SESSION ID: CXO-R05

DATA BREACH LITIGATION

HOW TO AVOID IT AND BE BETTER PREPARED

March 3, 2016

Ronald I. Raether, Jr.
Partner
Troutman Sanders

Andrea Hoy, CISSP, CISM, MBA
Founder and Virtual CISO
A. Hoy & Associates

Agenda

I. Background: Where are the Data Breaches occurring?

II. How to Be Better Prepared for When Your Company Data is Breached

  A. Incident Response Plan – Must Haves

  B. Components of Data Breach Litigation for the CXO

  C. Top Ten Suggestions For Effective Management of Complex Business Litigation and Class Actions

III. How to Avoid It: Lessons Learned & Best Practices

  A. Top 10 Steps for Data Litigation Preparedness

Cyberattacks and Breaches

1,023,108,267

Records
Breached in
2014

Cyberattacks in
the United
States in 2013:

$1.5 million

Cybercrime has cost
the global economy
annually:

$575 billion

Reported Breaches
in 2015 for 2014:

2,122 Global (781 US)

Data records were lost or stolen with the following frequency:

Every second	32
Every minute	1,947
Every day	2,803,036
Every hour	116,793

Data Breaches by Industry

Avg. Total Cost/lost or Stolen record

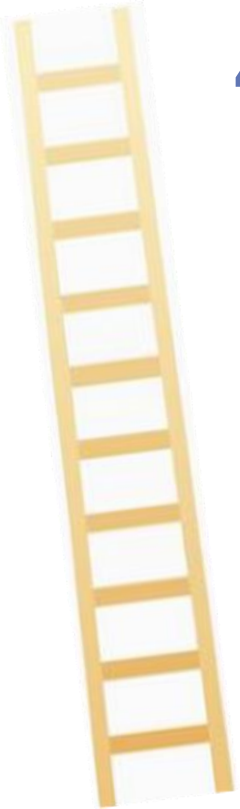
$217

35.5%

Healthcare

Avg. Total Cost of a Data Breach

$6.5 million



40.0%

Business → (Retail / Utilities
Travel / Hospitality
Transportation / Others)

