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, (3d Cir. 2015)
- ³²⁷ 16 CFR § 313.3(K)(viii)
- ³²⁸ Internet Privacy and Data Security: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility, 6 (2019). Testimony Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate
- ³²⁹ 15 U.S.C.A. § 6809 (West)
- ³³⁰ 15 U.S.C.A. § 6801 (West)

³³¹ Financial Institutions and Customer Information: Complying with the Safeguards Rule, FEDERAL TRADE COMMISSION (2019), <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> (last visited Mar 7, 2019).

³³² *In the Matter of Taxslayer, LLC*, FTC File No. 162 3063 (Oct. 20, 2017) (complaint); *In the Matter of Taxslayer, LLC*, FTC Docket No. C-4626 (Oct. 20, 2017) (decision and order), available at <https://www.ftc.gov/enforcement/cases-proceedings/162-3063/taxslayer>.

³³³ *In the Matter of Taxslayer, LLC*, FTC File No. 162 3063 (Oct. 20, 2017) (complaint); *In the Matter of Taxslayer, LLC*, FTC Docket No. C-4626 (Oct. 20, 2017) (decision and order), available at <https://www.ftc.gov/enforcement/cases-proceedings/162-3063/taxslayer>.

³³⁴ Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules, FEDERAL TRADE COMMISSION (2017), <https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges> (last visited Apr 15, 2019).

³³⁵ 15 U.S.C.A. § 6823 (West)

³³⁶ FTC seeks comment on proposed amendments to safeguards and privacy rules, CONSUMER FINANCE MONITOR (2019), <https://www.consumerfinancemonitor.com/2019/03/08/ftc-seeks-comment-on-proposed-amendments-to-safeguards-and-privacy-rules/> (last visited Mar 15, 2019).

³³⁷ 17 C.F.R. § 248.30

³³⁸ 17 C.F.R. § 248.30

³³⁹ 17 C.F.R. § 248.30

³⁴⁰ Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies, U.S. Securities and Exchange Commission - Office of Compliance Inspections and Examinations (2019), <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf> (last visited Apr 20, 2019)

³⁴¹ Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies, U.S. Securities and Exchange Commission - Office of Compliance Inspections and Examinations (2019), <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf> (last visited Apr 20, 2019)

³⁴² Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies, U.S. Securities and Exchange Commission - Office of Compliance Inspections and Examinations (2019), <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf> (last visited Apr 20, 2019)

³⁴³ Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies, U.S. Securities and Exchange Commission - Office of Compliance Inspections and Examinations (2019), <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf> (last visited Apr 20, 2019)

³⁴⁴ Cyber Enforcement Actions, U.S. Securities and Exchange Commission (Continuously Updated), <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions> (last visited Oct 01, 2019)

³⁴⁵ Crystal N. Skelton, *Etc Data Security Enforcement: Analyzing the Past, Present, and Future*, 25 Competition: J. Anti., UCL & Privacy Sec. St. B. Cal. 305, 319 (2016)

³⁴⁶ SEC: Morgan Stanley Failed to Safeguard Customer Data, U.S. Securities and Exchange Commission (Jun 8, 2016), <https://www.sec.gov/news/pressrelease/2016-112.html> (last visited Apr 20, 2019)

³⁴⁷ SEC: Morgan Stanley Failed to Safeguard Customer Data, U.S. Securities and Exchange Commission (Jun 8, 2016), <https://www.sec.gov/news/pressrelease/2016-112.html> (last visited Apr 20, 2019)

³⁴⁸ 17 C.F.R. § 275.206(4)-2 (Custody of funds or securities of clients by investment advisers.)

³⁴⁹ SEC Charges Three Firms With Violating Custody Rule, U.S. Securities and Exchange Commission (Oct 28, 2013), <https://www.sec.gov/news/press-release/2013-230> (last visited Apr 20, 2019)

³⁵⁰ *In the Matter of Gw & Wade, LLC, Respondent.*, Release No. 3706 (Oct. 28, 2013)

³⁵¹ *In the Matter of Gw & Wade, LLC, Respondent.*, Release No. 3706 (Oct. 28, 2013)

³⁵² SEC Charges Three Firms With Violating Custody Rule, U.S. Securities and Exchange Commission (Oct 28, 2013), <https://www.sec.gov/news/press-release/2013-230> (last visited Apr 20, 2019)

³⁵³ 181 Records Retention Report NL 2, the Red Flag Program Clarification Act of 2010.

³⁵⁴ 17 CFR §248.201(b)(10)

³⁵⁵ SEC Case Brings Rarely Used Cyber Rules into Limelight | Publications, KIRKLAND & ELLIS, LLP (2018), <https://www.kirkland.com/publications/article/2018/09/sec-case-brings-rarely-used-cyber-rules-into-lime> (last visited Apr 16, 2018).

³⁵⁶ SEC Charges Firm With Deficient Cybersecurity Procedures, U.S. SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/news/press-release/2018-213> (last visited Apr 7, 2019).

³⁵⁷ SEC Charges Firm With Deficient Cybersecurity Procedures, U.S. SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/news/press-release/2018-213> (last visited Apr 7, 2019).

³⁵⁸ SEC Charges Firm With Deficient Cybersecurity Procedures, U.S. SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/news/press-release/2018-213> (last visited Apr 7, 2019).

³⁵⁹ SEC Charges Firm With Deficient Cybersecurity Procedures, U.S. SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/news/press-release/2018-213> (last visited Apr 7, 2019).

-
- ³⁶⁰ SEC Charges Firm With Deficient Cybersecurity Procedures, U.S. SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/news/press-release/2018-213> (last visited Apr 7, 2019).
- ³⁶¹ In the Matter of Voya Fin. Advisors, Inc., Respondent., Release No. 5048 (Sept. 26, 2018)
- ³⁶² SEC Charges Firm With Deficient Cybersecurity Procedures, U.S. SECURITIES AND EXCHANGE COMMISSION (2018), <https://www.sec.gov/news/press-release/2018-213> (last visited Apr 7, 2019).
- ³⁶³ Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe) (2015), European Commission, http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm, (last visited Sep 13, 2019).
- ³⁶⁴ EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield (2016), European Commission, http://europa.eu/rapid/press-release_IP-16-216_en.htm, (last visited Sep 17, 2019).
- ³⁶⁵ Privacy Shield, Federal Trade Commission, <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield>, (last visited Sep 20, 2019).
- ³⁶⁶ Requirements of Participation - Privacy Shield Framework, The International Trade Administration (ITA), U.S. Department of Commerce, <https://www.privacyshield.gov/article?id=Requirements-of-Participation>, (last visited Sep 22, 2019).
- ³⁶⁷ Requirements of Participation - Privacy Shield Framework, The International Trade Administration (ITA), U.S. Department of Commerce, <https://www.privacyshield.gov/article?id=Requirements-of-Participation>, (last visited Sep 22, 2019).
- ³⁶⁸ Daniel R. Stoller, FTC Eyes Enforcement Boost for EU-U.S. Privacy Shield Data Moves (1) (Apr 26, 2019), <https://news.bloomberglaw.com/privacy-and-data-security/ftc-eyes-enforcement-boost-for-eu-u-s-privacy-shield-data-moves>, (last visited Sep 22, 2019).
- ³⁶⁹ Daniel R. Stoller, FTC Eyes Enforcement Boost for EU-U.S. Privacy Shield Data Moves (1) (Apr 26, 2019), <https://news.bloomberglaw.com/privacy-and-data-security/ftc-eyes-enforcement-boost-for-eu-u-s-privacy-shield-data-moves>, (last visited Sep 22, 2019).
- ³⁷⁰ SecurTest – Corporate Background, SecurTest, <https://securtest.com/2012/index.php> (last visited oct 06, 2019)
- ³⁷¹ In the Matter of SecurTest, Inc., a corporation., 2019 WL 2522167, at *2
- ³⁷² In the Matter of SecurTest, Inc., a corporation., 2019 WL 2522167, at *1
- ³⁷³ In the Matter of SecurTest, Inc., a corporation., 2019 WL 2522167, at *1
- ³⁷⁴ In the Matter of SecurTest, Inc., a corporation., 2019 WL 2522167, at *1
- ³⁷⁵ In the Matter of Securtest, Inc., A Corp.., No. 182-3152, 2019 WL 4052437 (MSNET Aug. 12, 2019)
- ³⁷⁶ Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards, PCI SECURITY

STANDARDS COUNCIL,

https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
(last visited Mar 23, 2019).

³⁷⁷ Official PCI Security Standards Council Site - Verify PCI Compliance,
Download Data Security and Credit Card Security Standards, PCI SECURITY
STANDARDS COUNCIL,

https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
(last visited Mar 23, 2019).

³⁷⁸ PCI DSS Compliance, Practical Law Practice Note 8-608-7192

³⁷⁹ P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM,
2016 WL 3055111, at *2 (D. Ariz. May 31, 2016)

³⁸⁰ PCI DSS Compliance, Practical Law Practice Note 8-608-7192

³⁸¹ LifeLock Will Pay \$12 Million to Settle Charges by the FTC and 35 States That
Identity Theft Prevention and Data Security Claims Were False, FEDERAL TRADE
COMMISSION (2019), [https://www.ftc.gov/news-events/press-
releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states](https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states) (last
visited Apr 7, 2019).

³⁸² LifeLock Will Pay \$12 Million to Settle Charges by the FTC and 35 States That
Identity Theft Prevention and Data Security Claims Were False, FEDERAL TRADE
COMMISSION (2019), [https://www.ftc.gov/news-events/press-
releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states](https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states) (last
visited Apr 7, 2019).

³⁸³ LifeLock Will Pay \$12 Million to Settle Charges by the FTC and 35 States That
Identity Theft Prevention and Data Security Claims Were False, FEDERAL TRADE
COMMISSION (2019), [https://www.ftc.gov/news-events/press-
releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states](https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states) (last
visited Apr 7, 2019).

³⁸⁴ LifeLock Will Pay \$12 Million to Settle Charges by the FTC and 35 States That
Identity Theft Prevention and Data Security Claims Were False, FEDERAL TRADE
COMMISSION (2019), [https://www.ftc.gov/news-events/press-
releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states](https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states) (last
visited Apr 7, 2019).

