Cybersecurity – A Team Sport: A Case Study of Building an Effective and Resilient Program

Thursday, January 12, 2017

Introductions

Presenters
Augustine Doe
VP ERM
Network Health Inc.

Tim Riley
CIO
Network Health Inc.

Joseph Abenio
VP, Commercial Services
Delta Risk LLC

Moderator
Jennifer Rathburn
Partner
Foley & Lardner LLP
Agenda

A. Data breach findings that have implications for organizations
B. Game prep—coming together to create a cyber ecosystem
C. Team roster and responsibilities
D. Playbook—executive risk officer
E. Playbook—executive information technology officer
F. Playbook—cyber risk consultant
G. Playbook—cyber attorney
H. Goal line themes
I. Appendices

Data Breach Findings that have Implications for Organizations

A. Hackers and criminal insiders cause the most data breaches

Distribution of Root Cause of Data Breach

- Malicious or criminal attack (48%)
- System glitch (25%)
- Human error (27%)

Data Breach Findings that have Implications for Organizations (cont.)

B. Based on threat action varieties in breaches overtime—phishing and point-of-sale are a big deal!

**Threat Action Varieties in Breaches Over Time**

Source: 2016 Verizon Data Breach Investigations Report

---

Data Breach Findings that have Implications for Organizations (cont.)

C. Where phishing and point-of-sale are root cause of breach—server and user device are assets of choice

**Percent of Breaches per Asset Category Over Time**

Source: 2016 Verizon Data Breach Investigations Report
Data Breach Findings that have Implications for Organizations (cont.)

D. The cost of data breach varies by industry—regulated industries such as health care and financial services have the most costly data breaches because of fines and the higher than average rate of lost business and customers.

**Per Capita Data Breach Cost by Industry Classification**

![Graph showing per capita data breach cost by industry classification.](source: Research Report, 2016 Cost of Data Breach Study: United States, Ponemon Institute (2016))

Data Breach Findings that have Implications for Organizations (cont.)

E. Factors that influence the cost of data breach—certain factors decreased the cost of data breach while others increased it.

**Impact of 16 Factors on the Per Capita Cost of Data Breach**

![Graph showing impact of factors on per capita cost of data breach.](source: Research Report, 2016 Cost of Data Breach Study: United States, Ponemon Institute (2016))
F. Inverse relationship between the probability of a data breach and the size of records—the probability of a data breach decreases as the size of records increases

Probability of a Data Breach Involving a Minimum of 10,000 to 100,000 Records


G. Time to identify and contain data breaches impact cost—the longer it takes to identify and contain data breach, the more it costs the organization

66% of the Cost of Data Breach Are Indirect Costs

Average Indirect Costs: $145/record
Average Direct Costs: $76/record

Indirect Costs Include:
- Time employees spend on data breach notification effort or investigations of the incident
- Loss of brand value and reputation
- Customer churn

Direct Costs Include:
- Forensic Experts
- Legal Fees
- Identity/Credit monitoring services to victims

Game Prep—Coming Together to Create a Cyber Ecosystem

Health Care Industry Risk Heat Map

TIE Framework
- Technology Solutions
- Insurance
- Enterprise-wide Risk Oversight

Consolidated view (n=383), measured in US $ (in millions):
- Description and Investigation: $0.79
- Notification Costs: $0.99
- Post-breach Costs: $1.72
- Lost Business: $3.97

Team Roster and Responsibilities

A. Executive information technology officer (CIO, CTO, etc.) responsible for **Technology Solutions**

B. Executive risk officer (CRO, VP ERM, etc.) responsible for **Insurance and Enterprise-wide Risk Oversight**

C. Expert cyber risk consultant (Cyber consultant, VP Sales, etc.) responsible for the **effective integration of People, Process, and Technology Solutions**

D. Cyber attorney (Partner) responsible for **Legal Advice**

---

Playbook—Executive Risk Officer

**A. Insurance: Cyber, Fiduciary, & D&O**

**Cyber**

*Aggregate limit and retention*

**Model for Estimating Aggregate Cyber Liability Limits & Retention**

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total insurable cyber loss and liabilities (5462* per exposure basis)</td>
<td>201,000,000</td>
</tr>
<tr>
<td>Potential insurable cyber losses and liabilities (based on probability of 0.25%)*</td>
<td>51,456,000</td>
</tr>
<tr>
<td>Loss reduction if security and cyber response programs discount (10%)</td>
<td>20,582,400</td>
</tr>
<tr>
<td>Net potential insurable cyber losses and liabilities</td>
<td>30,873,600</td>
</tr>
<tr>
<td>Retained potential insurable cyber losses and liabilities (varies by risk appetite: 3%)</td>
<td>1,543,680</td>
</tr>
<tr>
<td>Aggregate limit of cyber insurance that should be purchased (7%)</td>
<td>20,328,920</td>
</tr>
</tbody>
</table>

