Cybersecurity and the Evolving Role of Enterprise Risk Management

David Kidd
United Parcel Service
March 20, 2015
Agenda

• Risk Management / Enterprise Risk Management
• Legislative Landscape
• Cybersecurity / Privacy and Data Protection Trends
• ERM Process and Tools
Notable Breaches

Cybersecurity — is the protection of valuable intellectual property and business information in digital form against theft and misuse—is an increasingly critical management issue. The US government has identified cybersecurity as “one of the most serious economic and national security challenges we face as a nation.”

Source: Barack Obama, “Remarks by the President on securing our nation’s cyber infrastructure,” The White House, Washington, DC, May 29, 2009
Despite years of effort, and tens of billions of dollars spent annually, the global economy is still not sufficiently protected against cyberattacks — and it is getting worse. The risk of cyberattacks could materially slow the pace of technology and business innovation with as much as $3 trillion in aggregate impact.

Enterprise-technology executives agree on the seven practices they must put in place to improve their resilience in the face of cyberattacks; even so, most technology executives gave their institutions low scores in making the required changes.

Given the cross-functional, high-stakes nature of cybersecurity, it is a CEO-level issue, and progress toward cyber resiliency can only be achieved with active engagement from the senior leaders of public and private institutions.

Risk Management

(Traditional) Risk Management
The technique of assessing, minimizing, and/or offsetting a potential loss through the use of insurance or other measure

- Home owners/Renters Insurance/Life Insurance/Savings
- Fuel Prices – Supplier contracts / Options (Buy & Sell)
- Asset Protection – Traditional Insurance
- Portfolio/Fund – Treasury notes, fixed income, indexes, stocks
- Data Breach – Cyber-Security Insurance

EXAMPLE –

Empirical Analysis / Quantitative
Minimum age to rent a car: 25
• 18-20 $68 per day surcharge
• 21-25 $28 per day surcharge
We Rent Cars to Minors!
Enterprise Risk Management

Enterprise Risk Management dates back to the 1960’s
• Professors Robert Mehr and Bob Hedges
• First textbook “Risk Management and the Business Enterprise”

“Risks should be managed in a comprehensive manner, and not simply insured”

Objective: To maximize the productive efficiency of the enterprise
Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Enterprise Risk Management

Process used by organizations to identify and manage risks and seize opportunities related to the achievement of company objectives.

EXAMPLE –
- Geopolitical – Emerging/Frontier Markets
- Mergers/Acquisitions – Capitalize on synergies/Culture
- Work Stoppage – Labor Agreements (Union Contracts)
- Financial – FX, Interest Rates, Commodity Prices, Fraud

Risk and Opportunity
Legislative Landscape
Accounting Scandals

Legislative Landscape

ENRON
HEALTHSOUTH
ARTHUR ANDERSEN
GLOBAL CROSSING
WORLDCOM
TYCO
ADELPHIA
Fiduciary Failure. The Enron Board of Directors failed to safeguard Enron shareholders and contributed to the collapse of the seventh largest public company in the United States, by allowing Enron to engage in high risk accounting, inappropriate conflict of interest transactions, extensive undisclosed off-the-books activities, and excessive executive compensation. The Board witnessed numerous indications of questionable practices by Enron management over several years, but chose to ignore them to the detriment of Enron shareholders, employees and business associates.

High Risk Accounting.

Inappropriate Conflicts of Interest.

Despite clear conflicts of interest, the Enron Board of Directors approved an unprecedented arrangement allowing Enron's Chief Financial Officer to establish and operate the LJM private equity funds which transacted business with Enron and profited at Enron's expense. The Board exercised inadequate oversight of LJM transaction and compensation controls and failed to protect Enron shareholders from unfair dealing.

Extensive Undisclosed Off-the-Books Activity.

The Enron Board of Directors knowingly allowed Enron to conduct billions of dollars in off-the-books activity to make its financial condition appear better than it was and failed to ensure adequate public disclosure of material off-the-books liabilities that contributed to Enron's collapse.

Excessive Compensation.