9.1%

Financial

8.1%

Government /
Military

7.4%

Education

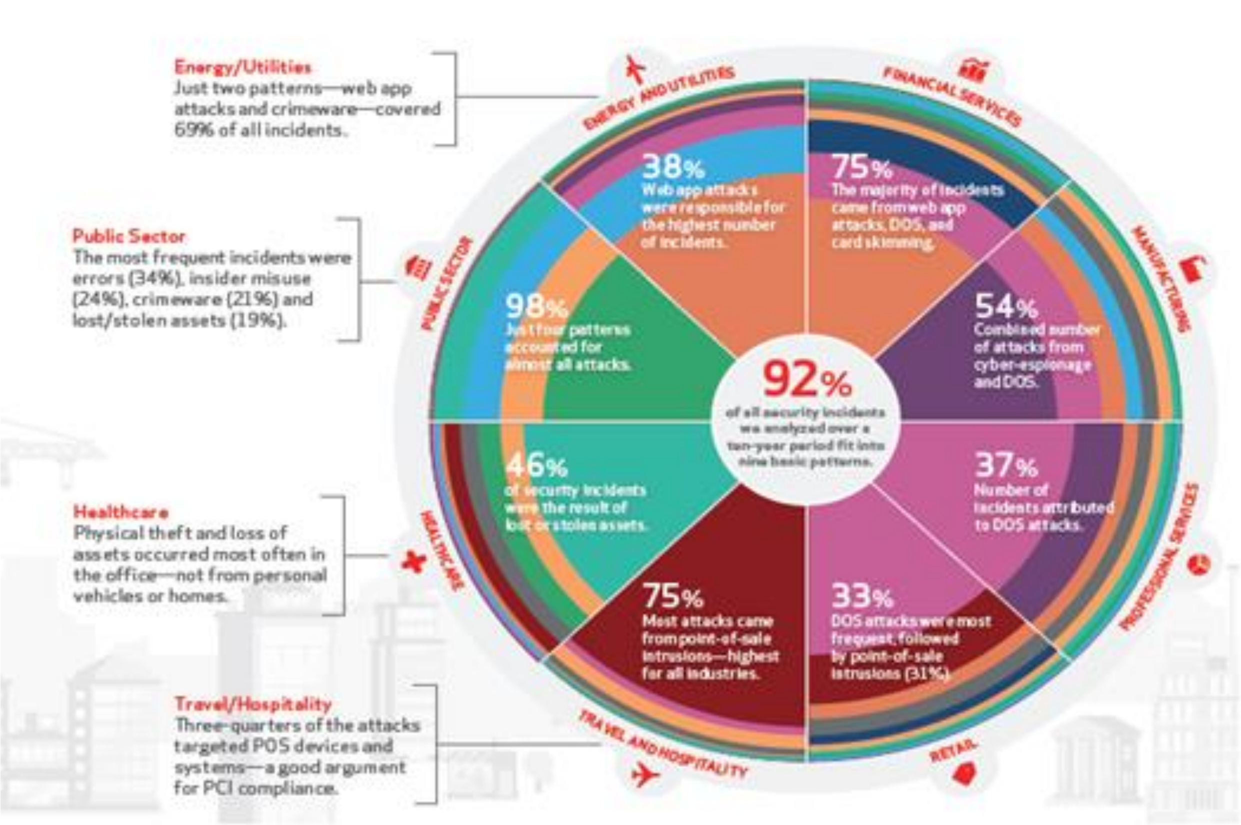
RSAConference2016

Source: 2015Ponemon and IBM Report

TROUTMAN SANDERS

A. HOY & ASSOCIATES

Major Types of Data Breaches by Industry



Energy/Utilities
Just two patterns—web app attacks and crimeware—covered 69% of all incidents.

Public Sector
The most frequent incidents were errors (34%), insider misuse (24%), crimeware (21%) and lost/stolen assets (19%).

Healthcare
Physical theft and loss of assets occurred most often in the office—not from personal vehicles or homes.

Travel/Hospitality
Three-quarters of the attacks targeted POS devices and systems—a good argument for PCI compliance.

38% Web app attacks were responsible for the highest number of incidents.

75% The majority of incidents came from web app attacks, DOS, and card skimming.

98% Just four patterns accounted for almost all attacks.

54% Combined number of attacks from cyber-espionage and DOS.

92% of all security incidents we analyzed over a ten-year period fit into nine basic patterns.

46% of security incidents were the result of lost or stolen assets.

37% Number of incidents attributed to DOS attacks.

75% Most attacks came from point-of-sale intrusions—highest for all industries.

33% DOS attacks were most frequent, followed by point-of-sale intrusions (31%).

Travel and Hospitality
- 91% up from 75 % POS

Financial Services
- 75% Web App attacks, DOS, card skimming

Public Sector
- 98% from 4 types

Healthcare*
- 46% Physical theft & loss

Energy/Utilities
- 38% Web App attacks
- 31% Crimeware

Retail
- 31% POS 33% DOS

Manufacturing
- 54% CyberEspionage And DOS

Professional Services
- 37% DOS

RSAConference2016

Source: Verizon 2014 Data Breach IR

TROUTMAN SANDERS

A. HOY & ASSOCIATES

Source: Verizon 2014 DBIR

Major Types of Data Breaches by Industry

Don’t Forget Data Breach can be Physical!

- Physical Loss and Theft
  - Public sector, followed by Healthcare and Financial
  - 55% Internal workplace
  - 22% Employee owned vehicles
  - Laptops, tablets, smartphones

So minor shifts between 2014 and 2015 reports

Considerations: Security Awareness Learning and Education,

Privileged Access Management

Lawsuits associated with Data Breaches

Reported Breaches in 2014 (2015):

1,367 (781)

BUT →

110

Lawsuits: 2014

Breaches - Retail

12.5%

BUT →

60%

Lawsuits – Retail

Incident Response – Being Prepared

1. Incident Response Plan
   - ✓ Address various types of Data Breach
   - ✓ Provide critical steps for reasonable investigation of each type
   - ✓ Execute and do table top tests quarterly/annually
   - ✓ Development and IR Team Members/Contact information
   - ✓ Critical Emergency Contact List
   - ✓ Identify regulated Notifications
     - ✓ Appropriate law enforcement
     - ✓ Affected parties – individuals and third parties
     - ✓ Federal Reserve Bank (FRB) / Federal Trade Commission (FTC) / States Attorney General(s)
     - ✓ Suspicious Activity Report (SAR)

Incident Response – Being Prepared

2. Third Party/Vendor Service Provider Incident Response
3. Keep an incident timeline and document efforts taken

- ✓ Who Reported the Breach
- ✓ How it was Discovered
- ✓ When and By Whom (may differ from who reported)
- ✓ Incident Response Team meeting(s)
- ✓ Actions taken to contain/control the breach or threat/vulnerability allowing the breach
- ✓ Additional Third Party / Forensic / Investigative assistance
- ✓ Regulatory notification

Incident Response – Being Prepared

4. Critical Emergency Contacts List
   - ✓ Incident Response Team
   - ✓ Data Breach Coach
   - ✓ Forensics expert/ Investigative expert
   - ✓ Public Relations Coach

5. Educate on where to store the IR Plan

6. Don't Forget to include a Sample Breach Notification

7. Timeline for Notification(s)

But what are the legal ramifications of giving Notice...

