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
Client data theft

"screw up"

Manual processes aren’t scalable

Competitive pricing pressures

Customer-base growing rapidly

Brand Recognition Increasing

Business Landscape

- Client data theft
- Manual processes aren’t scalable
- Competitive pricing pressures
- Customer-base growing rapidly
- Brand Recognition Increasing

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

- Client data theft

- "screw up"

- "OOOPS!"

- Manual processes aren’t scalable

- Competitive pricing pressures

- Customer-base growing rapidly

- Brand Recognition Increasing

- "OOOPS!"

- "screw up"

- "OOOPS!"

- "screw up"

- "OOOPS!"

- "screw up"
# NIST Risk Matrix

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

<table>
<thead>
<tr>
<th>Likelihood (Threat Event Occurs and Results in Adverse Impact)</th>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Moderate</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

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

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.

Objections to quantitative measurement models

- 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!
Scenario Analysis Approach

0. Prerequisite
- Conduct calibration exercise to ensure your stakeholders are comfortable with estimates

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)

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
Data Breach Case Study

Widget & Co.
We sell widgets

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

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

Common attack scenarios

Data breach threats

External Hacking results in the most severe confidentiality breaches

SANS Critical Controls for Effective Cyber Defense

Verizon DBIR
**Employee accidentally sends sensitive client data to the wrong client**

<table>
<thead>
<tr>
<th>Asset at Risk</th>
<th>Ad hoc process for client support to send confirmation email to clients including address and full payment details</th>
</tr>
</thead>
</table>
| 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**

<table>
<thead>
<tr>
<th>Asset at Risk</th>
<th>Mailing addresses and payment details for 10,000 clients in billing database</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking and securities</td>
<td>7.16%</td>
</tr>
<tr>
<td>Business and professional services</td>
<td>5.82%</td>
</tr>
<tr>
<td>Education and nonprofits</td>
<td>5.77%</td>
</tr>
<tr>
<td>Travel, media, and hospitality</td>
<td>4.39%</td>
</tr>
<tr>
<td>Technology and telecommunication</td>
<td>3.73%</td>
</tr>
<tr>
<td>Insurance</td>
<td>3.62%</td>
</tr>
<tr>
<td>Health care services</td>
<td>3.49%</td>
</tr>
<tr>
<td>Energy and resources</td>
<td>2.50%</td>
</tr>
<tr>
<td>Consumer business and retail</td>
<td>2.04%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1.95%</td>
</tr>
<tr>
<td>Construction</td>
<td>1.51%</td>
</tr>
</tbody>
</table>


Average is 3.28%

Cyber security budget as percentage of annual IT budget

- Majority is 4% - 8%
- Average for all industries is 3.28%
What am I worth on the dark web?

- Worth $5 - $15 per record

What Information Sells for on the Dark Web (U.S.)

- Personal Finance: $710.65
- Online Shopping Logins: $164.65
- Proof of Identity: $92.90
- Cable/Mobile Carrier Logins: $72.17
- Travel Logins: $45.53
- Entertainment Logins: $28.59
- Package Delivery Logins: $15.59
- Food Delivery Logins: $12.80
- Social Media Logins: $10.21
- Email Logins: $9.53
- Online Dating Logins: $8.82

Source: TopVPN, February 2018
Estimate the Frequency

W&C

\$100M

annual revenue

10k & \$130k

client records & annual security budget

VS.

\$50k – \$150k

potential profit for cyber criminal

\$130k

annual security budget

10k client records

\$100M annual revenue

\$100M

\$50k – \$150k

potential profit for cyber criminal
### Estimated Frequency

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

<table>
<thead>
<tr>
<th>Qualitative Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Adversary is <strong>almost certain</strong> to initiate the threat event.</td>
</tr>
<tr>
<td>High</td>
<td>Adversary is <strong>highly likely</strong> to initiate the threat event.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Adversary is <strong>somewhat likely</strong> to initiate the threat event.</td>
</tr>
<tr>
<td>Low</td>
<td>Adversary is <strong>unlikely</strong> to initiate the threat event.</td>
</tr>
<tr>
<td>Very Low</td>
<td>Adversary is <strong>highly unlikely</strong> to initiate the threat event.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Qualitative Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Error, accident, or act of nature is <strong>almost certain</strong> to occur, or occurs more than 100 times a year.</td>
</tr>
<tr>
<td>High</td>
<td>Error, accident, or act of nature is <strong>highly likely</strong> to occur, or occurs between 10-100 times a year.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Error, accident, or act of nature is <strong>somewhat likely</strong> to occur, or occurs between 1-10 times a year.</td>
</tr>
<tr>
<td>Low</td>
<td>Error, accident, or act of nature is <strong>unlikely</strong> to occur, or occurs less than once a year, but more than once every 10 years.</td>
</tr>
<tr>
<td>Very Low</td>
<td>Error, accident, or act of nature is <strong>highly unlikely</strong> to occur, or occurs less than once every 10 years.</td>
</tr>
</tbody>
</table>

Confidence:
- **Medium**

Confidence:
- **High**
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, and Penalties