³⁸⁵ Statement of the Federal Trade Commission FTC v. LifeLock , (2015),
https://www.ftc.gov/system/files/documents/public_statements/896143/151217lifelockcommstmt.pdf (last visited Apr 7, 2019).

³⁸⁶ Statement of the Federal Trade Commission FTC v. LifeLock , (2015),
https://www.ftc.gov/system/files/documents/public_statements/896143/151217lifelockcommstmt.pdf (last visited Apr 7, 2019).

³⁸⁷ Statement of the Federal Trade Commission FTC v. LifeLock , (2015),
https://www.ftc.gov/system/files/documents/public_statements/896143/151217lifelockcommstmt.pdf (last visited Apr 7, 2019).

³⁸⁸ LifeLock to Pay \$100 Million to Consumers to Settle FTC Charges it Violated
2010 Order, FEDERAL TRADE COMMISSION (2015), <https://www.ftc.gov/news->

events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated (last visited Apr 7, 2019).

³⁸⁹ PCI SECURITY STANDARDS COUNCIL TESTIFIES BEFORE U.S. HOUSE FINANCIAL SERVICES COMMITTEE, PCI SECURITY STANDARDS COUNCIL (2014),

https://www.pcisecuritystandards.org/pdfs/14_05_04_Congressional_Hearings_Press_Release.pdf (last visited Mar 25, 2019).

³⁹⁰ Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns, (2019), <https://www.irs.gov/pub/irs-pdf/p1345.pdf> (last visited Jan 8, 2019). Publication 1345 (Rev 2-2019) Catalog Number 64382J

³⁹¹ 26 U.S. Code § 7216.

³⁹² 26 U.S. Code § 6713.

³⁹³ Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns, (2019), <https://www.irs.gov/pub/irs-pdf/p1345.pdf> (last visited Jan 8, 2019). Publication 1345 (Rev 2-2019) Catalog Number 64382J

³⁹⁴ Tips for tax preparers on how to create a data security plan, INTERNAL REVENUE SERVICE (2018), <https://www.irs.gov/newsroom/tips-for-tax-preparers-on-how-to-create-a-data-security-plan> (last visited Apr 7, 2019).

³⁹⁵ Internal Revenue Bulletin: 2007-26, INTERNAL REVENUE SERVICE (2007), https://www.irs.gov/irb/2007-26_IRB (last visited Apr 7, 2019). See Rev. Proc. 2007-40 synopsis.

³⁹⁶ JOSEPH E. BRUNSMAN & DANIEL W. HUDSON, TRUE COURSE: THE DEFINITIVE GUIDE FOR CPA PRACTICE INSURANCE (1 ed.). See Chapter 4: Professional Liability Insurance Policy Specifics.

³⁹⁷ Nicole Hong & Robin Sidel, Hackers Breach Law Firms, Including Cravath and Weil Gotshal, WALL ST. J. (Mar. 29, 2016), <https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504>.

³⁹⁸ More Puckett & Faraj Lulz (Feb 4, 2012), <https://pastebin.com/nD2TW0fL>, (last visited Mar 29, 2019).

³⁹⁹ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁰ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477 Securing Communication of Protected Client Information (2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf, (last visited Aug 20, 2019)

ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰² ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰³ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁴ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁵ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁶ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁷ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁸ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018),

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, (last visited Aug 20, 2019)

⁴⁰⁹ ABA RULE 10. SANCTIONS, Mod. Rules Law. Displ. Enforce. Rule 10

⁴¹⁰ Small Firm Business Continuity Plan Template, SMALL FIRM BUSINESS CONTINUITY PLAN TEMPLATE (2010), <http://www.finra.org/industry/small-firm-business-continuity-plan-template> (last visited Apr 7, 2019).

⁴¹¹ February 2017 Disciplinary Actions, Financial Industry Regulatory Authority (2017),

https://www.finra.org/sites/default/files/publication_file/February_2017_Disciplinary_Actions.pdf (last visited Mar 20, 2019).

⁴¹² Investor Alert: Cybersecurity and Your Brokerage Firm, Financial Industry Regulatory Authority (2015), <http://www.finra.org/investors/alerts/cybersecurity-and-your-brokerage-firm>, (last visited Apr 13, 2019).

⁴¹³ Safeguarding Covered Defense Information, U.S. Department of Defense, <https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf>, (last visited Apr 15, 2019).

⁴¹⁴ DoD to debut new cyber assessment program for contractors in less than a year, FEDERAL NEWS NETWORK (2019), <https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2019/07/dod-to-debut-new-cyber-assessment-program-for-contractors-in-less-than-a-year/> (last visited Mar 7, 2020).

-
- ⁴¹⁵ Keeping track of the meaning of terms surrounding cybersecurity compliance can be difficult. We get it., CMMC, <https://www.cmmcab.org/glossary> (last visited Mar 7, 2020).
- ⁴¹⁶ DoD to debut new cyber assessment program for contractors in less than a year, FEDERAL NEWS NETWORK (2019), <https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2019/07/dod-to-debut-new-cyber-assessment-program-for-contractors-in-less-than-a-year/> (last visited Mar 7, 2020).
- ⁴¹⁷ CMMC: What Suppliers Need to Know, LOCKHEED MARTIN, <https://www.lockheedmartin.com/en-us/suppliers/news/features/2019/cybersecurity-cmmc.html> (last visited Mar 7, 2020).
- ⁴¹⁸ CMMC 2/28
- ⁴¹⁹ 48 C.F.R. § 52.204-21
- ⁴²⁰ Page 5/28
- ⁴²¹ 48 C.F.R. § 252.204-7012
- ⁴²² CUI Categories, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, <https://www.archives.gov/cui/registry/category-list> (last visited Mar 7, 2020).
- ⁴²³ CMMC page 5/28
- ⁴²⁴ CMMC page 5-6/28
- ⁴²⁵ CMMC page 4/28
- ⁴²⁶ CMMC page 6/28
- ⁴²⁷ CMMC page 6/28
- ⁴²⁸ CMMC page 7/28
- ⁴²⁹ CMMC page 11/28
- ⁴³⁰ Page 10/28
- ⁴³¹ Page 10/28
- ⁴³² 48 C.F.R. § 52.204-21
- ⁴³³ 48 C.F.R. § 252.204-7012
- ⁴³⁴ Safeguarding Covered Defense Information, U.S. Department of Defense, <https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf>, (last visited Apr 15, 2019).
- ⁴³⁵ Safeguarding Covered Defense Information, U.S. Department of Defense, <https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf>, (last visited Apr 15, 2019).
- ⁴³⁶ Special Publication (SP) 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, National Institute of Standards and Technology (NIST), <http://dx.doi.org/10.6028/NIST.SP.800–171>, (last visited Oct 06, 2019).
- ⁴³⁷ Special Publication (SP) 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, National Institute of Standards and Technology (NIST), <http://dx.doi.org/10.6028/NIST.SP.800–171>, (last visited Oct 06, 2019).
- ⁴³⁸ 48 C.F.R. § 252.204-7012
- ⁴³⁹ 48 C.F.R. § 252.204-7012

⁴⁴⁰ 48 C.F.R. § 252.204-7012

⁴⁴¹ 48 C.F.R. § 252.204-7012

⁴⁴² CMMC MODEL v1.0 CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC), <https://www.acq.osd.mil/cmmc/draft.html> (last visited Mar 7, 2020).

⁴⁴³ 48 C.F.R. § 252.204-7012

⁴⁴⁴ 48 C.F.R. § 252.204-7012

⁴⁴⁵ CMMC MODEL v1.0 Appendices CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC), <https://www.acq.osd.mil/cmmc/draft.html> (last visited Mar 7, 2020).

⁴⁴⁶ 48 C.F.R. § 252.204-7012

⁴⁴⁷ 48 C.F.R. § 252.204-7009

⁴⁴⁸ In re Netcracker Technology Corporation Non-Prosecution and Security Agreement, U.S. Department of Justice – National Security Division (2017), <https://www.justice.gov/opa/press-release/file/1017056/download>, (last visited Apr 16, 2019)

⁴⁴⁹ In re Netcracker Technology Corporation Non-Prosecution and Security Agreement, U.S. Department of Justice – National Security Division (2017), <https://www.justice.gov/opa/press-release/file/1017056/download>, (last visited Apr 16, 2019)

⁴⁵⁰ In re Netcracker Technology Corporation Non-Prosecution and Security Agreement, U.S. Department of Justice – National Security Division (2017), <https://www.justice.gov/opa/press-release/file/1017056/download>, (last visited Apr 16, 2019)

⁴⁵¹ John S. West, Laura Anne Kuykendall, New Requirements For Protecting Sensitive Government Data Adopted For Government Contractors: Is Your Company In Compliance? (2018), Troutman Sanders, LLP, <https://www.troutman.com/insights/new-requirements-for-protecting-sensitive-government-data-adopted-for-government-contractors-is-your-company-in-compliance.html>, (last visited Apr 16, 2019).

⁴⁵² In re Netcracker Technology Corporation Non-Prosecution and Security Agreement, U.S. Department of Justice – National Security Division (2017), <https://www.justice.gov/opa/press-release/file/1017056/download>, (last visited Apr 16, 2019).

⁴⁵³ In re Netcracker Technology Corporation Non-Prosecution and Security Agreement, U.S. Department of Justice – National Security Division (2017), <https://www.justice.gov/opa/press-release/file/1017056/download>, (last visited Apr 16, 2019).

⁴⁵⁴ Draft NIST Special Publication 800-171B: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Enhanced Security Requirements for Critical Programs and High Value Assets, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2019), <https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf> (last visited Mar 7, 2020).