Is Notice Required?

- Take a Breath.
- Breach - Did you indeed have a breach as defined in the law?
- PII - Does the compromised information fit the definition of “personally identifiable information” as defined by the law?
- Notify - Considering the above, is there a duty to notify?
- Plan - Did you have and follow your IR Plan?

Notice is Required: Now What?

“Sixty-three percent of respondents said notification letters they received offered no direction on the steps the consumer should take to protect their personal information. As a result, 31 percent said they terminated their relationship with the organization. Fifty-seven percent said they lost trust and confidence in the organization.”

PONEMON INSTITUTE FOR ID EXPERTS, THE CONSUMER’S REPORT CARD ON DATA BREACH NOTIFICATION, SURVEY OF 1,795 U.S. ADULTS, APRIL 2008.

Event Response: Best Practices

- Accuracy & Speed
- Media Management
- Transparency
- Accountability
- Be Thorough
- Contacting Regulators
- Using Third-Party Firms/Partners

Best Practices: Contacting Regulators

- Consider reaching out to regulators, such as State Attorney Generals, before issuing a breach notice in order to
  - Keep them well-informed;
  - Avoid misunderstandings;
  - Avoid unnecessary points of conflict; and
  - Request their review of the notice.
- Certain states publish notice online (e.g., New Hampshire, Washington)