**Notes:**
- Average cost of data breach for healthcare organizations based on Ponemon study is $605K.
- Probability of data breach involving a minimum of 1,000 to 10,000 records is between 25% and 60% based on Ponemon study.
Playbook—Executive Risk Officer (cont.)

- Insurance sub-limits

<table>
<thead>
<tr>
<th>Exposure Tools</th>
<th>Number of data type (PCI/PHI/PII), non-card financial or records</th>
<th>US Industry Averages</th>
<th>Sublimits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection and escalation: forensic and investigative activities, assessment and audit services, crisis team management and communications, management and board of directors</td>
<td>$57,733</td>
<td>$360,000</td>
<td></td>
</tr>
<tr>
<td>Notification and compliance: IT activities associated with creation of contact databases, determination of all regulatory requirements, engagement of outside experts, social expenditures, email bounce logs and in-bound communication set-up</td>
<td>$45,963</td>
<td>$279,000</td>
<td></td>
</tr>
<tr>
<td>Point breach: help desk activities, cloud computing, special investigative activities, remediation, legal expenditures, product discounts, identity protection services, and regulatory interventions</td>
<td>$177,000</td>
<td>$389,000</td>
<td></td>
</tr>
<tr>
<td>Unstructured data breach: abnormal turnover of customers, increased customer acquisition activities, regulation losses and threatened goodwill</td>
<td>$33,000</td>
<td>$1,985,000</td>
<td></td>
</tr>
</tbody>
</table>

Note: ‘Note to compute your specific industry average as average costs vary by industry

- Control Group Definition
- Panel law firm and vendors for privacy breach response services
- Credit monitoring services
- Identity theft prevention and information disposal programs
- PCI exclusions
- First party computer security coverage endorsement

Fiduciary & D/O
- Potential for DIs/OS to be subject to shareholder suits alleging breaches of fiduciary duties in the wake of system breaches—ensure Board provides oversight of cyber program
- Palkon ex rel. Wyndham Corp. v. Holmes

Playbook—Executive Risk Officer (cont.)

B. Enterprise-wide risk oversight

- Ensure board-level and enterprise-wide involvement through ERIM program
- Manage and monitor cyber risk through risk reporting tools

See Appendices for sample tools

- Business Continuity Management Program (BCMP) should include breach response and notification plan (team), IT disaster recovery plan, and continuity plan for each business operation
A. Technology Solutions
1. Executive planning approach—service excellence

<table>
<thead>
<tr>
<th>Manage:</th>
<th>Regulatory</th>
<th>Systems Continuous Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Schedule</td>
<td>Business Opportunities</td>
<td>• People</td>
</tr>
<tr>
<td>• Value ROI</td>
<td>Disruptive Events</td>
<td>• Process</td>
</tr>
<tr>
<td>• Usability</td>
<td>Release Management</td>
<td>• Technology</td>
</tr>
<tr>
<td>• Risk</td>
<td>TOI</td>
<td></td>
</tr>
<tr>
<td>• Cost</td>
<td>Other Project Resource Competition</td>
<td>Common Requests / Uncommon Requests / Incidents / Projects</td>
</tr>
<tr>
<td>• Quality</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Understand current state of organization’s network infrastructure
   • Conducted physical and firmware assessment
   • Conducted comprehensive security reviews and vulnerability assessments using vendors: Coalfire, Delta Risk, and Mandiant
   • Learned more about IT general controls from Model Audit Rule (MAR) implementation

3. Developed and began to implement solutions to address identified gaps
   • Redesigned network infrastructure to improve uptime and availability
     1. Equipment covered by 24X7 support, 4-hour response
     2. Redundant network equipment in case of equipment failure
     3. Updated uninterruptable power
     4. Installed climate control
   • Worked with third-party data center operator to tighten security with Web filtering, configuration of servers and updated McAfee to include current patches
4. Adopted new framework for administering IT functions and operations

5. Operationalized new IT framework

- Active Eye 24/7 coverage
- Managed Security Information and Event Management (SIEM)