-
- ⁴⁵⁵ Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets, NATIONAL INSTITUTES OF STANDARDS AND TECHNOLOGY (2019), <https://csrc.nist.gov/publications/detail/sp/800-171b/draft> (last visited Mar 7, 2020).
- ⁴⁵⁶ Request for Comments on Draft NIST Special Publication (SP) 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets. , NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, <https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf> (last visited Mar 7, 2020).
- ⁴⁵⁷ Request for Comments on Draft NIST Special Publication (SP) 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets. , NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, <https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf> (last visited Mar 7, 2020).
- ⁴⁵⁸ CMMC MODEL v1.0 Appendices CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC), <https://www.acq.osd.mil/cmmc/draft.html> (last visited Mar 7, 2020).
- ⁴⁵⁹ FAQ, CMMC, <https://www.cmmcab.org/faq> (last visited Mar 7, 2020).
- ⁴⁶⁰ Why DoD's decision to make cybersecurity an 'allowable cost' matters, FEDERAL NEWS NETWORK (2019), <https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/> (last visited Mar 7, 2020).
- ⁴⁶¹ Why DoD's decision to make cybersecurity an 'allowable cost' matters, FEDERAL NEWS NETWORK (2019), <https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/> (last visited Mar 7, 2020).
- ⁴⁶² *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1250 (E.D. Cal. 2019)
- ⁴⁶³ *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1250 (E.D. Cal. 2019)
- ⁴⁶⁴ *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1250 (E.D. Cal. 2019)
- ⁴⁶⁵ *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1250 (E.D. Cal. 2019)
- ⁴⁶⁶ *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1250 (E.D. Cal. 2019)
- ⁴⁶⁷ Covered Entities and Business Associates, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>, (last visited Apr 16, 2019).
- ⁴⁶⁸ HIPAA Administrative Simplification: Regulation Text; 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013)

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf> (last visited Apr 16, 2019).

⁴⁶⁹ *CVS Pharmacy, Inc. v. Press Am., Inc.*, 2018 WL 318479, at *7 (S.D.N.Y. Jan. 3, 2018)

⁴⁷⁰ HIPAA Administrative Simplification: Regulation Text; 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013)

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf> (last visited Apr 16, 2019).

⁴⁷¹ 45 C.F.R. § 160.103

⁴⁷² Mark O. Dietrich, CPA/ABV, How health care data security rules may affect you: CPAs need to understand their responsibilities under HIPAA to avoid potentially severe civil and criminal penalties (2015),

<https://www.journalofaccountancy.com/issues/2015/jan/health-care-data-security-rules.html>, (last visited Apr 20, 2019).

⁴⁷³ 45 C.F.R. § 160.103

⁴⁷⁴ 45 C.F.R. § 164.514(b)

⁴⁷⁵ Summary of HIPAA Privacy Rules, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>, (last visited Apr 16, 2019).

⁴⁷⁶ Mark O. Dietrich, CPA/ABV, How health care data security rules may affect you: CPAs need to understand their responsibilities under HIPAA to avoid potentially severe civil and criminal penalties (2015),

<https://www.journalofaccountancy.com/issues/2015/jan/health-care-data-security-rules.html>, (last visited Apr 20, 2019).

⁴⁷⁷ Business Associates: 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e), U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>, (last visited Apr 16, 2019).

⁴⁷⁸ 45 C.F.R. § 160.103

⁴⁷⁹ 45 C.F.R. § 164.520

⁴⁸⁰ 45 C.F.R. § 164.530(i)

⁴⁸¹ 45 C.F.R. § 164.530(b)

⁴⁸² 45 C.F.R. § 164.530 and 45 C.F.R. § 164.308

⁴⁸³ 45 C.F.R. § 164.530

⁴⁸⁴ HIPAA Privacy Rule, Practical Law Practice Note 4-501-7220

⁴⁸⁵ Summary of HIPAA Privacy Rules, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>, (last visited Apr 16, 2019).

⁴⁸⁶ HIPAA Security Rule, Practical Law Practice Note 5-502-1269

⁴⁸⁷ 45 C.F.R. § 164.308

⁴⁸⁸ 45 C.F.R. § 164.316

⁴⁸⁹ 45 C.F.R. § 164.310(a)(1)

⁴⁹⁰ 45 C.F.R. § 164.310(b)-(c)

-
- ⁴⁹¹ Summary of HIPAA Privacy Rules, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>, (last visited Apr 16, 2019).
- ⁴⁹² 45 C.F.R. § 164.310(d)(1)
- ⁴⁹³ August 2018 Cyber Security Newsletter: Considerations for Securing Electronic Media and Devices, U.S. Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-august-2018-device-and-media-controls.pdf>, (last visited Apr 16, 2019).
- ⁴⁹⁴ 45 C.F.R. § 164.312(a)(2)(iv)
- ⁴⁹⁵ 45 C.F.R. § 164.312(b)
- ⁴⁹⁶ 45 C.F.R. § 164.312(c)(1)
- ⁴⁹⁷ 45 C.F.R. § 164.312(c)(2)
- ⁴⁹⁸ 45 C.F.R. § 164.312(d)
- ⁴⁹⁹ 45 C.F.R. § 164.312(e)(1)
- ⁵⁰⁰ 45 C.F.R. § 164.312(e)(2)
- ⁵⁰¹ 45 C.F.R. § 164.316
- ⁵⁰² 45 C.F.R. § 164.402
- ⁵⁰³ Enforcement Data, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html>, (last visited Apr 16, 2019).
- ⁵⁰⁴ 2018 Cost of a Data Breach Study: Global Overview, IBM SECURITY, available at: <https://www.ibm.com> (last visited Mar 2019).
- ⁵⁰⁵ 45 CFR §§ 164.400-414
- ⁵⁰⁶ 45 C.F.R. § 164.314(a)
- ⁵⁰⁷ Guidance on HIPAA & Cloud Computing, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>, (last visited Apr 16, 2019).
- ⁵⁰⁸ Guidance on HIPAA & Cloud Computing, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>, (last visited Apr 16, 2019).
- ⁵⁰⁹ Guidance on HIPAA & Cloud Computing, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>, (last visited Apr 16, 2019).
- ⁵¹⁰ In re Center for Children’s Digestive Health, S.C. (2017), The United States Department of Health and Human Services – Office for Civil Rights, https://www.hhs.gov/sites/default/files/ra_cap_ccdh.pdf, (last visited Apr 20, 2019).
- ⁵¹¹ In re Center for Children’s Digestive Health, S.C. (2017), The United States Department of Health and Human Services – Office for Civil Rights, https://www.hhs.gov/sites/default/files/ra_cap_ccdh.pdf, (last visited Apr 20, 2019).
- ⁵¹² In re Center for Children’s Digestive Health, S.C. (2017), The United States Department of Health and Human Services – Office for Civil Rights, https://www.hhs.gov/sites/default/files/ra_cap_ccdh.pdf, (last visited Apr 20, 2019).

⁵¹³ In re Catholic Health Care Services of the Archdiocese of Philadelphia (2016) , The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/chcs-racap-final.pdf>, (last visited Feb 18, 2020).

⁵¹⁴ In re Catholic Health Care Services of the Archdiocese of Philadelphia (2016) , The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/chcs-racap-final.pdf>, (last visited Feb 18, 2020).

⁵¹⁵ In re Catholic Health Care Services of the Archdiocese of Philadelphia (2016) , The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/chcs-racap-final.pdf>, (last visited Feb 18, 2020).

⁵¹⁶ Guidance on HIPAA & Cloud Computing, U.S. Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>, (last visited Apr 16, 2019).

⁵¹⁷ In re Oregon Health & Science University (2014), The United States Department of Health and Human Services – Office for Civil Rights, https://www.hhs.gov/sites/default/files/ohsuracap_508.pdf, (last visited Apr 20, 2019).

⁵¹⁸ In re Oregon Health & Science University (2014), The United States Department of Health and Human Services – Office for Civil Rights, https://www.hhs.gov/sites/default/files/ohsuracap_508.pdf, (last visited Apr 20, 2019).

⁵¹⁹ In re Oregon Health & Science University (2014), The United States Department of Health and Human Services – Office for Civil Rights, https://www.hhs.gov/sites/default/files/ohsuracap_508.pdf, (last visited Apr 20, 2019).

⁵²⁰ In re Sandor Mark Jacobson (“Receiver”), acting on behalf of Filefax, Inc. as court appointed Receiver (2015), The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/filefax-receiver-racap.pdf>, (last visited Apr 23, 2019).

⁵²¹ Resolution Agreement regarding Sandor Mark Jacobson (“Receiver”), acting on behalf of Filefax, Inc. as court appointed Receiver (2015), The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/filefax-receiver-racap.pdf>, (last visited Apr 23, 2019).

⁵²² In re Anthem, Inc., (2018), The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/anthem-ra-cap.pdf>, (last visited Apr 23, 2019).

⁵²³ In re Anthem, Inc., (2018), The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/anthem-ra-cap.pdf>, (last visited Apr 23, 2019).

-
- ⁵²⁴ In re Anthem, Inc., (2018), The United States Department of Health and Human Services – Office for Civil Rights, <https://www.hhs.gov/sites/default/files/anthem-ra-cap.pdf>, (last visited Apr 23, 2019).
- ⁵²⁵ Anthem Pays OCR \$16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History (2018), The United States Department of Health and Human Services, <https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html>, (last visited Apr 23, 2019).
- ⁵²⁶ State of Indiana v. Joseph Beck, Beck Family Dentistry, 49D10-1412-PL-041613
- ⁵²⁷ Summary of 2018 HIPAA Fines and Settlements (2019), HIPAA Journal, <https://www.hipaajournal.com/summary-2018-hipaa-fines-and-settlements/>, (last visited May 08, 2019).
- ⁵²⁸ Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 472 (D.D.C. 2018)
- ⁵²⁹ Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 473 (D.D.C. 2018)
- ⁵³⁰ Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 473 (D.D.C. 2018)
- ⁵³¹ Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 473 (D.D.C. 2018)
- ⁵³² Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 474 (D.D.C. 2018)
- ⁵³³ 42 U.S.C.A. § 1320d-5 through 42 U.S.C.A. § 1320d-6 (West)
- ⁵³⁴ HIPAA Privacy, Security, and Breach Notification Audit Program, The United States Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#differ>, (last visited May 25, 2019).
- ⁵³⁵ HIPAA Privacy, Security, and Breach Notification Audit Program, The United States Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#differ>, (last visited May 25, 2019).
- ⁵³⁶ HIPAA Privacy, Security, and Breach Notification Audit Program, The United States Department of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#differ>, (last visited May 25, 2019).
- ⁵³⁷ Lynn M. Daggett, Bucking Up Buckley i: Making the Federal Student Records Statute Work, 46 Cath. U. L. Rev. 617, 620–21 (1997)
- ⁵³⁸ 34 C.F.R. § 99.1
- ⁵³⁹ Lynn M. Daggett, Bucking Up Buckley II: Using Civil Rights Claims to Enforce the Federal Student Records Statute, 21 Seattle U. L. Rev. 29 (1997)
- ⁵⁴⁰ 20 U.S.C. § 1232g(b)(1)
- ⁵⁴¹ 20 U.S.C. § 1232g(a)(2)
- ⁵⁴² 20 U.S.C. § 1232g(d)
- ⁵⁴³ 34 C.F.R. § 99.3
- ⁵⁴⁴ U.S. Government Accountability Office, FEDERAL STUDENT AID: BETTER PROGRAM MANAGEMENT AND OVERSIGHT OF POSTSECONDARY SCHOOLS NEEDED TO PROTECT STUDENT INFORMATION [REISSUED ON DECEMBER 15, 2017] U.S.

