RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-W02

Data Breach or Disclosure: A Quantitative Risk Analysis

Evan Wheeler

VP, Risk Management & CISO
Edelman Financial Engines

Risk Management Goals

- **Minimizing uncertainties** for the business
- Aligning and controlling organizational components to produce the maximum output
- **Improve decision-making** and planning
- Providing governance and oversight
- Operating in a cost effective manner

Business Landscape

Brand Recognition Increasing

Customer-base growing rapidly

Manual processes aren't scalable

Competitive pricing pressures

Client data theft

Client data "screw up"

- Intellectual Property
- Misconfiguration
- 3rd Party Data Leakage
- Certificates
- DDoS
- Disgruntled Employee
- Brand Misuse
- Brute Force
- Cross Site Scripting (XSS)
- Ransomware
- Impersonating Mobile App
- Customer Details Leakage
- Compromised Credentials
- Internal Marked Documents
- Phishing
- Impersonating Executives
- Typo Squatting
- Unintentional Info Disclosure
- Defamation
- Social Media Leakage
- Open Ports
- Hacktivist

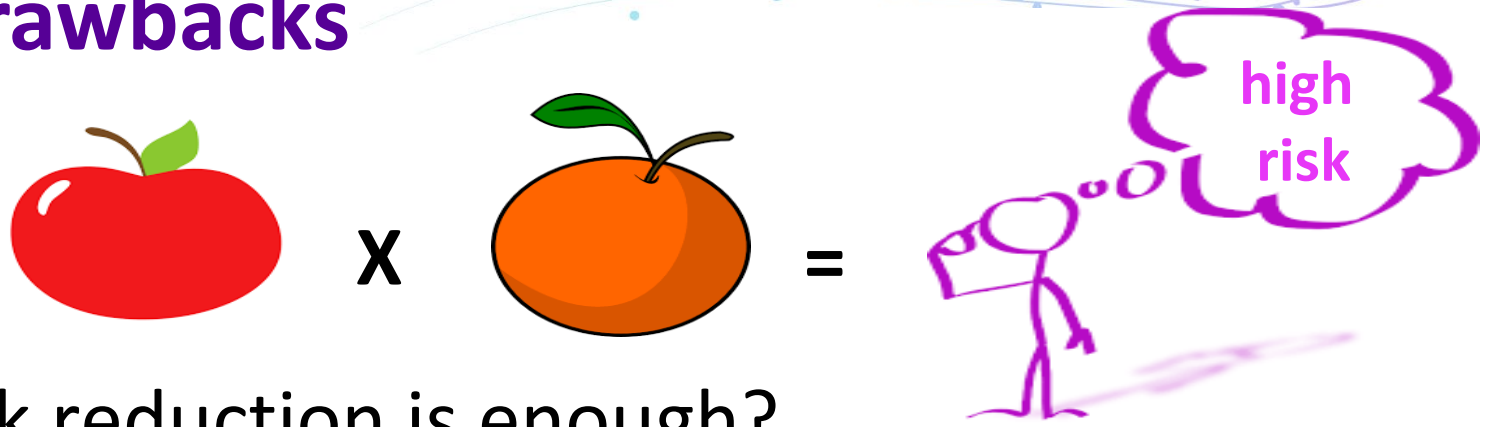
NIST Risk Matrix

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

1. Client data theft
2. Accidental client data disclosure

Qualitative Drawbacks



- How much risk reduction is enough?
- Where are the opportunities to reduce our exposure?
- How to compare one-time events with recurring?
- What is the time horizon for our outlook and estimates? Next 3 months, next 10 years?
- How many ‘Lows’ equals a ‘High’ rating?

Quantitative Assumptions

Won't our SMEs just be guessing?

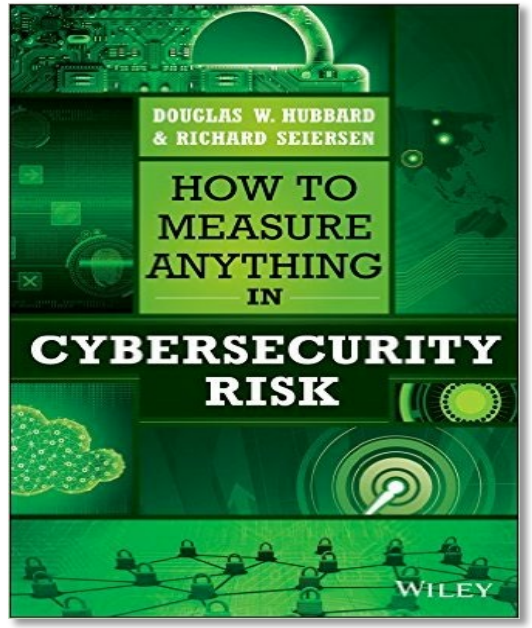
We don't have enough data …

How can we estimate when it has never happened before?