- Privacy Incidents
- Security Incidents
- Business Continuity Plan

- Training
- Bulletins
- Executive Expectations

---

B. Benefits we are experiencing from operationalized framework

1. Robust incident response and team—business continuity
2. Continuous corporate-wide employee awareness of ways to help organization manage and monitor cyber risks
3. Corporate training on how to spot cyber threats, report threat—participate in threat sharing
4. Extensive use of encryption to protect data—lost or stolen devices
5. Provision of ID protection
6. Scaled-back on cloud migration to provide control over data unless SOC report indicates robust cloud security
7. Reduced number of data in motion through reduction in number of IT-related third party involvement
8. Extensive use of DLP and data classification schema
Playbook—Cyber Risk Consultant

A. Technology Solutions
1. Support IT and organization with best-in-class cyber risk management practices and solutions
2. Active network monitoring—Delta Risk Active Eye
3. Integration of organization’s employees and business partners into the organization’s cyber risk management
4. Lead the development of the organization’s cyber risk response program

Playbook—Cyber Attorney

A. Legal Cyber Related Counseling
1. Involve Legal Counsel to Enhance Attorney Client Privilege and Control Communications
2. Cybersecurity and Privacy Program Documentation and Policy Review
3. Board of Director Training
4. Data Breach Preparation and Response
5. Hiring of Outside Security and Other Vendors
6. Government Investigations and Litigation Assistance
7. Vendor Management/Contract Review and Other Transactional Assistance
8. Cyber Insurance Review
Goal Line Themes

A. Ecosystem in which CRO, CIO, cyber attorney and cyber consultant collaboratively manage and monitor risk

B. Ongoing Board, senior management and organization-wide involvement in cyber risk management and monitoring

Appendices
Appendix A—Healthcare Industry Risk Heat Map: Sample

Appendix B—IT Risk Register: Sample

<table>
<thead>
<tr>
<th>KEY ASPECTS OF RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Name</strong></td>
</tr>
<tr>
<td><strong>Description of Risk</strong></td>
</tr>
<tr>
<td><strong>Risk Owner(s)</strong></td>
</tr>
<tr>
<td><strong>Key Drivers of Risk</strong></td>
</tr>
<tr>
<td><strong>Probability of Risk</strong></td>
</tr>
<tr>
<td><strong>Potential Financial Impact of Risk</strong></td>
</tr>
<tr>
<td><strong>Potential/Operational Impact of Risk</strong></td>
</tr>
<tr>
<td><strong>Key Performance Indicators (KPIs)</strong></td>
</tr>
<tr>
<td><strong>Key Risk Indicators (KRI)</strong></td>
</tr>
<tr>
<td><strong>Risk Control/Mitigating Measures</strong></td>
</tr>
<tr>
<td><strong>Actions Required</strong></td>
</tr>
</tbody>
</table>
Appendix C—Risk Dashboard: Samples

<table>
<thead>
<tr>
<th>Description of Risk</th>
<th>Key Risk/Performance Indicators (KRIs/KPIs)</th>
<th>Minimum Threshold</th>
<th>Maximum Threshold</th>
<th>Risk Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underwriting health insurance in post-ACA market</td>
<td>Quarterly loss ratio</td>
<td>76%</td>
<td>90%</td>
<td>Head of Anticipatory</td>
</tr>
<tr>
<td>Data loss and privacy breaches</td>
<td>Total number of successful hacking attempts per month</td>
<td>35</td>
<td>60</td>
<td>Head of IT</td>
</tr>
<tr>
<td>Brand-making and reputational incidents</td>
<td>Customer satisfaction (CSAT) score</td>
<td>85%</td>
<td>100%</td>
<td>Head of Communications</td>
</tr>
<tr>
<td>Decreasing ROIC</td>
<td>Quarterly ratio (% of TAC/ACL ROIC)</td>
<td>40%</td>
<td>50%</td>
<td>Head of Finance</td>
</tr>
<tr>
<td>Comprehensive people strategy</td>
<td>Monthly employee turnover (voluntary)</td>
<td>15%</td>
<td>20%</td>
<td>Head of Human Resources</td>
</tr>
<tr>
<td>IT unable to support operations</td>
<td>Monthly system uptime</td>
<td>200 hours</td>
<td>360 hours</td>
<td>Head of IT</td>
</tr>
<tr>
<td>Inability to accomplish risk-based audit</td>
<td>Total monthly hours available to audit</td>
<td>600 hours</td>
<td>750 hours</td>
<td>Head of Audit and/or Risk Management</td>
</tr>
<tr>
<td>Regulatory non-compliance</td>
<td>Number of regulatory warnings</td>
<td>10</td>
<td>20</td>
<td>Head of Legal or Risk Management</td>
</tr>
<tr>
<td>Subsidiary cost overruns</td>
<td>Subsidiary budget variance</td>
<td>$200,000</td>
<td>$400,000</td>
<td>Head of Finance</td>
</tr>
<tr>
<td>Substantial increase in Workers' Compensation reserves</td>
<td>Percentage change in WC reserves</td>
<td>3% monthly</td>
<td>8% monthly</td>
<td>Head of Audit and/or Risk Management</td>
</tr>
<tr>
<td>Declining investment portfolio</td>
<td>Monthly change in value of portfolio</td>
<td>3% monthly</td>
<td>7% monthly</td>
<td>Head of Finance</td>
</tr>
<tr>
<td>Decreasing DBA benefits</td>
<td>Percentage change in DBA benefits administered</td>
<td>5% monthly</td>
<td>8% monthly</td>
<td>Head of Business Unit</td>
</tr>
</tbody>
</table>