The Enron Board of Directors approved excessive compensation for company executives, failed to monitor the cumulative cash drain caused by Enron's 2000 annual bonus and performance unit plans, and failed to monitor or halt abuse by Board Chairman and Chief Executive Officer Kenneth Lay of a company-financed, multi-million dollar, personal credit line.

Lack of Independence.

The independence of the Enron Board of Directors was compromised by financial ties between the company and certain Board members. The Board also failed to ensure the independence of the company's auditor, allowing Andersen to provide internal audit and consulting services while serving as Enron's outside auditor.
Legislative Landscape

Global Financial Crisis
Without a doubt, the recent financial crisis has tested companies and their boards in ways not seen in many decades and has had a profound impact on corporate governance and risk management. Indeed, one group of institutional investors with $9.5 trillion in assets under management, has claimed, “It is now widely agreed that corporate governance failings were not the only cause of the crisis but they were highly significant, above all because boards failed to understand and manage risk and tolerated perverse incentives.”
Executive Order – 13636 / February 19, 2013
Improving Critical Infrastructure Cybersecurity

Background
The Department of Homeland Security (DHS) leads the Federal government’s efforts to secure our Nation’s critical infrastructure by working with owners and operators to prepare for, prevent, mitigate, and respond to threats. While DHS plays a central role, the Department cannot do this work alone. Public private partnerships are essential. It is through partnerships where the Department continues to see new value and positive impact in mitigating and rapidly responding to crises.

Facing threats to our Nation from cyber attacks that could disrupt our power, water, communication and other critical systems, the President issued the Executive Order (EO) on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience. These policies reinforce the need for holistic thinking about security and risk management. Implementation of the EO and PPD will drive action toward system and network security and resiliency, and will also enhance the efficiency and effectiveness of the U.S. government’s work to secure critical infrastructure and make it more resilient.

World Economic Forum and McKinsey & Company

1. Prioritize information assets based on business risks
2. Provide differentiated protection based on importance of assets
3. Deeply integrate security into the technology environment to drive scalability
4. Deploy active defenses to uncover attacks proactively
5. Test continuously to improve incident response
6. Enlist frontline personnel to help them understand the value of information assets

7. Integrate cyberresistance into enterprise-wide risk-management and governance processes

The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.
(2011) If we fail to protect the security of personal information about our guests and team members, we could be subject to costly government enforcement actions or private litigation and our reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests and team members. If we experience a data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of our credit card products, decline to use our pharmacy services, or stop shopping at our stores or Target.com altogether. The loss of confidence from a data security breach involving team members could hurt our reputation and cause team member recruiting and retention challenges.

(2012) If our efforts to protect the security of personal information about our guests and team members are unsuccessful, we could be subject to costly government enforcement actions and private litigation and our reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests and team members. We have a program in place to detect and respond to data security incidents. To date, all incidents we have experienced have been insignificant. If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.
The data breach we experienced in 2013 has resulted in government inquiries and private litigation, and if our efforts to protect the security of information about our guests and team members are unsuccessful, future issues may result in additional costly government enforcement actions and private litigation and our sales and reputation could suffer.

The nature of our business involves the receipt and storage of information about our guests and team members. We have a program in place to detect and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security. Unauthorized parties may also attempt to gain access to our systems or facilities through fraud, trickery or other forms of deceiving our team members, contractors and temporary staff. Until the fourth quarter of 2013, all incidents we experienced were insignificant. The Data Breach we experienced was significant and went undetected for several weeks. We experienced weaker than expected U.S. Segment sales immediately following the announcement of the Data Breach, and we are currently facing more than 80 civil lawsuits filed on behalf of guests, payment card issuing banks and shareholders. In addition, state and federal agencies, including State Attorneys General, the Federal Trade Commission and the SEC, are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. Those claims and investigations may have an adverse effect on how we operate our business and our results of operations.