But we are a unique snowflake!

Objections to quantitative measurement models

1. Your problem is not as unique as you think.
2. You have more data than you think.
3. You need less data than you think.
4. There is a useful measurement that is much simpler than you think.



Scenario Analysis Approach

0. Prerequisite	✓ ***Conduct calibration exercise to ensure your stakeholders are comfortable with estimates***	**Prep Meeting Sections**
1. Identify scenario scope	✓ ***Identify the asset at risk*** ✓ ***Identify the threat community under consideration***	
2. Evaluate Loss Event Frequency	✓ ***Estimate the Probable Frequency*** *(Results will drive Preventative Controls)*	**Workshop Sections**
3. Evaluate Loss Magnitude	✓ ***Estimate the Forms of Loss for probable impact*** *(Results will drive Detective and Response Controls)*	
4. Derive & articulate Risk	✓ ***Determine the risk and capture results in standard format*** ✓ ***Post-Scenario Steps***	**Post Workshop Section**

RSAConference2019

Data Breach Case Study

Widget & Co.

- We sell widgets
- Business processes are: sourcing materials, manufacturing, distribution, and marketing of widgets

Widget & Co.

- We have 10,000 client mailing addresses for shipping purposes, and payment details for billing purposes
- Private company, family owned
- Revenue of ~ $100M annually
- About 900 – 1,000 staff including contractors/consultants

Scenario Assumptions

- Approximately 10,000 client records in distribution and billing systems
- All operations and clients are only in the U.S.
- Clients are generally retail consumers, and some are small business owners
- Mailing addresses and payment details are easily monetizable
- Payment details may include bank account numbers and/or credit cards
- Client data has never been stolen before (best of our knowledge)
- Client turnover (loss of future business) has been minimal from previous data sharing errors
- Not all impacted clients will use the offered credit monitoring service
- No current insurance coverage

Choosing a Scenario - Accidental Disclosure

- Employee leaves client document on the commuter train
-  Client data emailed to the wrong client
- Misconfigured AWS storage reveals client database to Internet
- Unencrypted client data on a USB stick is lost outside office
- Client form is lost in the mail
- …

Choosing a Scenario – Data Theft

External Hacking results in the most server confidentiality breaches

Common attack scenarios

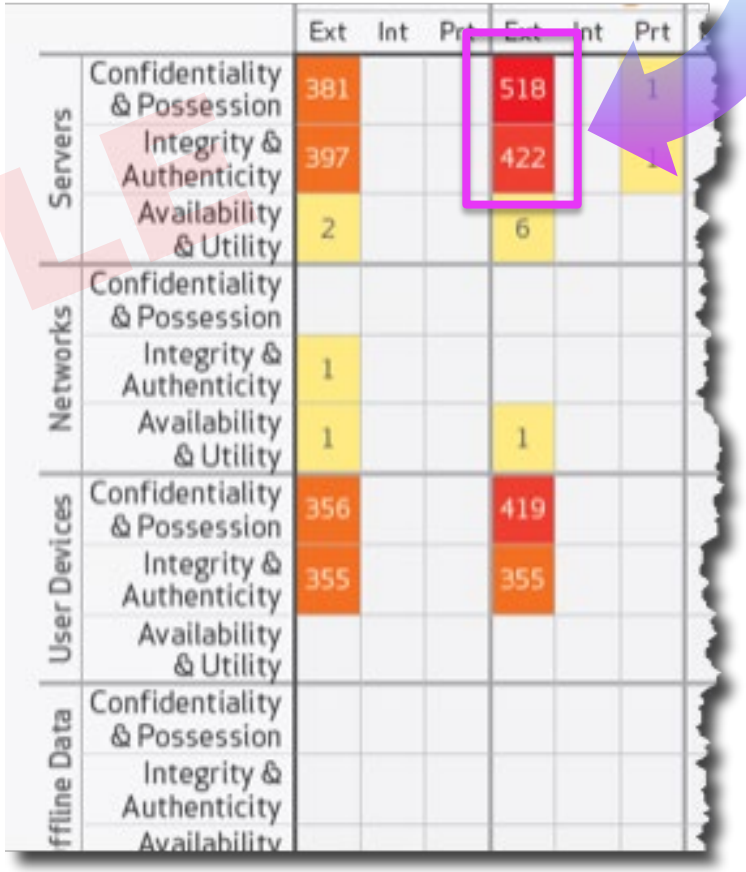
Appendix B: Attack Types

As described in the Introduction, numerous contributors who are responsible for responding to actual attacks or conducting red team exercises were involved in the creation of this document. The resulting Critical Controls are therefore based on first-hand knowledge of real-world attacks and the associated defenses.