**Reference Loss Table - Credit Monitoring**

<table>
<thead>
<tr>
<th>Consumers</th>
<th>Range Included</th>
<th>Min</th>
<th>M/L</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1-9)</td>
<td>$</td>
<td>$</td>
<td>$25</td>
</tr>
<tr>
<td>10</td>
<td>(10-99)</td>
<td>$</td>
<td>$36</td>
<td>$200</td>
</tr>
<tr>
<td>100</td>
<td>(100-999)</td>
<td>$10</td>
<td>$306</td>
<td>$2,000</td>
</tr>
<tr>
<td>1,000</td>
<td>(1,000-9,999)</td>
<td>$100</td>
<td>$2,970</td>
<td>$20,000</td>
</tr>
<tr>
<td>10,000</td>
<td>(10,000-99,999)</td>
<td>$1,000</td>
<td>$29,700</td>
<td>$200,000</td>
</tr>
<tr>
<td>100,000</td>
<td>(100,000-999,999)</td>
<td>$10,000</td>
<td>$29,700</td>
<td>$2,000,000</td>
</tr>
<tr>
<td>1,000,000</td>
<td>(1,000,000-9,999,999)</td>
<td>$100,000</td>
<td>$2,970,000</td>
<td>$20,000,000</td>
</tr>
<tr>
<td>10,000,000</td>
<td>(10,000,000-99,999,999)</td>
<td>$1,000,000</td>
<td>$29,700,000</td>
<td>$200,000,000</td>
</tr>
<tr>
<td>100,000,000</td>
<td>= and &gt; than 100,000,000</td>
<td>$10,000,000</td>
<td>$108,000,000</td>
<td>$600,000,000</td>
</tr>
</tbody>
</table>

“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
### Estimate the Magnitude

#### Qualitative Values

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>The threat event could be expected to have <strong>multiple severe or catastrophic</strong> adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.</td>
</tr>
<tr>
<td>High</td>
<td>The threat event could be expected to have a <strong>severe or catastrophic</strong> 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 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.</td>
</tr>
<tr>
<td>Moderate</td>
<td>The threat event could be expected to have a <strong>serious</strong> 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.</td>
</tr>
<tr>
<td>Low</td>
<td>The threat event could be expected to have a <strong>limited adverse effect</strong> 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.</td>
</tr>
<tr>
<td>Very Low</td>
<td>The threat event could be expected to have a <strong>negligible adverse effect</strong> on organizational operations, organizational assets, individuals other organizations, or the Nation.</td>
</tr>
</tbody>
</table>

---

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

---

### Fines & Judgments

<table>
<thead>
<tr>
<th>Confidence</th>
<th>Minimum</th>
<th>Most Likely</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>$0</td>
<td>$5,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>High</td>
<td>$0</td>
<td>$0</td>
<td>$100,000</td>
</tr>
</tbody>
</table>

---

### Response

<table>
<thead>
<tr>
<th>Confidence</th>
<th>Minimum</th>
<th>Most Likely</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>$1,000</td>
<td>$30,000</td>
<td>$200,000</td>
</tr>
</tbody>
</table>
### Data Theft

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Avg</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss Events / Year</td>
<td>0</td>
<td>0.56</td>
<td>2</td>
</tr>
<tr>
<td>Loss Magnitude</td>
<td>$1.0k</td>
<td>$53.3k</td>
<td>$179.2k</td>
</tr>
</tbody>
</table>

### Accidental Disclosure

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Avg</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss Events / Year</td>
<td>10</td>
<td>20.64</td>
<td>69</td>
</tr>
<tr>
<td>Loss Magnitude</td>
<td>$1</td>
<td>$181</td>
<td>$799</td>
</tr>
</tbody>
</table>

### Single Loss Max

- **Data Theft**: $270k
- **Annualized**: $320k
- **Accidental Disclosure**: $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

### Data Theft Costs

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>$34.9k</td>
<td>$318.4k</td>
<td>$350k</td>
</tr>
</tbody>
</table>

### Accidental Disclosure Costs

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>$63</td>
<td>$111.4k</td>
<td>$1.6M</td>
<td></td>
</tr>
<tr>
<td>$11</td>
<td>$3.7k</td>
<td>$28.5k</td>
<td></td>
</tr>
</tbody>
</table>
Trade-Offs - Data Theft

Investment Cost

<table>
<thead>
<tr>
<th>Category</th>
<th>Current Budget</th>
<th>Proposed Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight &amp; Audit</td>
<td>$19,000</td>
<td>$19,000</td>
</tr>
<tr>
<td>Protection</td>
<td>$85,000</td>
<td>$85,000</td>
</tr>
<tr>
<td>Detection &amp; Response</td>
<td>$25,000</td>
<td>$85,000</td>
</tr>
</tbody>
</table>

Risk Reduction

- Minimum: $0
- Average: $34.9k
- Maximum: $318.4k

- Minimum: $0
- Average: $24.7k
- Maximum: $307.6k

Total Investment Cost: $350k

- Total Risk Reduction: $350k
Sample On-Going Reporting

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.

<table>
<thead>
<tr>
<th>Scenario Scope</th>
<th>Threats</th>
<th>Motivation</th>
<th>Loss Area</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cyber Criminals</td>
<td>Accidental</td>
<td>Confidentiality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privileged Insiders</td>
<td>Financial Gain</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Embarrassment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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?
# 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
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](http://amzn.com/0124202314)