Security Risk Management Discussion
March 20, 2018
Great moments in risk management history...
Cyber risk has been addressed via regulation, quasi-regulation and massive investment

A number of information security guidance documents are currently available ... and more are on the way

Significant investment in cybersecurity products and services

... Challenge is how to prioritize planning in face of (a) adaptive threat, (b) limited resources, and (c) rapidly changing business and technology environment

(1) Source: Triangulation of Market Reports including Gartner, IDC, and others; TCG proprietary analysis
### Impact of Recent Cyber Attacks

<table>
<thead>
<tr>
<th>Company</th>
<th>Impact Details</th>
</tr>
</thead>
</table>
| **Equifax**    | • Approximately $150M 2017 impact  
                  • Expects additional $275M impact in 2018                              |
| **FedEx**      | • $400M impact to 2017 earnings                                                |
| **Merck**      | • Cumulative $590M 2017 impact  
                  • Forecasting another $200M adverse impact to sales in 2018          |
| **CHERTOFF**   | • Certain customers determined to defer or cancel new contracts  
                  • Some customers require Equifax to maintain ISO 27001 certification.  
                  Due to the 2017 cybersecurity incident, certain ISO certifications  
                  have been suspended.                                               |
| **Corporation**| • Impact was “primarily from loss of revenue due to decreased shipments” plus  
                  remediation costs.  
                  • While critical operational systems have been fully restored, “not  
                  all customers are shipping at pre-attack volume levels.”         |
| **Merck**      | • $260 million unfavorable sales impact based on an inability to fulfill orders  
                  in certain markets.  
                  • Merck ultimately had to borrow doses of HPV vaccine from U.S. CDC  
                  Pediatric Vaccine Stockpile.                                       |
What makes this so hard? Six implementation risks to consider

Even well-resourced programs can fail to consider these risks

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaps in Inherent Risk Understanding</td>
<td>Problems occur where the assessment of risk does not account for critical assets and how changing business, technology and threat drivers impact an enterprise risk profile.</td>
</tr>
<tr>
<td>Gaps in Planning &amp; Preparedness</td>
<td>When incidents occur, responders and victim organizations often identify gaps in preparedness that – had they been addressed – could have substantially mitigated the extent of damage.</td>
</tr>
<tr>
<td>Operational Burdens</td>
<td>Tools and technologies generate a high volume of security data (e.g., false alerts, large numbers of vulnerabilities, etc.)</td>
</tr>
<tr>
<td>Dependencies on IT Staff &amp; Technology</td>
<td>Implementation of security controls can require varying levels of IT staff support – the program can be impacted without right-sized IT resources. Legacy IT infrastructure adds additional risk.</td>
</tr>
<tr>
<td>Lack of Stakeholder Alignment</td>
<td>Business and IT leaders play a key role in advancing a security program. Without education and cultural change, the program may be impacted by lack of buy-in. Users are first line of defense – user education &amp; awareness is key.</td>
</tr>
<tr>
<td>Lack of Control Transparency</td>
<td>Without meaningful program evaluation, controls can decay over time, engendering a false sense of security. Pen test and audit reports can be confusing and lack meaningful risk context.</td>
</tr>
</tbody>
</table>
For more information...

Adam Isles
info@chertoffgroup.com
(202) 522-5280