Attack Summary	Most Directly Related Critical Control
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	1
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines.	2, 3
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.	2, 4
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.	2, 10
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.	3, 10
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.	4, 5

SANS Critical Controls for Effective Cyber Defense

Data breach threats



Verizon DBIR

Employee accidentally sends sensitive client data to the wrong client

Asset at Risk	Ad hoc process for client support to send confirmation email to clients including address and full payment details
Threat Community	☑ **Privileged Insider** ☒ Amateur Hacker ☒ Cyber Criminal ☒ Nation State ☒ Act of Nature
Motivation	☒ Malicious ☑ **Accidental**
Impact Area	☑ **Confidentiality** ☒ Integrity ☒ Availability
Forms of Loss	☒ Productivity Response ☒ **Response** ☒ Replacement ☑ **Fines & Judgments** ☒ Competitive Advantage / Reputation

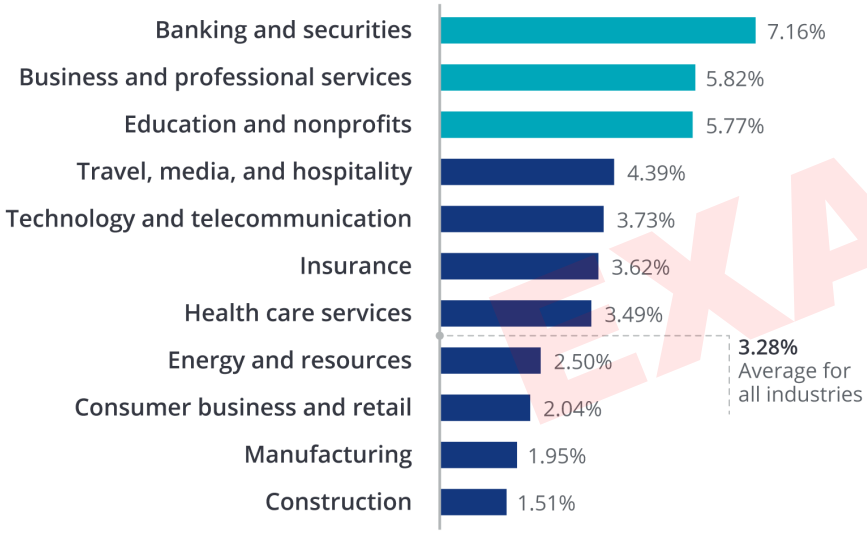
Cyber criminal exploits default password on production server to gain access to the client database, and sells data on black market

Asset at Risk	Mailing addresses and payment details for 10,000 clients in billing database
Threat Community	☒ Privileged Insider ☒ Amateur Hacker ☑ **Cyber Criminal** ☒ Nation State ☒ Act of Nature
Motivation	☑ **Malicious** ☒ Accidental
Impact Area	☑ **Confidentiality** ☒ Integrity ☒ Availability
Forms of Loss	☒ Productivity ☑ **Response** ☒ Replacement ☑ **Fines & Judgments** ☒ Competitive Advantage / Reputation

How much are we spending on security?