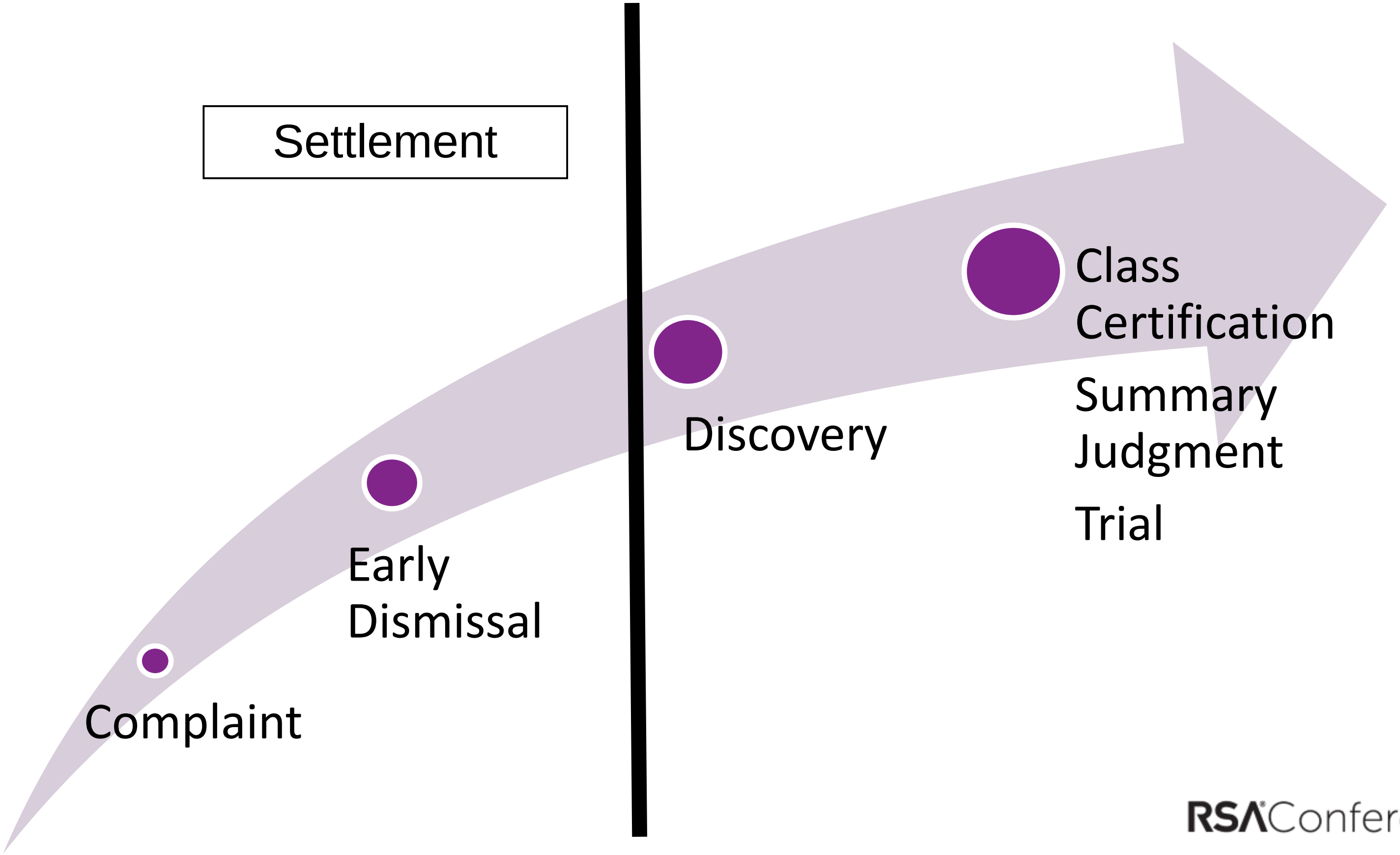
Best Practices: Documents & Regulators

- Privacy Policy
- Incident Response Plan
- Security Policies and Procedures
  - Content
  - Practice
- Security Awareness Learning and Education (S.A.L.E.)
- Business Continuity Plan
- Third Party/Vendor Management Plan

Top Ten Suggestions For Effective Management of Complex Business Litigation and Class Actions

1. Complex Litigation Needs to be Treated Differently – Select Appropriate Counsel
2. Avoid Side Issues – Preservation of Documents and Evidence
3. Control Costs and Budget Appropriately
4. Pay Attention to Changes In Law
5. Learn About Forum, Judge and Adversary
6. Participate Appropriately in Joint Defense Groups
7. Properly Assess the Risks of Litigation
8. Encourage Strategic Aggressiveness
9. Win the War, Not Just the Battles
10. Prepare to Win – If Appropriate, Settle Strategically

Lifecycle of Lawsuit



Settlement

Complaint

Early Dismissal

Discovery

Class Certification

Summary Judgment

Trial

What Is In The Complaint?

- You had unreasonable information security controls
- You took too long to notify me
- You breached your promise to provide reasonable security
- I would not have paid the stated price (or done business with you) had I known you had bad data security

In the future, please say "I object" rather than "that's total bullshit."

Opening Move – Alleged Harm

	Standing	Viable Claim
Unauthorized transaction (occurred)	YES	YES (but not if reimbursed)
Unauthorized transaction (future)	VARIES	NO
Time and Money spent resolving fraud	YES	YES (but not if reimbursed)
Time and Money spent protecting against future harm	VARIES	VARIES
Value of information	NO	NO
Overpayment	VARIES	VARIES

Shifting Blame and Liability

Payment Networks Liability Shift

- EMV (EuroPay, MasterCard, Visa)
- “Magstripe” to “Chip and PIN” or “Chip and Signature”
  - October 2015
  - Exception auto fuel dispensers - June 2017
  - Why? Card related financial fraud
- Bigger issue – shift of liability for this type of data breach
  - Affects banks, credit unions, financial institutions, merchants issuing credit/debit/payment cards

Why Are Cases Settling

- Lack of reasonable controls
- No Information Security Plan (ISP)
- ISPs inconsistent with practices
- Bad documents
- No witness

Governance, Risk and Compliance (GRC) But We Have To…

- The basic building blocks of any data governance plan are rooted in law and industry standards, best practices

HIPAA

GLBA, FFIEC CyberSecurity Assessment

PCI DSS

ISO/IEC 27001:2005

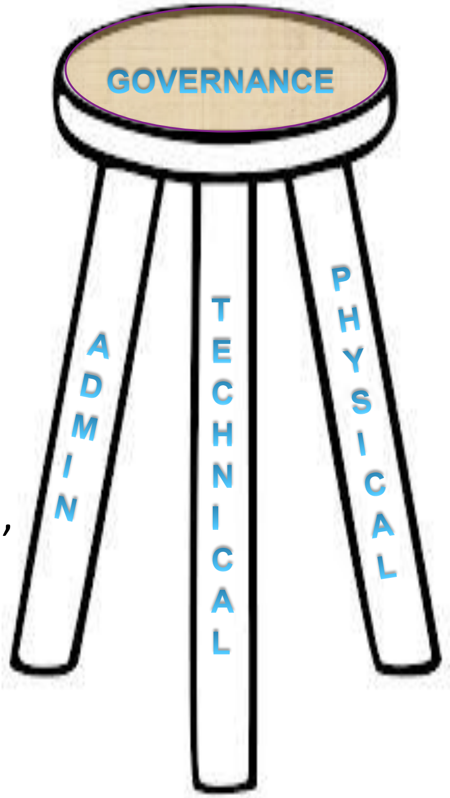
ISO 27001, NIST CyberSecurity Framework, Top 20 CSC and other industry standards

