Cyber Risk Case Study

A Scenario-Based Approach to Identifying and Mitigating Key Threats

October 23, 2019
Cyber Risk Case Study: A Scenario-Based Approach to Identifying and Mitigating Key Threats

IAA
October 23, 2019

Shahryar Shaghaghi  Sim Segal  Dave Bartholomew
Principal, CohnReznick  President, SimErgy Consulting  Director, Internal Audit
Panelists

Shahryar Shaghaghi
Principal, CohnReznick

Sim Segal
President, SimErgy Consulting

Dave Bartholomew
Director, Internal Audit
Agenda

- Current state of cybersecurity risks
- Value-based cyber risk management
- Applying value-based cyber risk management: Case study
CURRENT STATE OF CYBERSECURITY
Today’s cyber threat landscape

- Breaches increasing across industry
- Breaches are more sophisticated, on a larger scale and have greater impact
- Multiple incentives & types of breaches/threats
- Phishing, DDOS and Ransomware are the most common
- U.S. has the highest average Cost Per Breach

According to the Ponemon Institute’s most recent annual study, the average organizational cost of a data breach in 2016 was $4 million, or $158 per compromised record.
World’s biggest data breaches and hacks
by number of records compromised
Today’s cyber threat landscape

As digital transformation programs accelerate, the cybersecurity and data privacy landscape is constantly evolving.

- Today, we have 20 billion devices attached to the Internet. In less than 2 years, we will have 50 billion devices connected to the Internet.*
  - IoT and smart buildings are the major contributing factors.
- In order to design and build a smart but secure and private by design building, it is vital to understand what data is flowing through your environments including IoT devices and external entities including the entire ecosystem.
- Security and Privacy by design starts early in the development lifecycle.
- Hackers only need to be right once. Those who protect the organization need to be right all the time. Your cybersecurity program needs to not just be continuously evolving, but strategically engrained in your business strategy.

* Source: Cisco
Businesses will be hacked because it’s easy

- Have not fully assessed their cyber risks
- Have not classified their data
- Don’t have latest security controls in place
- Many use social media to market their products and services
- Spend money in siloes
- Challenge to attract and retain internal security talents
- Use encrypted devices and unsecure emails for sensitive data
- Depend on third parties for various functions
- Most concerned about losing their customer data and bank account
What should they do to minimize attack impact?

- Start by assessing your cyber risks: What is core to your business; impact to value; asset valuation and risk-based.
- Understand motives & drivers.
- Evaluate internal capabilities and outsource as appropriate.
- Incorporate key cybersecurity and privacy programs into your audit plans.
- Treat this as cost of running your business.

- Determine who has access to what.
- Classify and segment your critical data.
- Perform backups and patch management.
- Conduct ongoing security awareness training and social engineering testing.
- Have a tested Incident Response Plan.
Example of an Enterprise Security Framework

Enterprise Security Framework

Security Operations
- Access management
- Directory management
  - Authentication
  - User administration
  - Remote access
  - Application security
- Pen Test / Ethical Hack
- Change management
- Vulnerability management
  - Patch management
- Spam, anti-virus, & spy-ware
- Data protection-encryption

Governance
- Security program
  - Policies
  - Standards & procedures
  - Threat & risk assessment
  - Risk management
  - Metrics & reporting
- Asset classification
  - Awareness
- Security assessments
- Remediation management
- Vulnerability alerting
- Vendor management

Incident Response
- Incident detection
- Incident response plan
- Disaster recovery plan
- Data restoration
- System monitoring
  - Log Control
- Event management
  - Escalation
- Enterprise response plan
- Communication plan

People/Organization
- Roles & responsibilities
  - Training
  - Awareness

Risk Management
- Third-parties / Vendor Risk
- Risk Transfer & Mitigation
- Risk Assessment Program

Infrastructure
- Patch levels
- Application Security
- Cloud Security
- Data center

Drivers
- Business
  - Strategies
  - Threats
  - Risk tolerance
- IT
  - Strategies
  - Architecture
  - Organization
- Compliance
  - Methodology
  - Data
  - Standards

Identify
Protect
Detect
Respond
Recover
Cybersecurity Functional Model

Govern, Manage, Comply, and Manage Risk
Ensure that XX’s leadership, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization’s risk tolerance.