IT budget as percentage of revenue

Figure 1. IT budget as a percentage of revenue

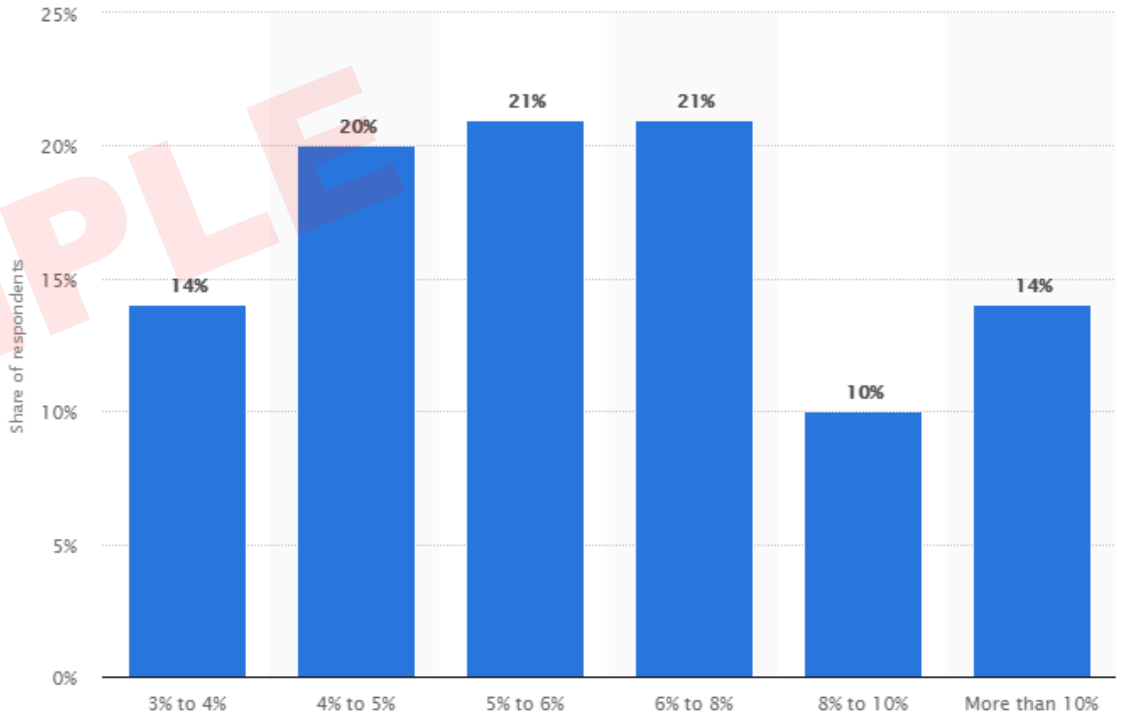


Source: Deloitte 2016–2017 Global CIO Survey, N=747.

Deloitte Insights | deloitte.com/insights

average is 3.28%

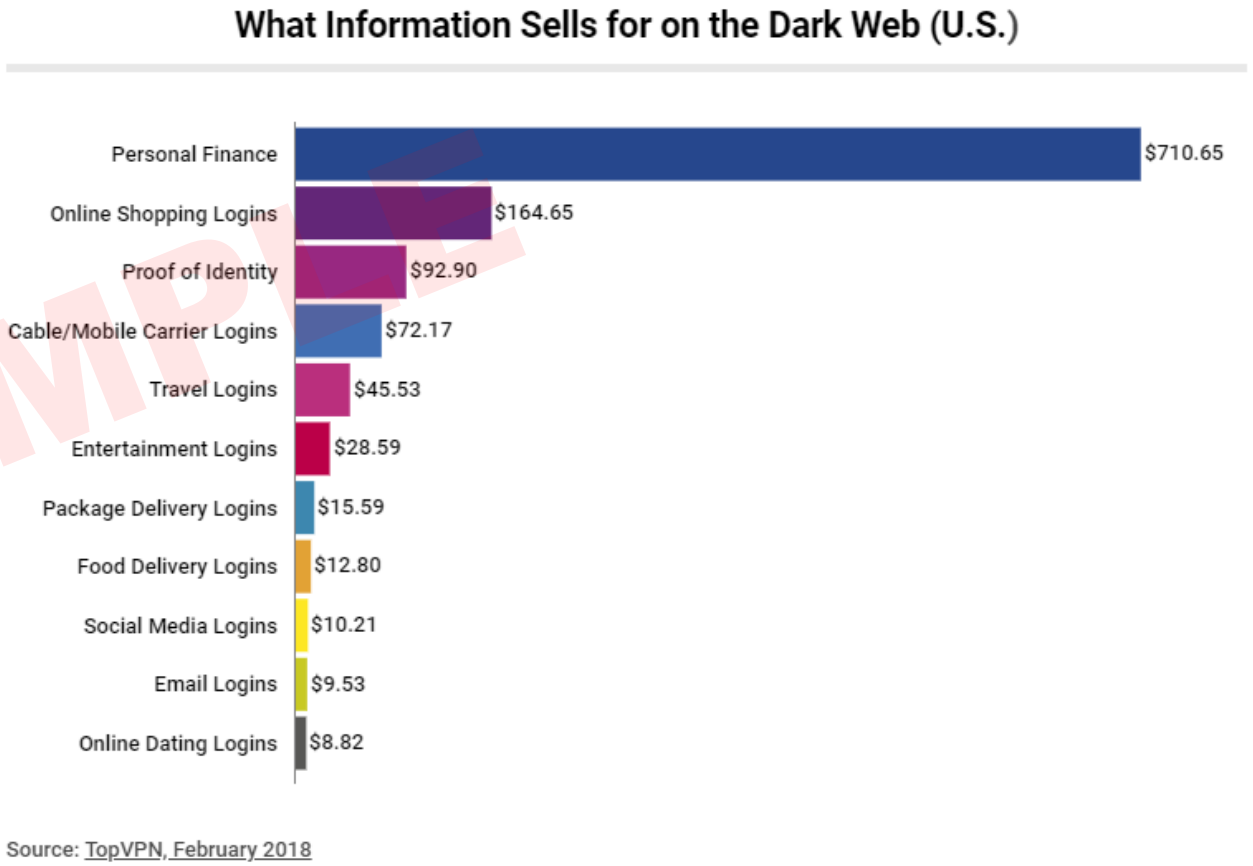
Cyber security budget as percentage of annual IT budget