Appendix D—Risk Tolerance Policy: Sample
Appendix E—Formal Risk Appetite Statement: Sample

This Formal Risk Appetite Statement is drafted solely for the purpose of providing Company XYZ, its subsidiaries and affiliates, guidance on how to manage enterprise-wide risks. No statements made herein bind Company XYZ, its subsidiaries and affiliates to any contemplated contracts or agreements. Company XYZ, its subsidiaries and affiliates reserve the right to change any statements made herein with or without notice to any third parties.

### Risk Elements

<table>
<thead>
<tr>
<th>Guiding Statement</th>
<th>Our Assertions</th>
<th>Additional Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Brand-making and reputation</strong></td>
<td>Brand protection and enhancements: We strive to proactively avoid any situation or action that has the potential to unnecessarily impair our brand and reputation. This involves ensuring our employees, business partners, and polioplastics are committed to our values and that our actions and transactions reflect these values. We believe this is what would allow us to take appropriate actions to preserve the strength of our brand and reputation in the areas of corporate compliance, customer privacy, corporate information security, governance, and positive public image.</td>
<td><strong>Vision and Mission Statements</strong></td>
</tr>
<tr>
<td><strong>Capital Adequacy</strong></td>
<td>Risk-based capital: We strive to grow to an IBC level appropriate to the risk of our non­market operations to ensure our sustainability in our market. (1) Controlled subsidiaries: Controlled subsidiaries are expected to manage their businesses and operations with the best interest of the shareholder and other appropriate stakeholders in mind. This expectation includes analysis and understanding of the risks associated with business initiatives to be undertaken by the controlled subsidiary. Further, controlled subsidiaries should comply with defined agreements, e.g., inter­company agreements, dividend policy, etc. (2) Non­market operations: Non­market operations should be managed based on the risk profile of our controlled subsidiaries, the risk profile of our non­market operations, and our business and Company XYZ's capital position.</td>
<td><strong>Employee Expenses Reimbursement Policies Employment Policies</strong></td>
</tr>
<tr>
<td><strong>Contribution to Surplus</strong></td>
<td>Incentivizing: In order to remain viable in our market, we target an annual operating margin of 5% across all non­market operations. Product segments (both core and non­core) are expected to have a positive contribution to IBC.</td>
<td><strong>Investment Policy Intercompany Agreements and Dividend Policies with Subsidiaries</strong></td>
</tr>
<tr>
<td><strong>Network Provider Penetration</strong></td>
<td>Provider reimbursements: We will maintain adequate market share to provide the best value to our polioplastics. We target no less than 50% of aggregate California health care providers' private payer network.</td>
<td></td>
</tr>
<tr>
<td><strong>Operational Risk Parameters</strong></td>
<td>Contract management and bid and proposal review: No projects or bids will be pursued without appropriate review and analysis based on defined governance processes, which should include an assessment of material risks and financial risk.</td>
<td></td>
</tr>
<tr>
<td><strong>Human Resources Risk Parameters</strong></td>
<td>Human Capital: We will ensure Company XYZ has identified key talent and leadership to develop new leaders through defined succession plans and development. We will maintain the resources and tools to attract, develop and retain the employees necessary to fulfill our mission.</td>
<td><strong>Human Resources Policies</strong></td>
</tr>
</tbody>
</table>

©2017 Foley & Lardner LLP