International (i.e. EUPD), state laws and regulations

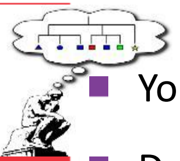
Governance, Risk and Compliance (GRC)

- GOVERNANCE is based on Administrative, Technical & Physical Safeguards
- What Your Company is EXPECTED to understand:
  - Data they collect
  - Where the Data is kept
  - How it is being used, and
  - With Whom is it Shared
  - Obligations to keep such information secure AND ensure employees, third parties, and contractors are educated to do the same
  - Obligations to mitigate harms and respond appropriately to all security incidents
- Functions are about MORE than RISK avoidance; its about creating a culture of privacy COMPLIANCE

Step #1:
Data Classification



Data Classification & Data Mapping



#1 Step of any GRC Program

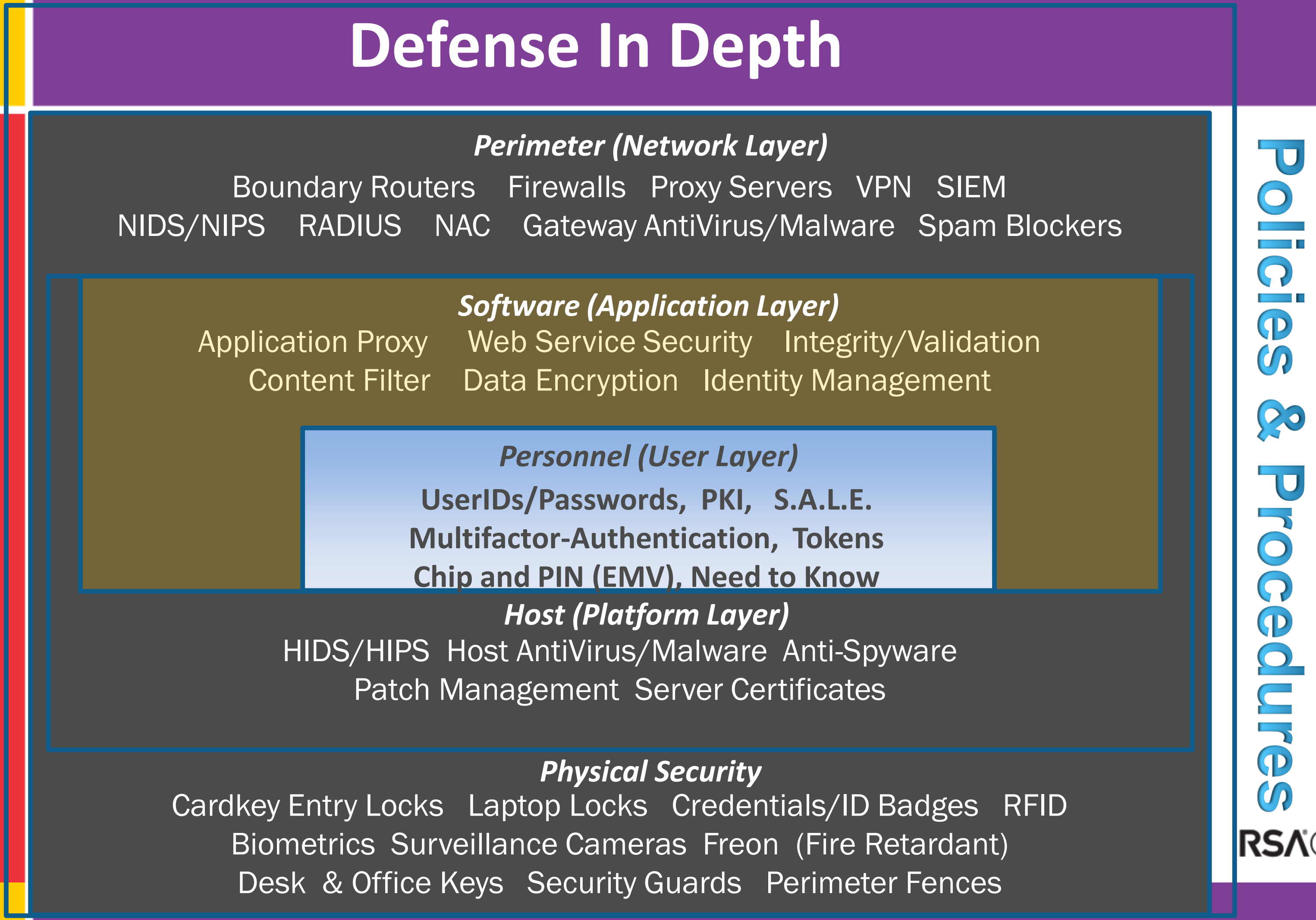
- You cannot govern what you do not understand
- Define the data in external terms
  - Personally identifiable information ("PII")
  - Protected health information ("PHI") ("HIPAA")
  - Nonpublic personal information ("NPI") ("GLBA")
- Define the data according to internal standard
  - High, medium and low risk
  - Level I, II & III
  - Confidential, Public & Proprietary

