Quantifying Cyber Security Risk in Dollars and Cents to Optimize Budgets

CRM008

Speakers:

• Chris Cooper, VP, Operational Risk Officer; RGA Reinsurance Company
• Steven Tabacek, President, RiskLens, Inc.
Learning Objectives

At the end of this session, you will:

- **Understand the Challenges of Cyber Risk Analysis Today**
  - Cyber Risk Communication
  - Common Risk Analysis tools & methodologies
  - Is compliance working?

- **Learn what is Factor Analysis of Information Risk (FAIR)**
  - About FAIR
  - Benefits of cyber risk quantification
  - Building a cyber risk quantification analysis scenario

- **See an example putting the FAIR model into practice**
  - Cyber Risk Analysis Scenario Composition
  - Cyber Risk Analysis Data
  - Communicating Analysis Results
The Communication Challenge

CFO
“How much loss exposure do we have? Are we spending too little or too much on mitigation?”

ERM
“How much loss exposure do we have? Are we spending too little or too much on mitigation?”

CISO
“Εχουμε πάνω από δέκα χιλιάδες τρωτά σημεία , είναι συμβατό με το ογδόντα τοις εκατό”

BOARD/CEO
“We don’t want to be the next news headline. Are we doing enough to minimize risk?”

CIO
“Are we spending our cybersecurity budget on the right things?”
Cyber Risk = Business Risk

A primary responsibility for a CIO or CISO when talking to the CEO or board of directors is to articulate how cyber security translates into dollars and cents. Putting monetary value on security events, and tying security to real-life business cases, can show senior executives the potential impact of a cyber event in terms that make sense to them.

Make security everyone’s business.
Risk Assessment Today…

The way most information security professionals measure risk today fails to quantify cyber-risk in terms the business can understand and use.
Is Compliance Working?

UPDATE 3-U.S. Postal Service data breach may compromise staff, customer details

Home Depot facing dozens of data breach lawsuits

White-hat hacker fights cyber intrusions on NATO systems

Staples Investigates Potential Data Breach In The Northeast

Official describes rampant computer hacking at VA

Lax Security at LinkedIn Is Laid Bare

Sony, Citi, Lockheed: Big Data Breaches in History

Exclusive: Apple, Macs hit by hackers who targeted Facebook

Class Action Targets Jimmy John’s in Data Breach

LivingSocial Hacked, 50 Million Names, Emails, Birthdates, Encrypted Passwords Accessed

BUSINESS

Hacking At Citi Is Latest Data Scare

New York Times, Wall Street Journal say Chinese hackers broke into computers

By Jethro Mullen, CNN

Updated 5:59 PM ET, Thu January 31, 2013
Defining Cyber Risk

*Risk*...
The probable frequency and probable magnitude of future loss

*In other words*...
How often bad things are likely to happen, and how bad they’re likely to be when they do happen
Cyber Risk Quantification

FAIR
Factor Analysis of Information Risk

- An ontology for information and operational risk
- Standard nomenclature for risk terms
- A framework for establishing data collection criteria
- Integrates into a computational engine for calculating risk
Building a Cyber Risk Scenario

1. Asset at risk
2. Threat Actors
   - Hacktivism
   - Crime
   - Insider
   - Espionage
   - Terrorism
   - Warfare
3. Threat Effect: Confidentiality, Integrity, Availability
Use Case: Attack on Web App

Purpose

• Determine the level of risk associated with attacks against a customer web application for a specialty service.

• The above information would serve as the basis for determining if current resources are appropriate to resolve identified vulnerabilities.

<table>
<thead>
<tr>
<th>Asset At Risk</th>
<th>Threat Community</th>
<th>Threat Type</th>
<th>Threat Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Web Application</td>
<td>General Hackers</td>
<td>Malicious</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>
Attack on Web Application

Threat Event Frequency = TEF
- Data from threat intelligence application

<table>
<thead>
<tr>
<th>TEF</th>
<th>Minimum</th>
<th>Most Likely</th>
<th>Maximum</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Event Frequency</td>
<td>12 p/yr.</td>
<td>19 p/yr.</td>
<td>26 p/yr.</td>
<td>Low</td>
</tr>
</tbody>
</table>

Risk
- Loss Event Frequency
- Vulnerability Level
- Primary Loss
- Secondary Loss

Data from threat intelligence application
Effectiveness of Controls

• The web application firewall effectively mitigates the largest percentage of threats events.