If we experience additional significant data security breaches or fail to detect and appropriately respond to significant data security breaches, we could be exposed to additional government enforcement actions and private litigation. In addition, our guests could further lose confidence in our ability to protect their information, which could cause them to discontinue using our REDcards or pharmacy services, or stop shopping with us altogether.
Target shareholder lawsuit—Case number 14-cv-14-cv-203—alleging Target’s board members and directors breached their fiduciary duties to the company by failing “to maintain proper internal controls” related to data security and misleading affected consumers about the scope of the breach after it occurred. That complaint alleges Target was damaged by having to pay costs associated with the data breach, including expending money for credit monitoring services for affected customers, causing Target “to be exposed to millions of dollars of potential liability in class-action lawsuits,” and through “substantial damage” to “the company’s sales during the 2013 holiday season, its market capitalization, goodwill, consumer confidence and brand trust.”
Cybersecurity / Privacy and Data Protection Trends
# Top 5 Increasing Risks

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Type of Risk</th>
<th>2015</th>
<th>2014</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our organization may not be sufficiently prepared to manage an unexpected crisis</td>
<td>Strategic</td>
<td>5.34</td>
<td>4.83</td>
<td>0.51</td>
</tr>
<tr>
<td>significantly impacting our reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inability to utilize data analytics and &quot;big data&quot; to achieve market intelligence</td>
<td>Operational</td>
<td>4.99</td>
<td>4.48</td>
<td>0.51</td>
</tr>
<tr>
<td>and increase productivity and efficiency may significantly affect our management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of core operations and strategic plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our organization may not be sufficiently prepared to manage cyberthreats that</td>
<td>Operational</td>
<td>5.70</td>
<td>5.26</td>
<td>0.44</td>
</tr>
<tr>
<td>have the potential to significantly disrupt core operations and/or damage our</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>brand</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our existing operations may not be able to meet performance expectations related</td>
<td>Operational</td>
<td>5.17</td>
<td>4.88</td>
<td>0.29</td>
</tr>
<tr>
<td>to quality, time to market, cost and innovation as well as our competitors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rapid speed of disruptive innovations and/or new technologies within the industry</td>
<td>Strategic</td>
<td>5.16</td>
<td>4.87</td>
<td>0.29</td>
</tr>
<tr>
<td>may outpace our organization's ability to compete and/or manage the risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>appropriately, without making significant changes to our operating model</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: NC State / Protiviti "Executive Perspectives on Top Risks for 2015"
Cybersecurity / Privacy and Data Protection Trends

Revenues $10 Billion or Greater

Source: NC State / Protiviti "Executive Perspectives on Top Risks for 2015"
Top Five – 2015 Information Security Trends

1. Cybercrime
2. Privacy and Regulation
3. Threats From Third-Party Providers
4. BYOx Trends in the Workplace
5. Engagement With Your People

Cybersecurity / Privacy and Data Protection Trends

Cybersecurity Oversight and Breach Response

- Establish rules of engagement between the board and management
- Pay attention to your initial response: how you start impacts how you finish
- Ensure the company is developing relationships with law enforcement

Recommendations for Directors to Follow

- Develop a high-level understanding of cyber-risks facing the company through briefings from senior management and others;
- Consider retaining outside consultants to evaluate the company’s security risk management;
- Ensure that the company has at least one committee that is responsible for overseeing and understanding cybersecurity issues, controls and procedures;
- Ensure that the vendors the company retains have adequate security measures in place to protect data and that there are sufficient contractual clauses between the company and the vendor regarding such security;
- Facilitate a culture that views cybersecurity as a business issue that all employees should understand and participate in. As part of that, companies should consider employee training and awareness programs;
- Include a cyber-expert on the company’s board of directors or receive regulator reports from a cybersecurity expert that are discussed at board meetings;
- Ensure the company has an updated plan to respond to a cybersecurity attack, should it experience one. As part of that, senior management should become familiar with the legal and contractual requirements to determine what steps they would be required to take if the company fell victim to a data breach;
- Ensure that the applicable directors and officers’ insurance covers data breach lawsuits, and
- Directors may consider the guidance provided by the Cybersecurity Framework released in February by the National Institute of Standards and Technology in response to U.S. President Barack Obama’s Executive Order 13636, which was intended to be used by companies to create a cybersecurity program.
ERM Process and Tools
Attributes of an Effective ERM Program

Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity’s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.

Event Identification – Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.

Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.

Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.