Protect, Shield, Defend, and Prevent
Ensure that XX’s staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization’s risk tolerance.

Monitor, Detect, and Hunt
Ensure that XX’s staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.

Respond, Recover, and Sustain
When a cybersecurity incident occurs, minimize its impact and ensure that XX’s staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include technologies, information, people, facilities, and supply chains.

Educate
Ensure that XX is providing the staff training on cybersecurity risk and course correction of all cybersecurity activities. This function includes creating a company-wide culture that is attuned to corporate risks.
Cybersecurity lifecycle

- Business Drivers
- Compliance Requirements
- Risk Tolerance
- Cyber Concerns
- Assessment Objectives
- Threats
- Vulnerabilities
- Risks
- Targets
- Threat Vectors

- Continuous Monitoring & Improvement

- Findings, Risks, Observations

- Tactics
- Techniques
- Procedures

- Roadmaps
- Implementation Plans
- Governance Model
- Strategies

- Solutions
- Policies
- Staff
- Tools
- Etc.

- Security Strategies & Tactics
- OPTIMIZE
- IDENTIFY
- DISCOVER
- PRIORITIZE
- RECOMMEND
- DEVELOP
- DEPLOY
- OPTIMIZE
How to keep the balance

What is the best balance between enhanced user experience and privacy / security in the context of digital transformation?
VALUE-BASED CYBER RISK MANAGEMENT
Obstacles in traditional cybersecurity risk management

1) Prioritizing focus amidst myriad cyber risks
2) Making the business case for mitigation decisions
3) Defining cyber risk appetite
Quantifying individual cyber risk scenarios

Company Value Impact

- Cyber Risk 3, Scen 2: (2.5%)
- Cyber Risk 11, Scen 1: (5%)
- Cyber Risk 24, Scen 3: (1%)
- Cyber Risk 17, Scen 1: (3.5%)
- Cyber Risk 5, Scen 2: (0.5%)
- Cyber Risk 9, Scen 4: (5%)
- Cyber Risk 1, Scen 2: (3.5%)
- Cyber Risk 16, Scen 1: (4%)
- Cyber Risk 6, Scen 5: (2%)
- Cyber Risk 2, Scen 3: (2.5%)
- Cyber Risk 4, Scen 1: (5%)
- Cyber Risk 19, Scen 3: (1%)
- Cyber Risk 3, Scen 1: (2%)
1) Prioritizing focus amidst myriad cyber risks

<table>
<thead>
<tr>
<th>Traditional Approach</th>
<th>Value-based Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method 1: Qualitative</td>
<td>Quantifies impact to value / supports decision-making</td>
</tr>
<tr>
<td>Cannot support decision-making</td>
<td></td>
</tr>
<tr>
<td>Method 2: Industry data</td>
<td>Available, company/situation-specific, dynamic</td>
</tr>
<tr>
<td>Often unavailable, inappropriate, static</td>
<td></td>
</tr>
<tr>
<td>Method 3: Risk capital</td>
<td>Risk-based</td>
</tr>
<tr>
<td>Arbitrary / often directionally incorrect</td>
<td></td>
</tr>
</tbody>
</table>
Developing risk scenarios: FMEA

1) Identify interviewees
   - Those closest to the risk
   - Usually 1 or 2 risk experts

2) Develop risk scenarios
   - Begin with credible worst case
   - Select specific scenario and think it through

3) Assign likelihoods

4) Quantify
   - Determine impacts on distributable cash flows
Prioritizing focus through quantification

Company Value Impact

- Cyber Risk 3, Scen 2: (2.5%)
- Cyber Risk 11, Scen 1: (5%)
- Cyber Risk 24, Scen 3: (1%)
- Cyber Risk 17, Scen 1: (3.5%)
- Cyber Risk 5, Scen 2: (0.5%)
- Cyber Risk 9, Scen 4: (5%)
- Cyber Risk 1, Scen 2: (3.5%)
- Cyber Risk 16, Scen 1: (4%)
- Cyber Risk 6, Scen 5: (2%)
- Cyber Risk 2, Scen 3: (2.5%)
- Cyber Risk 4, Scen 1: (5%)
- Cyber Risk 19, Scen 3: (1%)
- Cyber Risk 3, Scen 1: (2%)
2) Making the business case for mitigation decisions