• Other factors to reduce vulnerability for an attack on this web application:
  • Based on review, the web application has a number of identified vulnerabilities that have not been patched within 180 days.
  • Some user’s accounts are known to use simple-to-guess passwords that still meeting required criteria (ex. Spring.16)
Vulnerability = VULN
- Other measurably effective resistive controls
Loss Event Frequency = LEF
- This is a calculated field from the distributions of threat event frequency and vulnerability
- LEF = ~Once every 3 years
Loss Magnitude = LM
- Primary Loss Magnitude
  - Productivity (employee)
  - Loss Revenue
  - Initial Response

RISK

Loss Event Frequency
Vulnerability Level
Primary Loss
Secondary Loss

Loss Magnitude

Primary Loss

PL
Minimum
Most Likely
Maximum
Confidence

$20K
$37K
$45K
Moderate
Attack on Web Application

Loss Magnitude = LM
- Secondary Loss Magnitude
  - Fines & Judgements
  - Secondary Response
    - Credit Monitoring

Loss Event Frequency
- Vulnerability Level
- Primary Loss
- Secondary Loss

RISK

SL
- Minimum: $819K
- Most Likely: $2.6M
- Maximum: $4.8M
- Confidence: Low
Loss Exposure

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>$4.9M</td>
</tr>
<tr>
<td>90th %</td>
<td>$2.7M</td>
</tr>
<tr>
<td>Average</td>
<td>$657K</td>
</tr>
<tr>
<td>10th %</td>
<td>$0</td>
</tr>
<tr>
<td>Minimum</td>
<td>$0</td>
</tr>
</tbody>
</table>
Tactical vs. Strategic Analysis

Tactical
• Single scenario pre-mitigation analysis such as the previous example of the “Attack on Web Application”
• Post-mitigation analysis following control improvements

Strategic
• Multiple scenario analysis providing a probabilistic view of enterprise risk supporting case studies such as:
  • Reporting “Top-Ten Risks and Aggregate Loss Exposure to the Board
  • Tracking Departmental or Enterprise Loss Exposure over Time to establish ROI of security budgets and performance of managers.
## Risk Quantification Benefits

<table>
<thead>
<tr>
<th>USE CASES</th>
<th>ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand Loss Exposure</td>
<td>Preserve business value</td>
</tr>
<tr>
<td>Prioritize Risk Mitigations</td>
<td>Maximize risk reduction</td>
</tr>
<tr>
<td>Assess ROI of security initiatives</td>
<td>Optimize cyber security investments</td>
</tr>
<tr>
<td>Optimize Cyber Insurance Coverage</td>
<td>Facilitate risk transfer</td>
</tr>
<tr>
<td>Effectively Assess Third Party Risk</td>
<td>Reduce supply-chain risk</td>
</tr>
</tbody>
</table>
Aggregate Enterprise Risk

Aggregate Loss Exposure

The aggregation of all independently analyzed risk scenarios.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>$1.3B</td>
</tr>
<tr>
<td>90th %</td>
<td>$405.3M</td>
</tr>
<tr>
<td>Average</td>
<td>$228.5M</td>
</tr>
<tr>
<td>10th %</td>
<td>$112.9M</td>
</tr>
<tr>
<td>Minimum</td>
<td>$31.3M</td>
</tr>
<tr>
<td>Risk Appetite</td>
<td>$130.0M</td>
</tr>
</tbody>
</table>
Are we adequately insured?

- **Productivity** (e.g. Business Interruption): $7.2M
- **Replacement** (e.g. Capital Assets): $719K
- **Primary Response** (e.g. Crisis Management): $536K
- **Fines and Judgements** (e.g. Civil & Govt. Fines): $16.0M
- **Reputation** (e.g. Stakeholder Impact): $63.5M
- **Secondary Response** (e.g. Privacy Liability): $140.5M
Are we reducing risk over time?

Loss Exposure over Time

- 2015 Q1
- 2015 Q2
- 2015 Q3
- 2015 Q4
- 2016 Q1

- 90th
- Avg
- RA
- 10th

Loss Exposure

- $600.0M
- $500.0M
- $400.0M
- $300.0M
- $200.0M
- $100.0M
- $0