-
- GOVERNMENT ACCOUNTABILITY OFFICE (U.S. GAO) (2017),
<https://www.gao.gov/products/GAO-18-121> (last visited Mar 7, 2020).
- ⁵⁴⁵ Benjamin Herold, SCHOOLS SUFFERED AT LEAST 122 CYBERSECURITY INCIDENTS LAST YEAR EDUCATION WEEK - DIGITAL EDUCATION (2019),
http://blogs.edweek.org/edweek/DigitalEducation/2019/02/schools_cybersecurity_incidents_2018.html (last visited Mar 7, 2020).
- ⁵⁴⁶ 34 C.F.R. § 99.31
- ⁵⁴⁷ 34 C.F.R. § 99.33
- ⁵⁴⁸ Daniel Solove, FERPA AND THE CLOUD: WHY FERPA DESPERATELY NEEDS REFORM NYU | LAW,
http://www.law.nyu.edu/sites/default/files/ECM_PRO_074960.pdf (last visited Mar 7, 2020).
- ⁵⁴⁹ 20 U.S.C.A. § 1232h(b) (West)
- ⁵⁵⁰ 20 U.S.C.A. § 1232h(c) (West)
- ⁵⁵¹ 20 U.S.C.A. § 1232h(c) (West)
- ⁵⁵² 20 U.S.C.A. § 1232g (West)
- ⁵⁵³ 34 C.F.R. § 99.67
- ⁵⁵⁴ Gonzaga Univ. v. Doe, 536 U.S. 273, 277, 122 S. Ct. 2268, 2272, 153 L. Ed. 2d 309 (2002)
- ⁵⁵⁵ Gonzaga Univ. v. Doe, 536 U.S. 273, 287, 122 S. Ct. 2268, 2277, 153 L. Ed. 2d 309 (2002)
- ⁵⁵⁶ Gonzaga Univ. v. Doe, 536 U.S. 273, 290, 122 S. Ct. 2268, 2279, 153 L. Ed. 2d 309 (2002)
- ⁵⁵⁷ United States v. Miami Univ., 294 F.3d 797 (6th Cir. 2002)
- ⁵⁵⁸ Cal. Bus. & Prof. Code § 22584 (West)
- ⁵⁵⁹ Cal. Bus. & Prof. Code § 22586 (West)
- ⁵⁶⁰ Katie Beaudin, College and University Data Breaches: Regulating Higher Education Cybersecurity Under State and Federal Law, 41 J.C. & U.L. 657, 675 (2015)
- ⁵⁶¹ Article concerning Maricopa College Students Data Breach (2015), AZ Central, archived at:
<http://archive.azcentral.com/community/phoenix/articles/20131127arizona-college-students-data-breach.html>.
- ⁵⁶² Roberts v. Maricopa County Cmty. Coll. Dist., No. CV2014-007411 (Ariz. Super. Ct. Apr. 28, 2014)
- ⁵⁶³ Angela Gonzales, MARICOPA COMMUNITY COLLEGES SETTLES DATA BREACH CLASS-ACTION LAWSUITS BIZJOURNALS.COM (2015),
<https://www.bizjournals.com/phoenix/blog/business/2015/12/maricopa-community-colleges-settles-data-breach.html> (last visited Mar 7, 2020).
- ⁵⁶⁴ Mary Beth Faller, MARICOPA COMMUNITY COLLEGE DATA BREACH COSTS APPROACH \$20 MILLION AZCENTRAL (2014),
<https://www.azcentral.com/story/news/local/phoenix/2014/05/19/data-breach-costs-approach-million/9312729/> (last visited Mar 7, 2020).

-
- ⁵⁶⁵ Mary Beth Faller, MARICOPA COMMUNITY COLLEGE DISTRICT RAISES PROPERTY TAXES FOR THE SECOND YEAR IN A ROW AZCENTRAL (2014), <https://www.azcentral.com/story/news/local/phoenix/2014/05/28/maricopa-college-district-raises-property-taxes/9677067/> (last visited Mar 7, 2020).
- ⁵⁶⁶ In re Maricopa County Community College: Complaint, Request for Investigation, Injunction, and Other Relief Under the Safeguards Rule (2014), Submitted by “Dissent” of databreaches.net, available at: https://www.databreaches.net/wp-content/uploads/MCCCD_SafeguardsRule.pdf
- ⁵⁶⁷ See 16 C.F.R. § 313.3
- ⁵⁶⁸ Timothy Tobin, THE GRAMM-LEACH-BLILEY ACT FOR INDEPENDENT SCHOOLS NATIONAL ASSOCIATION OF INDEPENDENT SCHOOLS (2014), http://www.nais.org/Articles/Documents/Gramm_Leach_BlileyAct2014final.pdf (last visited Mar 7, 2020).
- ⁵⁶⁹ 16 C.F.R. § 313.1
- ⁵⁷⁰ Timothy Tobin, THE GRAMM-LEACH-BLILEY ACT FOR INDEPENDENT SCHOOLS NATIONAL ASSOCIATION OF INDEPENDENT SCHOOLS (2014), http://www.nais.org/Articles/Documents/Gramm_Leach_BlileyAct2014final.pdf (last visited Mar 7, 2020).
- ⁵⁷¹ 12 C.F.R. § 1016.7
- ⁵⁷² 16 C.F.R. § 313.3
- ⁵⁷³ 15 U.S.C.A. § 6801 (West)
- ⁵⁷⁴ Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy, FEDERAL TRADE COMMISSION (2007), <https://www.ftc.gov/news-events/press-releases/2007/10/agencies-issue-final-rules-identity-theft-red-flags-and-notices> (last visited Mar 7, 2020).
- ⁵⁷⁵ Federal Student Aid - IFAP: (GEN-16-12) Subject: Protecting Student Information, IFAP (2016), <https://ifap.ed.gov/dear-colleague-letters/07-01-2016-gen-16-12-subject-protecting-student-information> (last visited Mar 7, 2020).
- ⁵⁷⁶ 2 C.F.R. § Pt. 200, App. XI Compliance Supplement
- ⁵⁷⁷ 16 C.F.R. § 314.4(b), and 2 C.F.R. § Pt. 200, App. XI Compliance Supplement
- ⁵⁷⁸ 2 C.F.R. § Pt. 200, App. XI Compliance Supplement
- ⁵⁷⁹ Federal Student Aid - IFAP: (GEN-16-12) Subject: Protecting Student Information, IFAP (2016), <https://ifap.ed.gov/dear-colleague-letters/07-01-2016-gen-16-12-subject-protecting-student-information> (last visited Mar 7, 2020).
- ⁵⁸⁰ Neil, DATA BREACHES PUT A DENT IN COLLEGES' FINANCES AS WELL AS REPUTATIONS THE CHRONICLE OF HIGHER EDUCATION (2014), <https://www.chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/> (last visited Mar 7, 2020).
- ⁵⁸¹ Neil, DATA BREACHES PUT A DENT IN COLLEGES' FINANCES AS WELL AS REPUTATIONS THE CHRONICLE OF HIGHER EDUCATION (2014), <https://www.chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/> (last visited Mar 7, 2020).
- ⁵⁸² Ponemon cost of data breach study 2018.

⁵⁸³ Haley Blum, MAINTAINING STUDENT RECORDS COUNCIL ON ACADEMIC ACCREDITATION (2017), <https://caa.asha.org/news/maintaining-student-records/> (last visited Mar 7, 2020).

⁵⁸⁴ Richard Pérez-peña, UNIVERSITIES FACE A RISING BARRAGE OF CYBERATTACKS THE NEW YORK TIMES (2013), <https://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html> (last visited Mar 7, 2020).

⁵⁸⁵ 47 U.S.C. § 227

⁵⁸⁶ Telephone Consumer Protection Act (TCPA): Overview, Practical Law Practice Note Overview w-000-5609

⁵⁸⁷ Hiscox CyberClear Policy TPCCYB P0001 CW (05/16) pg. 10.

⁵⁸⁸ Victoria FLORES, an individual, Plaintiff, v. ACE AMERICAN INSURANCE COMPANY, a Pennsylvania corporation, Defendant., 2018 WL 3525500 (S.D.N.Y.)

⁵⁸⁹ Victoria FLORES, an individual, Plaintiff, v. ACE AMERICAN INSURANCE COMPANY, a Pennsylvania corporation, Defendant., 2018 WL 3525500 (S.D.N.Y.)

⁵⁹⁰ Victoria FLORES, an individual, Plaintiff, v. ACE AMERICAN INSURANCE COMPANY, a Pennsylvania corporation, Defendant., 2018 WL 3525500 (S.D.N.Y.)

⁵⁹¹ Victoria FLORES, an individual, Plaintiff, v. ACE AMERICAN INSURANCE COMPANY, a Pennsylvania corporation, Defendant., 2018 WL 3525500 (S.D.N.Y.)

⁵⁹² 3 A.L.R.6th 625 (Originally published in 2005)

⁵⁹³ Telephone Consumer Protection Act (TCPA): Overview, Practical Law Practice Note Overview w-000-5609

⁵⁹⁴ § 13:1.Introduction, Corp Couns. Gd. to Advertising L and Agrmts. § 13:1

⁵⁹⁵ § 13:3.CAN-SPAM Act—Preemption of state laws, Corp Couns. Gd. to Advertising L and Agrmts. § 13:3

⁵⁹⁶ See 15 U.S.C. § 7704

⁵⁹⁷ See 15 U.S.C. § 7706(f)

⁵⁹⁸ See 15 U.S.C. § 7706(g)

⁵⁹⁹ CAN-SPAM Act: A Compliance Guide for Business, Federal Trade Commission, <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>, (last visited May 29, 2019).