© Statista 2019

majority is 4% - 8%

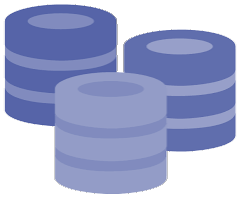
What am I worth on the dark web?



worth $5 - $15 per record

1 Estimate the Frequency

$100M
annual revenue



10k client records **&** **$130k** annual security budget

W&C

VS.

$50k – $150k
potential profit for cyber criminal

1 Estimate the Frequency

Qualitative Values	Description
Very High	Adversary is **almost certain** to initiate the threat event.
High	Adversary is **highly likely** to initiate the threat event.
Moderate	Adversary is **somewhat likely** to initiate the treat event.
Low	Adversary is **unlikely** to initiate the threat event.
Very Low	Adversary is **highly unlikely** to initiate the threat event.

NIST Special Publication 800-30 Revision 1, Table G-2

Minimum	Most Likely	Maximum
0.1	0.3	2

Confidence: Medium

Qualitative Values	Description
Very High	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

NIST Special Publication 800-30 Revision 1 , Table G-3

Minimum	Most Likely	Maximum
10	12	100

Confidence: High

2 Estimate the Magnitude

Data Theft

- **Productivity** – Operations may be disrupted during the investigation
- **Response** – Significant support needed from external forensic consultants, outside counsel, and PR firm. Offer free credit monitoring to clients
- **F&J** – Potential client lawsuits, state privacy and PCI fines
- **Reputation** – Mostly consumer clients, but one large corporate client is a household name

Accidental Disclosure

- **Productivity** – Negligible
- **Response** – Procedure to handle these cases is operationalized and resources are minimal. Offer free credit monitoring to impacted client
- **F&J** – Client contract caps damages at $1k per event, PCI fines less likely
- **Reputation** – Difficult for clients to switch to a competitor

2 Estimate the Magnitude

Potential Costs

- Forensics
- Legal Advice
- Notification Costs
- Call Center
- Credit Monitoring
- Public Relations
- Data Replacement
- Cyber Extortion
- Customer Suits
- PCI-DSS Fines
- Regulatory Defense, Fines, a… Penalties

Reference Loss Table - Credit Monitoring

Consumers	Range Included	Min	M/L	Max
1	(1-9)	$ -	$ -	$ 25
10	(10-99)	$ -	$ 36	$ 200
100	(100-999)	$ 10	$ 306	$ 2,000
1,000	(1,000-9,999)	$ 100	$ 2,970	$ 20,000
10,000	**(10,000-999,999)**	**$ 1,000**	**$ 29,700**	**$ 200,000**
100,000	(100,000-999,999)	$ 10,000	$ 297,000	$ 2,000,000
1,000,000	(1,000,000-9,999,999)	$ 100,000	$ 2,970,000	$ 20,000,000
10,000,000	(10,000,000-999,999,999)	$ 1,000,000	$ 29,700,000	$ 200,000,000
100,000,000	= and > than 100,000,000	$ 10,000,000	$ 108,000,000	$ 600,000,000

"You'll hear talk of PCI compliance fines, and those fines can range from **$5,000 to $100,000** a month, depending on factors like the size of your business and the length and degree of your non-compliance." Oct 11, 2017

2 Estimate the Magnitude

Qualitative Values	Description
Very High	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