- You cannot safeguard what you cannot locate
- Map existing locations where PII/NPI/PHI is stored
  - Technical locations: databases, servers and systems
  - Physical locations: office, floor and office buildings
  - Don’t forget the "cloud"
- Map of existing data flows
  - Internal: between locations
  - External: from internal locations to external locations
- Map of existing applications
  - Internal: what functions and what data
  - External (including cloud): what functions and what data

Administrative Safeguards

- Drafting policies (the "why")
- Drafting procedures (the "how")
- Educate on policies and procedures
  - Regularly scheduled training sessions
    - Assessments
    - Evaluation of competency
  - Awareness program (there is a difference)
- Programs with Documented Plans
  - Incident Response Plan with Data Breach Response
  - Business Continuity Plan
  - Security Awareness and Learning/Training Plan

Defense In Depth



Perimeter (Network Layer)

Boundary Routers Firewalls Proxy Servers VPN SIEM
NIDS/NIPS RADIUS NAC Gateway AntiVirus/Malware Spam Blockers

Software (Application Layer)

Application Proxy Web Service Security Integrity/Validation
Content Filter Data Encryption Identity Management

Personnel (User Layer)

UserIDs/Passwords, PKI, S.A.L.E.
Multifactor-Authentication, Tokens
Chip and PIN (EMV), Need to Know

Host (Platform Layer)

HIDS/HIPS Host AntiVirus/Malware Anti-Spyware
Patch Management Server Certificates

Physical Security

Cardkey Entry Locks Laptop Locks Credentials/ID Badges RFID
Biometrics Surveillance Cameras Freon (Fire Retardant)
Desk & Office Keys Security Guards Perimeter Fences

Policies & Procedures

Tensions in Data Governance

Security	vs.	Privacy
Obligation to provide security for personal information and other confidential material		Rules for processing Personal Information (and analogs outside the EU)
Quick response to attacks and changing strategies		Requirements to obtain user consent and register applications/processing
Need to retain log and traffic data for analysis		Restrictions on data retention
Need to consolidate data for analysis		Export limitations on "personal data," banking information and "state secrets"

IT Operational Business Needs

Obligation to keep systems available/operational SLAs
Customer experience Time to market Expense Concerns
Technology needs Retain everything
Competitive pressures Internal Deadlines for Project Implementations

Data Governance

- Finding a balance between:
  - Technology
  - Operations
  - Data use and needs
  - Security
  - Authority
  - Accountability
  - Privacy

Resolution of Competing Interests

Who Decides?

- Business
- IT
- CISO
- CEO

How is the risk captured?