⁶⁰⁰ 15 U.S.C. § 7706(f)

⁶⁰¹ Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, International Risk Management Institute, Inc., <https://www.irmi.com/term/insurance-definitions/controlling-the-assault-of-non-solicited-pornography-and-marketing-act-of-2003>, (last visited May 25, 2019).

⁶⁰² Hiscox CyberClear Policy TPCCYB P0001 CW (05/16) pg. 10.

⁶⁰³ Beazley Group, Beazley Breach Response Policy F00653, 112017 ed.

⁶⁰⁴ 42 U.S.C.A. § 12111(5)(A) (West)

-
- ⁶⁰⁵ The Muddy Waters of ADA Website Compliance May Become Less Murky in 2019, Hunton Andrews Kurth, LLP, <https://www.huntonlaborblog.com/2019/01/articles/public-accommodations/muddy-waters-ada-website-compliance-may-become-less-murky-2019/>, (last visited May 25, 2019).
- ⁶⁰⁶ Letter from Stephen E. Boyd, Assistant Attorney General United States Department of Justice to Rep. Ted Budd (2018), Seyfarth Shaw, LLP, <https://www.adatitleiii.com/wp-content/uploads/sites/121/2018/10/DOJ-letter-to-congress.pdf>, (last visited May 25, 2019).
- ⁶⁰⁷ Information and Communication Technology (ICT) Standards and Guidelines, 82 FR 5790-01
- ⁶⁰⁸ Web Content Accessibility Guidelines (WCAG) 2.0 (2008), W3C, <https://www.w3.org/TR/WCAG20/>, (last visited May 25, 2019).
- ⁶⁰⁹ The Muddy Waters of ADA Website Compliance May Become Less Murky in 2019, Hunton Andrews Kurth, LLP, <https://www.huntonlaborblog.com/2019/01/articles/public-accommodations/muddy-waters-ada-website-compliance-may-become-less-murky-2019/>, (last visited May 25, 2019).
- ⁶¹⁰ Understanding Conformance, W3C, <https://www.w3.org/TR/UNDERSTANDING-WCAG20/conformance.html#uc-levels-head>, (last visited May 25, 2019).
- ⁶¹¹ The Bureau, CONSUMER FINANCIAL PROTECTION BUREAU, <https://www.consumerfinance.gov/about-us/the-bureau/> (last visited Mar 7, 2020).
- ⁶¹² 12 U.S.C.A. § 5531 (West)
- ⁶¹³ In re Dwolla, Inc., 2016-CFPB-0007 (2016)
- ⁶¹⁴ In re Dwolla, Inc., 2016-CFPB-0007 (2016)
- ⁶¹⁵ In re Dwolla, Inc., 2016-CFPB-0007 (2016)
- ⁶¹⁶ In re Dwolla, Inc., 2016-CFPB-0007 (2016)
- ⁶¹⁷ In re Dwolla, Inc., 2016-CFPB-0007 (2016)
- ⁶¹⁸ In re Dwolla, Inc., 2016-CFPB-0007 (2016)
- ⁶¹⁹ Rachel Witkowski, AGs, NOT CFPB, SHOULD TAKE GREATER ROLE ON ENFORCEMENT: MULVANEY AMERICAN BANKER (2019), <https://www.americanbanker.com/news/ags-not-cfpb-should-take-greater-role-on-enforcement-mulvaney> (last visited Mar 7, 2020).
- ⁶²⁰ Rachel Witkowski, AGs, NOT CFPB, SHOULD TAKE GREATER ROLE ON ENFORCEMENT: MULVANEY AMERICAN BANKER (2019), <https://www.americanbanker.com/news/ags-not-cfpb-should-take-greater-role-on-enforcement-mulvaney> (last visited Mar 7, 2020). <https://www.americanbanker.com/opinion/a-hands-off-cfpb-might-cause-trouble-for-fintechs>
- ⁶²¹ Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay \$35 Million, SEC (2018), <https://www.sec.gov/news/press-release/2018-71> (last visited Mar 7, 2020).

⁶²² Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²³ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²⁴ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²⁵ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²⁶ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²⁷ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²⁸ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶²⁹ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶³⁰ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶³¹ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶³² Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶³³ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶³⁴ Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 FR 8166-01

⁶³⁵ § 27:37. Collecting documents located in foreign countries: Privacy laws, 3 N.Y. Prac., Com. Litig. in New York State Courts § 27:37 (4th ed.)

⁶³⁶ Regulation (EU)2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1 [hereinafter GDPR].

⁶³⁷ GDPR art. 4(1)

⁶³⁸ GDPR art. 4(1)

⁶³⁹ GDPR art. 6(2)

⁶⁴⁰ GDPR art. 58

⁶⁴¹ GDPR art. 58(4)

⁶⁴² Nina Bryant, et al, Early GDPR Enforcement Signals Complicated Future Landscape (Mar 21, 2019), <https://www.lawtechnologytoday.org/2019/03/early-gdpr-enforcement-signals-complicated-future-landscape/> (last visited Jun 12, 2019).

⁶⁴³ Mostafa Al Khonaizi, Fines Under GDPR in Non-EU Jurisdictions: Enforceable or Mere Reputation Risk?, <http://www.mjilonline.org/fines-under-eu-gdpr-in-non-eu-jurisdictions-enforceable-or-mere-reputation-risk/> (last visited Nov 17, 2019).

-
- ⁶⁴⁴ Privacy Shield Framework, The International Trade Administration (ITA), U.S. Department of Commerce, <https://www.privacyshield.gov/EU-US-Framework> (last visited Oct 1, 2019).
- ⁶⁴⁵ Privacy Shield Framework, The International Trade Administration (ITA), U.S. Department of Commerce, <https://www.privacyshield.gov/EU-US-Framework> (last visited Oct 1, 2019).
- ⁶⁴⁶ GDPR art. 2
- ⁶⁴⁷ General Data Protection Regulation (GDPR) FAQs for small organisations, INFORMATION COMMISSIONERS OFFICE (UK), <https://ico.org.uk/for-organisations/in-your-sector/business/guide-to-the-general-data-protection-regulation-gdpr-faqs/> (last visited Mar 7, 2019).
- ⁶⁴⁸ Mission Statement, Asia-Pacific Economic Cooperation, <https://www.apec.org/About-Us/About-APEC/Mission-Statement> (last visited Oct 05, 2019).
- ⁶⁴⁹ Member Economies, Asia-Pacific Economic Cooperation, <https://www.apec.org/About-Us/About-APEC/Member-Economies> (last visited Oct 05, 2019).
- ⁶⁵⁰ APEC Cross-Border Privacy Rules System goes public, Asia-Pacific Economic Cooperation, https://www.apec.org/Press/News-Releases/2012/0731_cbpr, (last visited Oct 07, 2019).
- ⁶⁵¹ APEC Cross-Border Privacy Rules System goes public (2012), <https://iapp.org/news/a/apec-announces-schellman-company-as-newest-us-accountability-agent-for-cbpr-certifications/>, (last visited Oct 05, 2019).
- ⁶⁵² Alex Wall, GDPR matchup: The APEC Privacy Framework and Cross-Border Privacy Rules, International Association of Privacy Professionals, <https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/>, (last visited Sep 13, 2019).
- ⁶⁵³ *In the Matter of Very Incognito Techs., Inc., Corp. d/b/a Vipvape.*, No. 162-3034, 2016 WL 2739343, at *1 (MSNET May 4, 2016)
- ⁶⁵⁴ *In the Matter of Very Incognito Techs., Inc., Corp. d/b/a Vipvape.*, No. 162-3034, 2016 WL 2739343, at *1 (MSNET May 4, 2016)
- ⁶⁵⁵ *In the Matter of Very Incognito Techs., Inc., A Corp. d/b/a Vipvape.*, No. 162-3034, 2016 WL 3626839, at *1 (MSNET June 21, 2016)
- ⁶⁵⁶ United States – Mexico – Canada Agreement, Executive Office of the President, Office of the United States Trade Representative, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>, (last visited Sep 13, 2019).
- ⁶⁵⁷ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 493 (2018).
- ⁶⁵⁸ See *Eyeblaster*, 613 F.3d at 800-802 and *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001)
- ⁶⁵⁹ *American Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 95 (4th Cir. 2003)

⁶⁶⁰ Liberty Corp. Capital Ltd. v. Security Safe Outlet, Inc., 937 F. Supp. 2d 891, 901 (E.D. Ky. 2013)

⁶⁶¹ Robert H. Jerry & Douglas R. Richmond, Understanding Insurance Law 497 (2018).

⁶⁶² Robert H. Jerry & Douglas R. Richmond, Understanding Insurance Law 497 (2018).

⁶⁶³ *Travelers Indemnity Company of America v. Portal Healthcare Solutions, LLC*, No. 14-1944 (4th Cir. April 11, 2016)(unpublished)

⁶⁶⁴ *Travelers Indemnity Company of America v. Portal Healthcare Solutions, LLC*, No. 14-1944 (4th Cir. April 11, 2016)(unpublished)

⁶⁶⁵ Zurich American Insurance Co. v. Sony Corp., No 651982/2011 (N.Y. Sup. Ct. 2014)

⁶⁶⁶ Zurich American Insurance Co. v. Sony Corp., No 651982/2011 (N.Y. Sup. Ct. 2014)

⁶⁶⁷ Creative Hospitality Ventures, Inc. v. United States Liability Insurance Co., 444 Fed. (11th Cir. Sept. 30, 2011)

⁶⁶⁸ Creative Hospitality Ventures, Inc. v. United States Liability Insurance Co., 444 Fed. (11th Cir. Sept. 30, 2011)

⁶⁶⁹ ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, INSURANCE JOURNAL (2014), <https://www.insurancejournal.com/news/east/2014/07/18/332655.htm> (last visited Apr 7, 2019).

⁶⁷⁰ ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, INSURANCE JOURNAL (2014), <https://www.insurancejournal.com/news/east/2014/07/18/332655.htm> (last visited Apr 7, 2019).

⁶⁷¹ ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, INSURANCE JOURNAL (2014), <https://www.insurancejournal.com/news/east/2014/07/18/332655.htm> (last visited Apr 7, 2019).