NIST Special Publication 800-30 Revision 1, Table H-3

Response

Minimum	Most Likely	Maximum
$1,000	$30,000	$200,000

Confidence: Medium

Fines & Judgments

Minimum	Most Likely	Maximum
0%	50%	98%

Confidence	Minimum	Most Likely	Maximum
Low	$0	$5,000	$100,000

Confidence: Medium

Response

Minimum	Most Likely	Maximum
$0	$100	$1,000

Confidence: High

Fines & Judgments

Minimum	Most Likely	Maximum
0%	10%	50%

Confidence	Minimum	Most Likely	Maximum
Medium	$0	$5,000	$100,000

Confidence: Low

Data Theft

$0	$34.9k	$318.4k
Minimum	Average	Maximum

Primary

	Min	Avg	Max
Loss Events / Year	0	0.56	2
Loss Magnitude	$1.0k	$53.3k	$179.2k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0.27	2
Loss Magnitude	$3	$19.9k	$88.7k

Single Loss Max: $270k
Annualized: $320k

Accidental Disclosure

$63	$111.4k	$1.6M
Minimum	Average	Maximum

Primary

	Min	Avg	Max
Loss Events / Year	10	20.64	69
Loss Magnitude	$1	$181	$799

Secondary

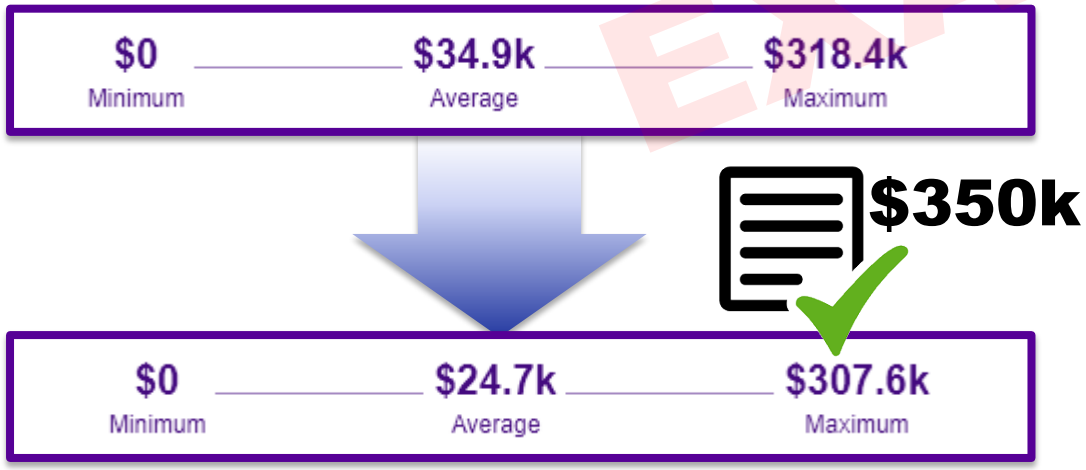
	Min	Avg	Max
Loss Events / Year	0	3.09	23
Loss Magnitude	$8	$34.9k	$99.5k

Single Loss Max: $100k
Annualized: $1.6M

Risk Treatment

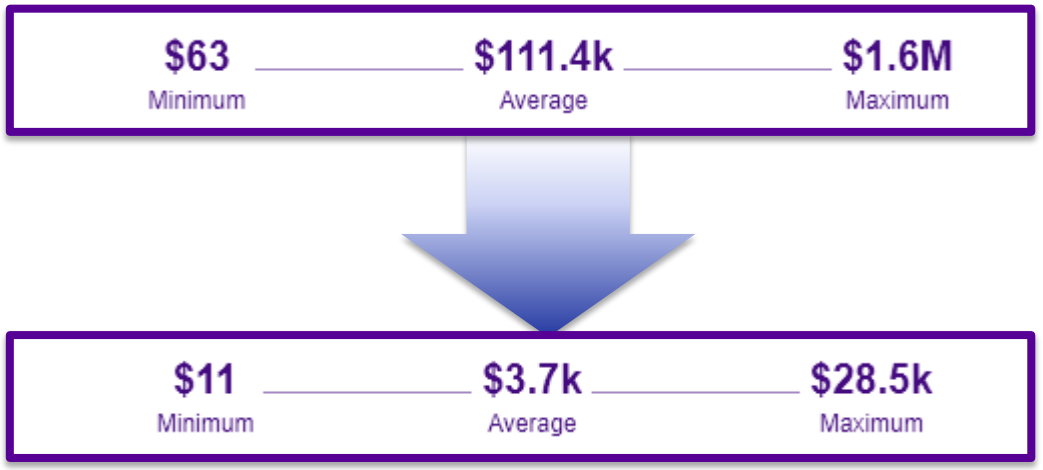
Data Theft

- Improve detection, containment, and response capability
- Purchase cyber insurance coverage