- Reserve
- Cyber Insurance

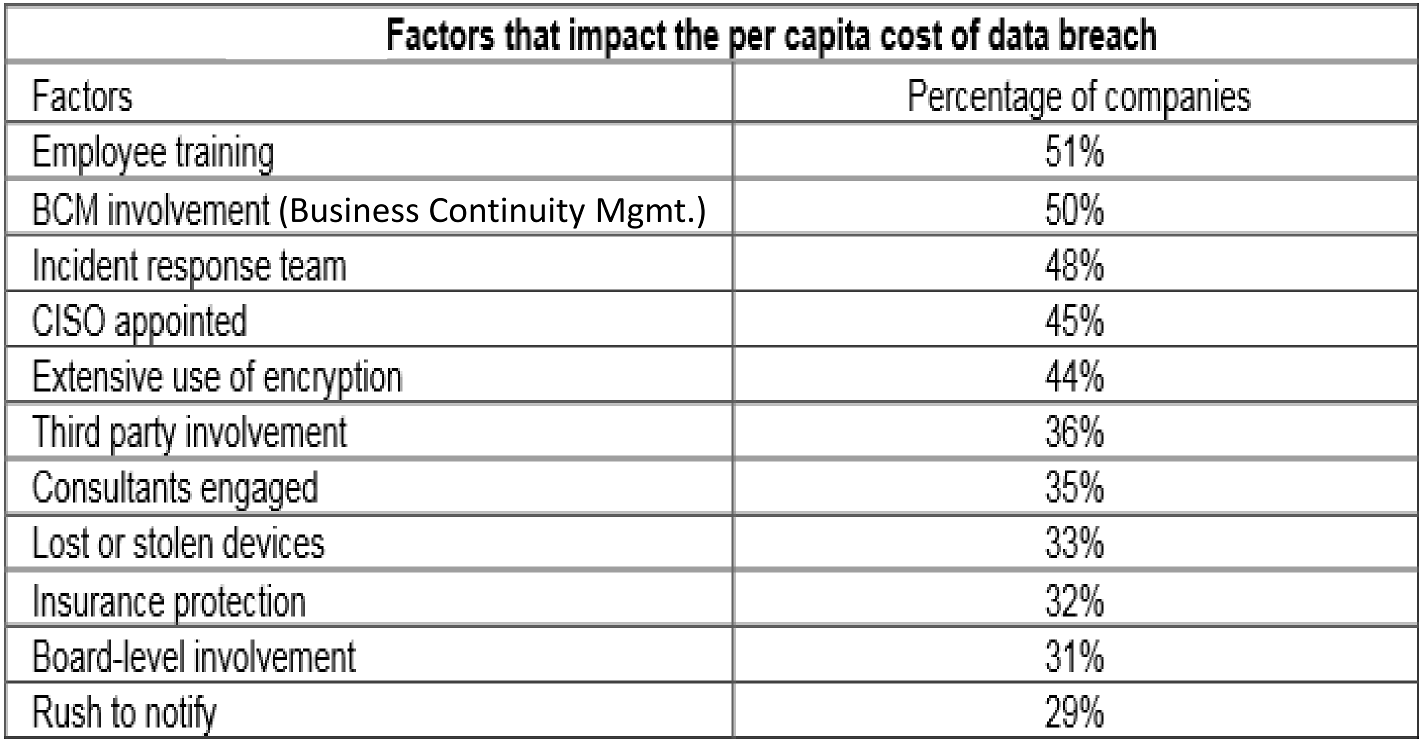
Reconsider Skills and Role of CISO

Compliance: Documentation of the CISO Process

- Project Management
  - Initial Risk Assessment
  - Identification of NPI/PII/PHI
  - Identify external access to data onsite
  - Identify encryption utilized
  - Identify remote access requirements
  - CyberSecurity Insurance Assessment
  - Third party contracts
  - Incident Response Plan execution
- Process
  - Timing of decisions
  - Threat timeline
  - Results
- Documentation

Finding a Home for an Unsolicited Proposal
Experiment or theory/computation?
theory
Theory development?
yes
Theory, Models and Computational Methods
experiment
both
no
Measurement/instrumentation/data analysis?
yes
Chemical Measurement and Imaging
no
Environment?
no
Biology/Biochemistry?
no
Catalysis?
no
Nano/Supra/Macro?
no
yes
yes
yes
yes
Environmental Chemical Sciences
Chemistry of Life Processes
Chemical Catalysis
Macromolecular, Supramolecular and Nanochemistry
Is the focus on synthesis?
yes
Chemical Synthesis
no
Dynamics, mechanism, or structure?
yes
Chemical Structure, Dynamics and Mechanisms
no
Contact a Program Director!

Food For Thought....



Factors that impact the per capita cost of data breach	
Factors	Percentage of companies
Employee training	51%
BCM involvement (Business Continuity Mgmt.)	50%
Incident response team	48%
CISO appointed	45%
Extensive use of encryption	44%
Third party involvement	36%
Consultants engaged	35%
Lost or stolen devices	33%
Insurance protection	32%
Board-level involvement	31%
Rush to notify	29%

Many of the factors we suggest based on practice, are supported by statistics, for decreasing the data breach financial impact.

Source: 2015 Ponemon Data Breach Research

TROUTMAN SANDERS

A. HOY & ASSOCIATES

Source: 2015 Ponemon Research Study

So To Be Better Prepared for Data Breach Litigation…. Top 10 Steps

1. Educate your users on Security and Privacy Responsibilities

   Signed User Agreements

   Signed Contractor 3rd Party User Agreements

2. Involve your Business Continuity team
3. Identify and have an exercised Incident Response Team
4. Appoint / Hire a CISO who has responsibilities
5. Exercise consistent Data Classification and then Encrypt Sensitive information

   Don’t forget Laptops, Tablets, and Mobile Device Encryption

6. Execute signed 3rd Party Agreement Services in advance
   a. IR team
   b. Data Breach Coach
   c. Crisis Mgmt PR team
7. Reporting and Handling of Lost or Stolen Devices
8. Invest in a CyberSecurity Policy..or two
9. Educate the Board prior to the Event and Involve them after
10. Remember tips on Notification

TROUTMAN SANDERS

A. HOY & ASSOCIATES

Questions on Data Breach Litigation and Being Prepared?