⁶⁷² Travelers Crime Policy Form CRI-3001 Ed. 01-09

⁶⁷³ Travelers Crime Policy Form CRI-3001 Ed. 01-09

⁶⁷⁴ Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 253 (5th Cir. 2016)

⁶⁷⁵ Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 254 (5th Cir. 2016)

⁶⁷⁶ Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 254 (5th Cir. 2016)

⁶⁷⁷ Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 254 (5th Cir. 2016)

⁶⁷⁸ Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 256–57 (5th Cir. 2016)

⁶⁷⁹ See *International Communications v. Great American Ins. Co.*, 2018 WL 2149769 at *4 (11th Cir., May 10, 2018); *Pestmaster Servs., Inc. v. Travelers Casualty & Ins. Co.*, 656 Fed. App'x. 332, 333 (9th Cir. 2016); *Pinnacle Processing Group, Inc. v. Hartford Casualty Ins.*, 2011 WL 5299557, at *5 (W.D. Wash. Nov. 4, 2011)

⁶⁸⁰ Travelers Crime Policy Form CRI-3001 Ed. 01-09

⁶⁸¹ Travelers Crime Policy Form CRI-3001 Ed. 01-09

⁶⁸² Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368RSL, 2016 WL 3655265, at *1 (W.D. Wash. July 8, 2016), aff'd, 719 F. App'x 701 (9th Cir. 2018).

⁶⁸³ Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368RSL, 2016 WL 3655265, at *2 (W.D. Wash. July 8, 2016), aff'd, 719 F. App'x 701 (9th Cir. 2018).

⁶⁸⁴ Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368RSL, 2016 WL 3655265, at *3 (W.D. Wash. July 8, 2016), aff'd, 719 F. App'x 701 (9th Cir. 2018).

⁶⁸⁵ Authors' survey of 15 well known Crime Insurance Policies.

⁶⁸⁶ CAMICO Mutual Insurance Company Privacy and Client Network Damage Liability Coverage Endorsement Form PL-1049-A

⁶⁸⁷ CAMICO Mutual Insurance Company Privacy and Client Network Damage Liability Coverage Endorsement Form PL-1049-A

⁶⁸⁸ Authors' survey of 15 Professional Liability Insurance Policies.

⁶⁸⁹ CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, LLP, No. CIV.A. 11-4753, 2013 WL 3481527, at *1–2 (E.D. Pa. June 28, 2013), aff'd sub nom.

CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, L.L.P., 587 F. App'x 726 (3d Cir. 2014).

⁶⁹⁰ CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, LLP, No. CIV.A. 11-4753, 2013 WL 3481527, at *2 (E.D. Pa. June 28, 2013), aff'd sub nom. CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, L.L.P., 587 F. App'x 726 (3d Cir. 2014).

⁶⁹¹ CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, LLP, No. CIV.A. 11-4753, 2013 WL 3481527, at *10 (E.D. Pa. June 28, 2013), aff'd sub nom. CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, L.L.P., 587 F. App'x 726 (3d Cir. 2014).

⁶⁹² CAMICO Mut. Ins. Co. v. Heffler, Radetich & Saitta, L.L.P., 587 F. App'x 726, 731 (3d Cir. 2014).

⁶⁹³ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 539 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁶⁹⁴ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 539 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁶⁹⁵ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 539 (E.D. Va. 2010).

⁶⁹⁶ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 539 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁶⁹⁷ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 540 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011),

and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁶⁹⁸ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 540–41 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁶⁹⁹ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 541 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁷⁰⁰ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 542 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁷⁰¹ Bryan Bros. Inc. v. Cont'l Cas. Corp., 704 F. Supp. 2d 537, 544 (E.D. Va. 2010), aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 660 F.3d 827 (4th Cir. 2011), and aff'd sub nom. Bryan Bros. Inc. v. Cont'l Cas. Co., 419 F. App'x 422 (4th Cir. 2011).

⁷⁰² Joseph E Brunsman & Daniel W Hudson, *Should CPA Firms Be Worried about Data Breach Claims?: Hurdles to Establishing Standing and Demonstrating Economic Viability*, THE CPA JOURNAL, 2019, at 16–18.

⁷⁰³ CNA Policy CAN-87510XX (11-16) CPA NetProtect Endorsement

⁷⁰⁴ CNA Policy CAN-87510XX (11-16) CPA NetProtect Endorsement

⁷⁰⁵ CNA Policy CAN-87510XX (11-16) CPA NetProtect Endorsement

⁷⁰⁶ Average demanded ransom from ransomware attacks 2017 | Statistic, STATISTA (2017), <https://www.statista.com/statistics/701003/average-amount-of-ransom-requested-to-msp-clients/> (last visited Apr 7, 2019).

⁷⁰⁷ CNA Policy CAN-87510XX (11-16) CPA NetProtect Endorsement

⁷⁰⁸ Authors' review of over 15 Accountants Professional Liability Insurance policy endorsements

⁷⁰⁹ ROBERT H. JERRY & DOUGLAS R. RICHMOND, UNDERSTANDING INSURANCE LAW 128 (2018).

⁷¹⁰ Employment Practices Liability Insurance (EPLI) Policies and Coverage, Practical Law Practice Note w-006-7127

⁷¹¹ Kevin LaCroix, Fifth Circuit Reverses Dismissal of Data Breach Coverage Suit Against D&O Insurer (2018), The D&O Diary, <https://www.dandodiary.com/2018/07/articles/d-o-insurance/fifth-circuit-reverses-dismissal-data-breach-coverage-suit-insurer/>, (last visited Jul 7, 2019).

⁷¹² Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 234 (5th Cir. 2018)

⁷¹³ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 234–35 (5th Cir. 2018)

⁷¹⁴ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 236 (5th Cir. 2018)

-
- ⁷¹⁵ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 236 (5th Cir. 2018)
- ⁷¹⁶ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 235–36 (5th Cir. 2018)
- ⁷¹⁷ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 236 (5th Cir. 2018)
- ⁷¹⁸ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 240 (5th Cir. 2018)
- ⁷¹⁹ Spec's Family Partners, Ltd. v. Hanover Ins. Co., 739 F. App'x 233, 239 (5th Cir. 2018)
- ⁷²⁰ Kevin LaCroix, Fifth Circuit Reverses Dismissal of Data Breach Coverage Suit Against D&O Insurer (2018), The D&O Diary, <https://www.dandodiary.com/2018/07/articles/d-o-insurance/fifth-circuit-reverses-dismissal-data-breach-coverage-suit-insurer/>, (last visited Jul 7, 2019).
- ⁷²¹ § 14:24.Technology Errors and Omissions Liability (“Tech E&O”), 2 Data Sec. & Privacy Law § 14:24 (2018)
- ⁷²² See Hiscox Pro Privacy Pre-Priced Application PLPPVY A0001 (11/15) for Conditional Terms and Quotes.
- ⁷²³ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 5 JOURNAL OF CYBERSECURITY 16-18 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.
- ⁷²⁴ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 5 JOURNAL OF CYBERSECURITY 18-19 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.
- ⁷²⁵ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 5 JOURNAL OF CYBERSECURITY 19-20 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.
- ⁷²⁶ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 5 JOURNAL OF CYBERSECURITY 19-20 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.
- ⁷²⁷ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 5 JOURNAL OF CYBERSECURITY 20 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.
- ⁷²⁸ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)
- ⁷²⁹ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)
- ⁷³⁰ Kenneth RICE, individually, and on behalf of all others similarly situated, Plaintiffs, v. INSYNC, an unknown type of corporation, Cottage Health System, a California corporation; Santa Barbara Cottage Hospital, a California corporation, Goleta Valley Cottage Hospital, a California Corporation, and Santa Ynez Valley Hospital, and Does 1-100, Inclusive, Defendants., 2014 WL 358703 (Cal.Super.)
- ⁷³¹ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³² Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³³ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³⁴ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³⁵ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³⁶ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³⁷ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³⁸ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷³⁹ Columbia Casualty Company, Plaintiff, v. Cottage Health System, Defendant., 2015 WL 2393298 (C.D.Cal.)

⁷⁴⁰ Columbia Cas. Co. v. Cottage Health Sys., No. CV1503432DDPAGRX, 2015 WL 4497730, at *1 (C.D. Cal. July 17, 2015)

⁷⁴¹ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 5 JOURNAL OF CYBERSECURITY 5 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.

⁷⁴² Lloyd's Annual Report 2017, https://www.lloyds.com/~media/files/lloyds/investor-relations/results/2017ar/ar2017_annual-report-2017.pdf, (last visited Jul 9, 2019).

⁷⁴³ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁴⁴ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁴⁵ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁴⁶ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁴⁷ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁴⁸ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁴⁹ Mondelez International, Inc., Plaintiff, v. Zurich American Insurance Company, Defendant., 2018 WL 4941760 (Ill.Cir.Ct.)

⁷⁵⁰ See *Addison Insurance Co. v. Fay*, 232 Ill.2d 446, 453–54, 328 Ill.Dec. 858, 905 N.E.2d 747 (2009)

⁷⁵¹ Statement from the Press Secretary, THE WHITE HOUSE (2018), <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/> (last visited Apr 8, 2019).