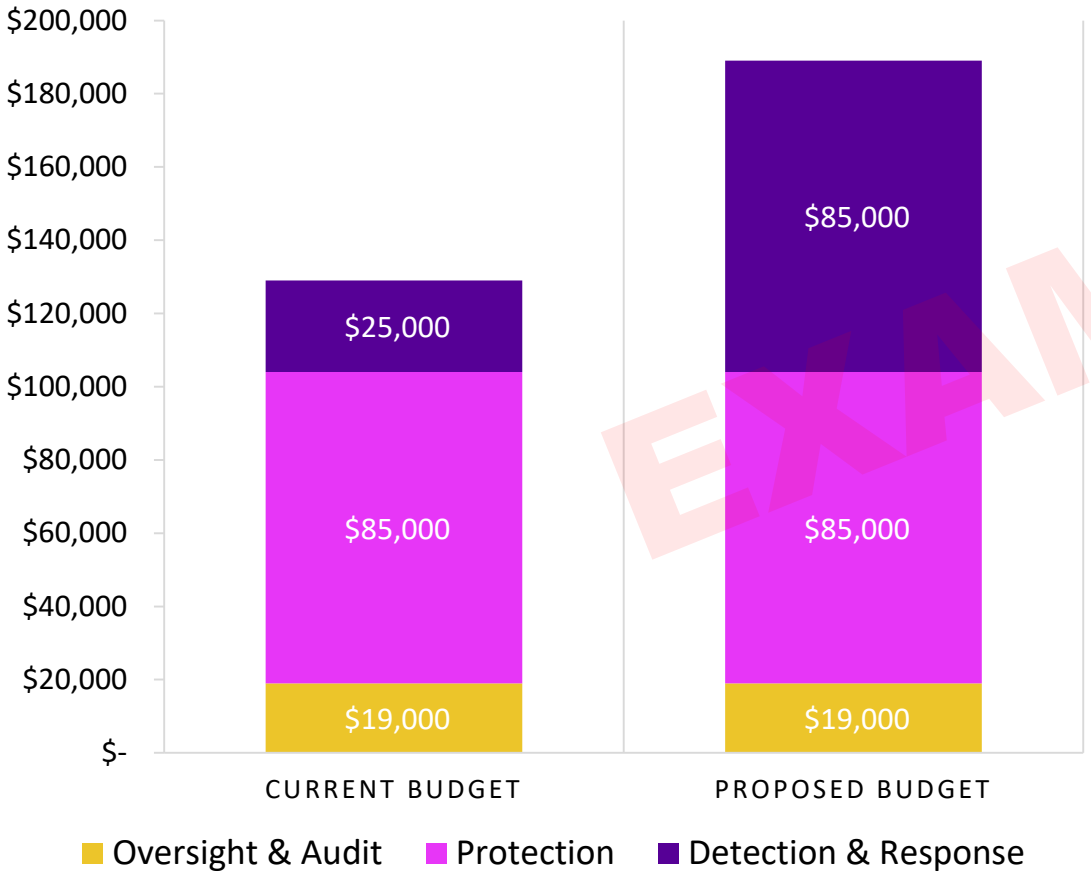
Accidental Disclosure

- Remove credit card information from the confirmation emails
- Invest in process improvements on emails going to clients