Ronald I. Raether, Jr.
Ronald.Raether@troutmansanders.com
(949) 622-2722

Andrea C.Hoy CISSP, CISM, MBA
ahoy (at) securIT.us or ahoy (at) ISSA.org
(949) 606-5333 office

RSAConference2016

TROUTMAN SANDERS

A. HOY & ASSOCIATES

Ronald I. Raether, Jr.

Partner

Ron Raether is a partner in the Cybersecurity, Information Governance and Privacy, and Financial Services Litigation practices at Troutman Sanders. Ron is known as the interpreter between the business and information technology, guiding both parties to the best result. In this role, Ron has assisted companies in navigating federal and state privacy laws for almost twenty years. Ron's experience with technology-related issues, including data security, patent, antitrust, and licensing and contracts, helps bring a fresh and creative perspective to novel data compliance issues. Ron has been involved in seminal data compliance cases, assisting one of the first companies required to provide notice of a data breach and successfully defending companies in over 50 class actions. Ron also has represented companies in over 200 individual FCRA cases involving CRAs, resellers, furnishers, users, and public record vendors. Ron has developed a reputation for assisting companies not traditionally viewed as subject to the FCRA or with FCRA compliance questions where the law remains uncertain or unresolved.

Ron not only works with companies which have experienced unauthorized access to consumer data or have been named defendants in class actions and before regulators, but also has advised companies in developing compliance programs to proactively address these issues. As a thought leader, Ron speaks nationally and publishes frequently on cutting-edge compliance issues. Ron is also a Certified Information Privacy Professional.

Firm Highlights

- "And in the most dramatic shift, Troutman Sanders, which ranked No. 53 in last year's survey, jumped to the No. 3 spot, having handled 87 district court cases in 2014, according to the survey...." – *Corporate Counsel's 2015 Patent Litigation Survey*.

- Troutman Sanders ranked nationally in 39 practice areas in the 2016 edition of *U.S. News – Best Lawyers* "Best Law Firms."

- 40 Troutman Sanders litigators have been highlighted in the most recent issues of *Chambers USA* or *Chambers Global*.

- Clients rank Troutman Sanders in the top 5% of firms for class actions, according to BTI Litigation Outlook 2016, and the 2015 *U.S. News – Best Law Firms* rates the firm as Tier 1 in the nation for Class Action Defense.

- Troutman Sanders was mentioned in a June 24 *Law360* *article* about 25 law firms that general counsels recommend to their friends as reported in The BTI Consulting Group's 2015 *Most Recommended Law Firms* report.

Andrea C. Hoy, CISSP, CISM, MBA

Andrea Hoy, received her initiation into the infosec community when her hard work and dedication for a safe international event earned her the role as an Asst. Venue Manager for the highly successful LA Summer Olympic Games. Andrea’s leadership positions include McDonnell Douglas, Rockwell, Boeing NA and Fluor. Her clients are from a diverse mix of industries that include Litton, Pacific Life, Genentech, Molina Healthcare, Activision, WAMU (now Chase), Hamni, and East West Banks. She’s served and been recognized as an advisor to the Pentagon and as ISO for the 5th largest credit union as it went through its most major technology and growth past $10 billion in assets and 600,000 in membership.

Ms. Hoy is the founder of A.Hoy & Associates, a “virtual CISO” provider as well as infosecurity consulting, GRC, incident response, CISO Bootcamp training firm, assisting companies to establish policies and procedures to comply with NIST CyberSecurity Framework, top 20 Critical Controls, EUPD and privacy laws here and abroad to name a few.   She represented the US as diplomat to China on eDiscovery and forensics.

Andrea is actively involved in the community serving as the International President of the Information Systems Security Association (ISSA) the commun ity of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information, after elected Vice President. ISSA members represent >10,000 security professionals worldwide with 137 chapters in 71 countries. Ms. Hoy cofounded the CISO Executive Forum and recently chartered the Financial SIG.

She previously served on the Technical Advisory Board for RSA for 4 years, advised the International Board of Directors for PointSec/ProtectData of Sweden, as well as Board of Advisors for Encentuate, a global identity management and provisioning company, leading to its acquisition by IBM, and DigitalSafe in Switzerland. She has previously been in the LA Times, Orange County Register: People in Technology to Watch”, MiCTa Radio, TechTarget and KNX News Radio. Andrea received her MBA from Pepperdine University in Malibu, and prior to that graduated Magna Cum Laude and was entered into the honor society of Beta Gamma Sigma, the Phi Beta Kappa of the School of Business.

TROUTMAN SANDERS

A. HOY & ASSOCIATES