-
- ⁷⁵² Cybersecurity Insurance Workshop Readout Report, (2012), [https://www.dhs.gov/sites/default/files/publications/November 2012 Cybersecurity Insurance Workshop.pdf](https://www.dhs.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf) (last visited Feb 2019).
- ⁷⁵³ Hiscox Policy PLP P0004 CW (06/14)
- ⁷⁵⁴ Hiscox Policy PLP P0004 CW (06/14)
- ⁷⁵⁵ Axis Policy PBR-0300 (05-11)
- ⁷⁵⁶ Axis Policy PBR-0300 (05-11)
- ⁷⁵⁷ Thomas H. Bentz, Jr., Is Your Cyber Liability Insurance Any Good? A Guide for Banks to Evaluate Their Cyber Liability Insurance Coverage, 21 N.C. Banking Inst. 39 (2017)
- ⁷⁵⁸ Thomas H. Bentz, Jr., Is Your Cyber Liability Insurance Any Good? A Guide for Banks to Evaluate Their Cyber Liability Insurance Coverage, 21 N.C. Banking Inst. 39 (2017)
- ⁷⁵⁹ Beazley Policy F00654 112017 ed.
- ⁷⁶⁰ Hiscox Policy PLP D0001 CW (04/14)
- ⁷⁶¹ 2018 Cost of a Data Breach Study: Global Overview, IBM SECURITY, available at: <https://www.ibm.com> (last visited Mar 2019).
- ⁷⁶² Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *1 (N.D. Ala. Oct. 25, 2016)
- ⁷⁶³ Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *1 (N.D. Ala. Oct. 25, 2016)
- ⁷⁶⁴ Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *1 (N.D. Ala. Oct. 25, 2016)
- ⁷⁶⁵ Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *5 (N.D. Ala. Oct. 25, 2016)
- ⁷⁶⁶ Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *6 (N.D. Ala. Oct. 25, 2016)
- ⁷⁶⁷ Hiscox CyberClear Policy TPCCYB P0001 CW (05/16)
- ⁷⁶⁸ Markel American Insurance Company Professional Liability Policy MPL 0002 07 17
- ⁷⁶⁹ Robert H. Jerry & Douglas R. Richmond, Understanding Insurance Law 678-679 (2018).
- ⁷⁷⁰ Robert H. Jerry & Douglas R. Richmond, Understanding Insurance Law 687 (2018).
- ⁷⁷¹ § 98:19.Doctrine of mutual repugnancy, 7 Couch on Ins. § 98:19
- ⁷⁷² Robert H. Jerry & Douglas R. Richmond, Understanding Insurance Law 701-705 (2018).
- ⁷⁷³ Robert H. Jerry & Douglas R. Richmond, Understanding Insurance Law 680-692 (2018).
- ⁷⁷⁴ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyperpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁷⁵ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁷⁶ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁷⁷ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁷⁸ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁷⁹ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁸⁰ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835

⁷⁸¹ New Hotel Monteleone, Llc, V. Certain Underwriters at Lloyd's Of London, Subscribing to Ascent Cyberpro Policy No. ASC14C000944, and Eustis Insurance, Inc., 2016 WL 109835 (E.D.La.)

⁷⁸² See *National Union Fire Ins. Co. of Pittsburgh v. Willis*, 139 F.Supp.2d 827, 832 (S.D.Tex.2001), *aff'd*, 296 F.3d 336, 339 (5th Cir.2002)

⁷⁸³ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 579-581 (2018).

⁷⁸⁴ *Cyber Insurance: Insuring for Data Breach Risk*, Practical Law Practice Note 2-588-8785

⁷⁸⁵ 2018 Cost of a Data Breach Study: Global Overview, IBM SECURITY, available at: <https://www.ibm.com> (last visited Mar 2019).

⁷⁸⁶ *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 696 (7th Cir. 2015)

⁷⁸⁷ *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307, 198 L. Ed. 2d 728 (2017)

⁷⁸⁸ Hack attack causes 'massive damage' at steel works, BBC NEWS (2014), <https://www.bbc.com/news/technology-30575104> (last visited Mar 7, 2020).

⁷⁸⁹ Chuck Squatriglia, POLISH TEEN HACKS HIS CITY'S TRAMS, CHAOS ENSUES WIRED (2017), <https://www.wired.com/2008/01/polish-teen-hac/> (last visited Mar 7, 2020).

⁷⁹⁰ Sasha Romanosky et al., *Content analysis of cyber insurance policies: how do carriers price cyber risk?*, 14 – Footnote 24 JOURNAL OF CYBERSECURITY 5 (2019), <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>.

⁷⁹¹ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 422-427 (2018).

⁷⁹² See HiscoxPro Policy PLP P0005 CW (06/14)

⁷⁹³ See HiscoxPro Policy PLP P0005 CW (06/14)

-
- ⁷⁹⁴ See HiscoxPro Policy PLP P0005 CW (06/14)
- ⁷⁹⁵ 16 A.L.R.4th 11 (Originally published in 1982)
- ⁷⁹⁶ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 527 (2018).
- ⁷⁹⁷ Kevin LaCroix, ARE GDPR FINES AND PENALTIES INSURABLE? THE D&O DIARY (2018), <https://www.dandodiary.com/2018/11/articles/cyber-liability/gdpr-fines-penalties-insurable/> (last visited Mar 7, 2020).
- ⁷⁹⁸ 16 A.L.R.4th 11 (Originally published in 1982)
- ⁷⁹⁹ See generally Erie R. Co. v. Tompkins, 304 U.S. 64, 58 S. Ct. 817, 82 L. Ed. 1188 (1938), and 28 U.S.C.A. § 1652 (West)
- ⁸⁰⁰ Drexel Burnham Lambert Grp., Inc. v. Vigilant Ins. Co., 157 Misc. 2d 198, 213, 595 N.Y.S.2d 999, 1010 (Sup. Ct. 1993)
- ⁸⁰¹ Fairfield Ins. Co. v. Stephens Martin Paving, LP, 246 S.W.3d 653 (Tex. 2008)
- ⁸⁰² Fairfield Ins. Co. v. Stephens Martin Paving, LP, 246 S.W.3d 653, 670 (Tex. 2008)
- ⁸⁰³ Fairfield Ins. Co. v. Stephens Martin Paving, LP, 246 S.W.3d 653, 670 (Tex. 2008)
- ⁸⁰⁴ Wilson v. Chem-Solv, Inc., No. 85-C-MY-1, 1988 WL 109375, at *1 (Del. Super. Ct. Oct. 14, 1988)
- ⁸⁰⁵ Wilson v. Chem-Solv, Inc., No. 85-C-MY-1, 1988 WL 109375, at *1 (Del. Super. Ct. Oct. 14, 1988)
- ⁸⁰⁶ Bullock v. Maryland Cas. Co., 85 Cal. App. 4th 1435, 1447, 102 Cal. Rptr. 2d 804, 812 (2001)
- ⁸⁰⁷ Elise Hu, I FEEL NOTHING: THE HOME DEPOT HACK AND DATA BREACH FATIGUE NPR (2014), <https://www.npr.org/sections/alltechconsidered/2014/09/03/345539074/i-feel-nothing-the-home-depot-hack-and-data-breach-fatigue> (last visited Mar 7, 2020).
- ⁸⁰⁸ Updated guide on the insurability of GDPR fines across Europe: Insights: DLA Piper Global Law Firm, DLA PIPER, <https://www.dlapiper.com/en/uk/insights/publications/2019/07/updated-guide-on-the-insurability-of-gdpr-fines-across-europe/> (last visited Mar 7, 2020).
- ⁸⁰⁹ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 976 (2018).
- ⁸¹⁰ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 977-978 (2018).
- ⁸¹¹ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 976 (2018).
- ⁸¹² QBE Excess Policy Form # QBEX-1000 (01-14)
- ⁸¹³ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 978 (2018).
- ⁸¹⁴ QBE Excess Policy Form # QBEX-1000 (01-14)
- ⁸¹⁵ In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1326 (N.D. Ga. 2019)
- ⁸¹⁶ Hiscox Pro Policy PLP P0004 CW (06/14) at 4.

-
- ⁸¹⁷ Hiscox Pro Policy PLP P0004 CW (06/14) at 4.
- ⁸¹⁸ Public Statement - Network and Service Interruptions (2019), Wolters Kluwer, <https://wolterskluwer.com/company/newsroom/news/2019/05/media-statement---network-and-service-interruptions.html>, (last visited Oct 6, 2019).
- ⁸¹⁹ Public Statement - Network and Service Interruptions (2019), Wolters Kluwer, <https://wolterskluwer.com/company/newsroom/news/2019/05/media-statement---network-and-service-interruptions.html>, (last visited Oct 6, 2019).
- ⁸²⁰ Hiscox CyberClear Policy form: TPCCYB P0001 CW (05/16)
- ⁸²¹ Hiscox CyberClear Policy form: TPCCYB P0001 CW (05/16)
- ⁸²² Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 982 (2018).
- ⁸²³ CFC Cyber Private enterprise policy form v2.1
- ⁸²⁴ Hiscox Pro Policy Form, New Jersey Amendatory Endorsement, PLP E9027 NJ (07/14)
- ⁸²⁵ Robert H. Jerry & Douglas R. Richmond, *Understanding Insurance Law* 738 (2018).
- ⁸²⁶ *Understanding Insurance Law* page 738
- ⁸²⁷ Hiscox CyberClear new business application form: XXX A00XXS CW (XX/XX)
- ⁸²⁸ *Understanding Insurance Law* page 744
- ⁸²⁹ Paul A. Grassi *et al.*, Nist Special Publication 800-63b: Digital Identity Guidelines - Authentication And Lifecycle Management Nist Special Publication 800-63b: Digital Identity Guidelines - Authentication And Lifecycle Management (2017), <https://pages.nist.gov/800-63-3/sp800-63b.html#sec3>, (last visited Sep 7, 2019).
- ⁸³⁰ Paul Cichonski, *et al.*, Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide, National Institute of Standards and Technology – U.S. Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>, (last visited Sep 7, 2019).
- ⁸³¹ NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds, DARK READING (2016), <https://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901> (last visited Oct 15, 2018).
- ⁸³² The NIST Cybersecurity Framework, Practical Law Practice Note 5-599-6825 (West)
- ⁸³³ The NIST Cybersecurity Framework and the FTC, FEDERAL TRADE COMMISSION (2017), <https://www.ftc.gov/news-events/audio-video/video/nist-cybersecurity-framework-ftc> (last visited Oct 18, 2018).
- ⁸³⁴ OHIO REV. CODE ANN. §1354.01-05 (West 2018)
- ⁸³⁵ OHIO REV. CODE ANN. §1354.01-05 (West 2018)
- ⁸³⁶ OHIO REV. CODE ANN. §1354.01-05 (West 2018)
- ⁸³⁷ Exec. Order No. 13800, 82 FR 22391, 2017 WL 2062698(Pres.)