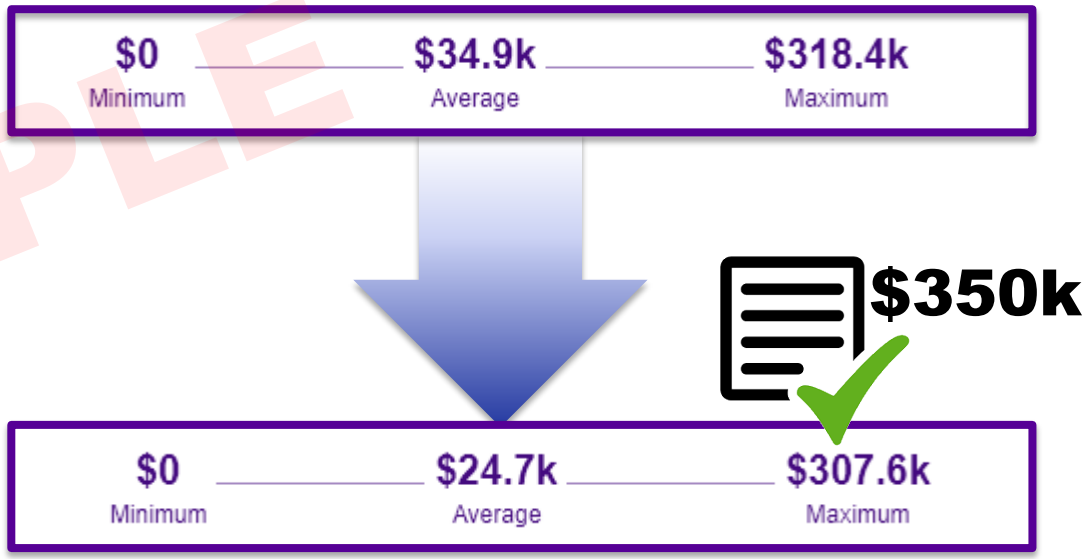


Trade-Offs - Data Theft

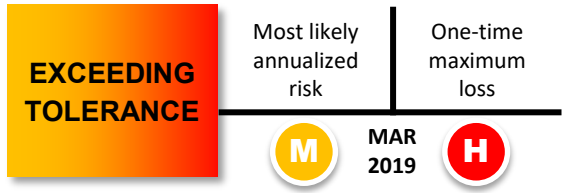
Investment Cost



Risk Reduction



Sample On-Going Reporting



Scenario Scope	
Threats	▪ Cyber Criminals ▪ Privileged Insiders
Motivation	▪ Accidental ▪ Financial Gain ▪ Embarrassment
Loss Area	▪ Confidentiality
Targets	▪ client PII ▪ credit card data ▪ corporate emails

Q2 2019 Progress

Scenario Exercises Run	2
Action Items	4
Projects	2
Risk Acceptances	1
SEV 1/2 Incidents	3

Action Plan Outlook: MAR 2019 – FEB 2020

Inadvertent or malicious disclosure of sensitive data

Sensitive data could be exposed to an unauthorized party through an error, or by an intentionally act of a malicious party. The cost of such as event is most driven by the type of data and number of records exposed. Generally, privileged insiders will disclose fewer records, whereas cyber criminals target large volumes of data to steal.

Although generally doesn't process a lot of data that would be attractive to cyber criminals or easy monetize, there are business lines that receive personally identifiable and heath information ancillary to the service. Other businesses such regularly process such data.

Most common accidental data disclosures are due to manual processing errors, and less often software coding defects.

Typical breach points for cyber criminals would be phishing campaigns, malware infected websites, and compromising application vulnerabilities.

Key Findings

- Several businesses regularly exchange sensitive data with clients via email
- Lacking peer review on billing confirmation emails sent to clients
- Breach response procedures have never been tested
- Monitoring gaps exist on the distribution servers

Recent Developments

+ Added four-eyes check on billing confirmation emails to clients
+ Confirmed insurance policy covers most of the notification and investigation cost
- Identified further gaps in tools and technologies to prevent confidentiality issues
- Project to remove credit card details from billing confirmation emails has been delayed

Further Research Needed

- Are consumers more forgiving of a data breach than an accidental disclosure?
- Do external attackers tend to steal higher volume of records than insiders?
- How attractive is a database of consumer mailing addresses for a cyber criminal?
- How monetizable is a list of client bank account numbers?
- How might new privacy laws like CCPA change the loss estimates?

RSAConference2019

Program Implementation

Initial Methodology Rollout

Benefits

Defensible

- The scope of an analysis is clearly defined
- Terminology and relationships between factors are pre-established, and not subject to different mental models
- Assumptions are explicit and open to discussion/debate

Supports Decision-Making

- Probability is taken into account and forecast timeframe is explicit
- Scenarios can be aggregated and compared
- Promotes meaningful metrics and supports tolerance thresholds

Extensible

- Designed for incremental integration
- Modularity to grow in line with risk program maturity lifecycle

Program Challenges

Scoping and measurement

- SMEs aren't used to formally documenting their assumptions
- Not comfortable with estimations of impact and frequency
- Hesitation to commit to predefined impact table thresholds

Different mental risk models

- Resistant to change
- Clouded by historical failed models
- Rarely data driven

Next Steps

- Run two scenarios using free FAIR tools
  - Analyze incidents and public data
  - Determine initial impact and frequency ranges
  - Analyze scenarios in parallel with existing model
  - Recalibrate and refine ranges
  - Identify opportunities to gather more data
  - Run sensitivity analysis on alternatives
- Train analysts
- Evangelize benefits of new methodology

FAIR
POWERED BY RISKLENS

THE Open GROUP

Resources to Get Started

Cybersecurity Research Library

- Building a scientific basis for the cybersecurity decisions
- Library of over 65 data sources

Questions?

Measuring and Managing Information Risk: A FAIR Approach

- ISBN: 978-0124202313
- Amazon Link: http://amzn.com/0124202314