<table>
<thead>
<tr>
<th>Do metrics support decision-making?</th>
<th>Traditional Cyber RM</th>
<th>Value-Based Cyber RM</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Usually qualitative only</td>
<td>▪ Only risk, not return</td>
<td>▪ Metrics for all cyber risks</td>
</tr>
<tr>
<td>▪ Only risk, not return</td>
<td>▪ ΔValue = business case</td>
<td></td>
</tr>
<tr>
<td>Is there buy-in?</td>
<td>▪ Corporate-driven</td>
<td>▪ SME/CISO-driven</td>
</tr>
<tr>
<td></td>
<td>▪ Compliance-oriented</td>
<td>▪ Supports SME/CISO goals</td>
</tr>
</tbody>
</table>
Supports decision making

Case studies:
- Enhancement of info sec risk management (tech)
- Data breach guarantee decision (telecomm)
- Business case for mitigation of privacy data breach (insurance)
3) Defining cyber risk appetite

<table>
<thead>
<tr>
<th></th>
<th>Traditional Approach</th>
<th>Value-Based Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics</td>
<td>Multiple, competing metrics</td>
<td>Single, unifying metrics</td>
</tr>
<tr>
<td>Trade-off decisions between exposures?</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Aggregated enterprise cyber risk exposure?</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber risk limits set by cascading downward?</td>
<td>X</td>
<td>✓</td>
</tr>
</tbody>
</table>
Enterprise cyber risk exposure “pain points” define cyber risk appetite

<table>
<thead>
<tr>
<th>&quot;Pain Point&quot;</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>ΔValue ≤ -10%</td>
<td>25%</td>
</tr>
<tr>
<td>ΔValue ≤ -30%</td>
<td>4%</td>
</tr>
</tbody>
</table>

What is it now?

<table>
<thead>
<tr>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
</tr>
<tr>
<td>?</td>
</tr>
</tbody>
</table>

What do we want it to be?

Target exposure (defined by Risk Committee)

CYBER RISK APPETITE

Current exposure (calculated)
APPLYING VALUE-BASED CYBER RISK MANAGEMENT: CASE STUDY
Company/ERM background

- CUNA Mutual Group
- Began ERM program 2014
- Engaged SimErgy 2016 for value-based ERM
Quantification of cybersecurity risks

- Historical approaches applied – 2012-2016
  - Ponemon Institute report
  - Verizon Data Breach report
  - Analysis of public company data breach results
  - Internal Monte Carlo simulations using data/approaches these reports

- Challenges
  - Cost per record/per event are poorly defined
  - General models not applicable to our business
  - Impact to future sales, surrenders, cancellations, etc.
Cyber risk identification

- Sources of cyber risk:
  - Internal malicious users
  - External actors
  - Third parties

- Direct impacts:
  - Disruption of operations
  - Theft of $x$
  - Theft of intellectual property
  - Data breach of NPPI

- Qualitative risk assessment to prioritize risks
- Validation with management to select risks for quantification
For selected risks:

- Failures Modes and Effects Analysis (FMEA) interviews
  - Developed multiple deterministic scenarios
  - Captured likely shocks to assumptions driving performance
  - Gathered likely mitigation/response plans
  - Validated “guesses” by experts throughout the company

- Used Excel-based model to develop individual risk scenario quantification $\rightarrow$ impact to company value, RBC

- Ranked these risks with all other quantified risks
Results from quantification process

- Management agreement on definition of risks
- Scenarios that are easy to understand
- Quantification of scenarios which is easy to understand
- Comparison of cyber security risks to all other operational and strategic risks
- Development of a quantitative and qualitative cyber risk management policy
- Highlight areas of improvement needed:
  - Data breach incident response
  - Management of third party improvements
Further use of the model

- New third party relationships contemplated
  - Model financial impact of relationship
  - Model impact to risks
  - Architect the relationship to balance risk and reward
Contact information

Shahryar Shaghaghi
Principal, CohnReznick
Shahryar.Shaghaghi@CohnReznick.com

Sim Segal
President, SimErgy Consulting
sim@simergy.com

Dave Bartholomew
Director, Internal Audit
david.bartholomew@pacificlife.com

CohnReznick
SimErgy
PACIFIC LIFE