-
- ⁸³⁸ The NIST Cybersecurity Framework at 8,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018>.
- ⁸³⁹ The NIST Cybersecurity Framework at 9,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018>.
- ⁸⁴⁰ The NIST Cybersecurity Framework at 9,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018>.
- ⁸⁴¹ The NIST Cybersecurity Framework at 10,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018>.
- ⁸⁴² The NIST Cybersecurity Framework at 10,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018>.
- ⁸⁴³ Nicole Keller, AN INTRODUCTION TO THE COMPONENTS OF THE FRAMEWORK NIST (2018), <https://www.nist.gov/cyberframework/online-learning/components-framework> (last visited Apr 16, 2019).
- ⁸⁴⁴ The NIST Cybersecurity Framework at 7,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- ⁸⁴⁵ The NIST Cybersecurity Framework at 8,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- ⁸⁴⁶ The NIST Cybersecurity Framework at 7,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- ⁸⁴⁷ The NIST Cybersecurity Framework at 38-39,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- ⁸⁴⁸ The NIST Cybersecurity Framework at 18,
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- ⁸⁴⁹ Managing Enterprise Risks in a Digital World: Privacy, Cybersecurity, and Compliance Collide Baker Hostetler (2019), BakerHostetler,
https://f.datasrvr.com/fr1/019/33725/2019_BakerHostetler_DSIR_Final.pdf, (last visited Oct 6, 2019)
- ⁸⁵⁰ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)
- ⁸⁵¹ Lindsey Howard, individually and on behalf of all others similarly situated, Plaintiff, v. Citrix Systems, Inc., Defendant., 2019 WL 2263036 (S.D.Fla.)
- ⁸⁵² Lindsey Howard, individually and on behalf of all others similarly situated, Plaintiff, v. Citrix Systems, Inc., Defendant., 2019 WL 2263036 (S.D.Fla.)
- ⁸⁵³ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)
- ⁸⁵⁴ U.S. Dep't of Homeland Security, Alert (TA18-086A): Brute Force Attacks Conducted by Cyber Actors (Mar. 27, 2018, last revised March 28, 2018), available at: <https://www.us-cert.gov/ncas/alerts/TA18-086A> (last visited June 3, 2019).
- ⁸⁵⁵ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)
- ⁸⁵⁶ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)

⁸⁵⁷ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)

⁸⁵⁸ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)

⁸⁵⁹ Lindsey HOWARD, individually and on behalf of all others similarly situated, Plaintiff, v. CITRIX SYSTEMS, INC., Defendant., 2019 WL 2263036 (S.D.Fla.)

⁸⁶⁰ About: Overview, Cloud Security Alliance,
<https://cloudsecurityalliance.org/about/>, (last visited Oct 07, 2019).

⁸⁶¹ Working Group: Cloud Controls Matrix; Introduction,
https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview, (last visited Oct 07, 2019).

⁸⁶² Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2011), Cloud Security Alliance,
<https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>, (last visited Oct 07, 2019).

⁸⁶³ In the Matter of Gmr Transcription Servs., Inc., A Corp., Ajay Prasad & Shreekant Srivastava, Individually & As Officers of Gmr Transcription Servs., Inc., 2015-1 Trade Cas. (CCH) 17070 (MSNET Aug. 14, 2014)

⁸⁶⁴ In the Matter of Gmr Transcription Servs., Inc., A Corp., Ajay Prasad & Shreekant Srivastava, Individually & As Officers of Gmr Transcription Servs., Inc., 2015-1 Trade Cas. (CCH) 17070 (MSNET Aug. 14, 2014)

⁸⁶⁵ In the Matter of Gmr Transcription Servs., Inc., A Corp., Ajay Prasad & Shreekant Srivastava, Individually & As Officers of Gmr Transcription Servs., Inc., 2015-1 Trade Cas. (CCH) 17070 (MSNET Aug. 14, 2014)

⁸⁶⁶ In the Matter of Gmr Transcription Servs., Inc., A Corp., Ajay Prasad & Shreekant Srivastava, Individually & As Officers of Gmr Transcription Servs., Inc., 2015-1 Trade Cas. (CCH) 17070 (MSNET Aug. 14, 2014)

⁸⁶⁷ Written Information security Program (WISP), Practical Law Standard Document w-001-0073

⁸⁶⁸ Developing Information security Policies, Practical Law Practice Note w-001-1336

⁸⁶⁹ SOC For Cybersecurity, AICPA (2020),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservice/s/downloadabledocuments/soc-for-cybersecurity-brochure.pdf> (last visited Mar 7, 2020).

⁸⁷⁰ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 457 (6th Cir. 2018)

⁸⁷¹ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 458 (6th Cir. 2018)

⁸⁷² Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 458 (6th Cir. 2018)

⁸⁷³ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 458 (6th Cir. 2018)

-
- ⁸⁷⁴ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356, at *1 (E.D. Mich. Aug. 1, 2017), rev'd and remanded, 895 F.3d 455 (6th Cir. 2018)
- ⁸⁷⁵ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 458 (6th Cir. 2018)
- ⁸⁷⁶ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 458 (6th Cir. 2018)
- ⁸⁷⁷ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 457 (6th Cir. 2018)
- ⁸⁷⁸ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017), rev'd and remanded, 895 F.3d 455 (6th Cir. 2018)
- ⁸⁷⁹ Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 465 (6th Cir. 2018)
- ⁸⁸⁰ Kevin L. Miller, What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach, Fla. B.J., September/October 2016, at 22, 26
- ⁸⁸¹ Statement on Standards for Attestation Engagements (SSAE) 18, (2016), <https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf> (last visited Jan 7, 2020).
- ⁸⁸² Statement on Standards for Attestation Engagements (SSAE) 18, (2016), <https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf> (last visited Jan 7, 2020).
- ⁸⁸³ Statement on Standards for Attestation Engagements (SSAE) 18, (2016), <https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf> (last visited Jan 7, 2020).
- ⁸⁸⁴ Statement on Standards for Attestation Engagements (SSAE) 18, (2016), <https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf> (last visited Jan 7, 2020).
- ⁸⁸⁵ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017), <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁸⁶ Statement on Standards for Attestation Engagements (SSAE) 18, (2016), <https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf> (last visited Jan 7, 2020).
- ⁸⁸⁷ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017), <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁸⁸ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017), <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).

-
- ⁸⁸⁹ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹⁰ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹¹ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹² Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹³ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹⁴ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹⁵ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹⁶ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹⁷ Assurance Services Executive Committee (ASEC), TRUST SERVICES CRITERIA AICPA (2017),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf> (last visited Feb 8, 2020).
- ⁸⁹⁸ SOC For Cybersecurity, AICPA (2020),
<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-brochure.pdf> (last visited Mar 7, 2020).
- ⁸⁹⁹ SOC for Cybersecurity: Information for Organizations, AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS,
<https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityfororganizations.html> (last visited Mar 7, 2020).

-
- ⁹⁰⁰ In the Matter of Gmr Transcription Servs., Inc., A Corp., Ajay Prasad & Shreekant Srivastava, Individually & As Officers of Gmr Transcription Servs., Inc., 2015-1 Trade Cas. (CCH) 17070 (MSNET Aug. 14, 2014)
- ⁹⁰¹ § 6:4.Gramm-Leach-Bliley Act (GLBA)—GLBA's Safeguards Rule, 1 Law and Business of Computer Software § 6:4 (2d ed.)
- ⁹⁰² 45 C.F.R. § 164.504(e)(2)(ii)(B)
- ⁹⁰³ 45 C.F.R. § 164.314
- ⁹⁰⁴ 34 C.F.R. § 99.31
- ⁹⁰⁵ Regulation (EU)2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1
- ⁹⁰⁶ 201 Mass. Code Regs. 17.04
- ⁹⁰⁷ Ala. Code 1975, § 8-38-3
- ⁹⁰⁸ A.C.A. § 4-110-104(b)
- ⁹⁰⁹ Cal. Civ. Code § 1798.81.5
- ⁹¹⁰ Colo. Rev. Stat. Ann. § 6-1-713.5
- ⁹¹¹ Conn. Gen. Stat. Ann. § 42-471(a)
- ⁹¹² Del. Code Ann. tit. 6, § 12B-100
- ⁹¹³ Fla. Stat. Ann. § 501.171 (West)
- ⁹¹⁴ 815 ILCS 530/45
- ⁹¹⁵ Ind. Code Ann. § 24-4.9-3-3.5
- ⁹¹⁶ K.S.A 50-6,139b
- ⁹¹⁷ La. R.S. 51:3074(A)
- ⁹¹⁸ Md. Code Ann., Com. Law § 14-3503
- ⁹¹⁹ Neb. Rev. Stat. §§ 87-801 through 87-808
- ⁹²⁰ NRS 603A.210, 603A.215
- ⁹²¹ NMSA 1978, §§ 57-12C-4, 57-12C-5
- ⁹²² S.5575B/A.5635 § 4
- ⁹²³ Or. Rev. Stat. § 646A.622
- ⁹²⁴ R.I. Gen. Laws § 11-49.3-2
- ⁹²⁵ Tex. Bus. & Com. Code Ann. § 521.052 (West)
- ⁹²⁶ Utah Code § 13-44-201(1)(a)
- ⁹²⁷ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.3
- ⁹²⁸ Markel Cambridge Alliance, Safeguarding Client Information And Avoiding Wire Fraud. (n.d) retrieved January 2016, from Markel Cambridge Alliance Web Site: <http://www.markelinsurance.com/risk-management-home/msc-articles/investment-advisors/safeguarding-client-information-and-avoiding-wire-fraud>
- ⁹²⁹ U.S. Securities and Exchange Commission, (2015, September, 22). *SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach*. retrieved December 2015, from SEC Web Site: <http://www.sec.gov/news/pressrelease/2015-202.html>

⁹³⁰ Cipriani, J. (2015, June, 15). *Two-factor authentication: What you need to know (FAQ)*. retrieved December 2015, from c|net Web Site:

<http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>

⁹³¹ Coutin, C. (2015, August, 13). *Educating Clients About Cyber Security Should Be Part of Your Role as an RIA*. retrieved September 13 2015, from Morningstar:

ByAllAccounts Web Site: <http://byallaccounts.morningstar.com/blog/586-educating-clients-about-cyber-security-should-be-part-of-your-role-as-an-ria.html>

⁹³² Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³³ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³⁴ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³⁵ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³⁶ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³⁷ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³⁸ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 1391493 (S.D.Tex.)

⁹³⁹ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 2728739 (S.D.Tex.)

⁹⁴⁰ Ameriforge Group, Inc., a Texas corporation d/b/a AFGlobal Corporation, Plaintiff, v. Federal Insurance Company, an Indiana corporation admitted to conduct insurance business in Texas, including Chubb & Son, a Division of Federal Insurance Company, Defendant., 2016 WL 2728739 (S.D.Tex.)

~Fair Winds & Following Seas~