Cybersecurity for the CFO: Risks, Challenges, and Opportunities

Henry Raduege, Lieutenant General (USAF Ret.)
Director and Chairman, Deloitte Center for Cyber Innovation
Deloitte LLP

Kelly Bissell
Principal, Security and Privacy
Deloitte & Touche LLP
Video
A Company Like Yours
What is new with cybersecurity?

The business and IT environment is changing
• New business models – cloud, mobile
• Enterprise IT environment disrupted – BYOD and “rogue IT”
• Regulatory changes with SEC rules, state and country laws, industry regulation, emerging NIST standards, EU, and more

Leading to new, persistent, evolving risks
• More frequent, sophisticated, and malicious attacks
• Wide range of motives: economic, campaigns, hactivists
• Hackers already inside the organization
• Data easily available and it’s money
• C-suite, board, and key staff are sitting targets

Clients are struggling to keep pace
• Risks are evolving faster than clients can react
• Need to transform how they think about cybersecurity
• Companies large and small do not have the skills in house
• Greater need for comprehensive, enterprise solutions
• Boards and management are struggling on how to measure cyber risk
The threat landscape has changed

And so must you

The Adversary

- Well resourced, even nation-state-sponsored, multiyear campaigns
- Highly organized, capable, professional, and able to innovate faster than you

The Tactics

- No longer “smash and grab” but focused on maintaining a presence for years, operating below the security radar of the victim organization
- Classic security controls (firewalls, antivirus, IDS/IPS, etc.) are increasingly less effective as attackers employ innovative techniques to evade them
- They are not just after credit card data, they are after what makes you competitive as an organization

The Outcomes

- Theft of IP, marketing strategies, R&D information, customer data, etc., subsequent loss of revenue, negative impact to brand, loss of competitive positioning, loss in shareholder value, and regulatory impacts
- High cost of investigation/remediation, fraud, potential litigation, fines, etc.
- CEOs are worried, boards are asking tough questions, investors are uneasy, and customers are increasingly concerned with the safety of their information
How are attacks occurring across the market?

It is important for all employees, contractors, and suppliers to be aware of how bad guys target you for carrying out well-planned attacks and what it could mean to our businesses.
### By the numbers: 621 breaches reported in 2012*

In the Ponemon Institute’s 2012 study, data breach incidents cost U.S. companies an average of $194 per compromised customer record. The per-incident costs averaged $5.5 million, with the least breach reported being $750k.

<table>
<thead>
<tr>
<th>Who found the incident?</th>
<th>Who is behind the incidents?</th>
<th>How do incidents occur?</th>
</tr>
</thead>
<tbody>
<tr>
<td>69% discovered by outsider</td>
<td>70% of IP cases were insiders</td>
<td>76% weak or stolen credentials</td>
</tr>
<tr>
<td>9% discovered by customer</td>
<td>48% were caused by insiders</td>
<td>75% opportunistic not targeted</td>
</tr>
<tr>
<td>11% implicated business partners</td>
<td>11% implicated business partners</td>
<td>38% used malware</td>
</tr>
<tr>
<td>27% involved multiple parties</td>
<td>27% involved multiple parties</td>
<td>41% rogue hardware</td>
</tr>
<tr>
<td>2% intrusion detection system</td>
<td>0% data stolen in transit</td>
<td>19% by state actors (of these 95% used phishing)</td>
</tr>
</tbody>
</table>

Attacks are getting more frequent, opportunistic, and sophisticated.

How do they attack us?

*Attack methodology*

It is important for all employees, contractors, and suppliers to be aware of how bad guys target you for carrying out well-planned attacks.

**Attack sequence**

1. Open source intelligence collection
2. Intelligence analysis and review
3. Attack planning and target selection
4. Attack execution

**Goals**
- Denial of service
- PHI and identity theft
- Espionage
- System and network access

**Common Attack Vectors**
- M&A data
- Hedge positions
- Investment client data
- Pre-regulatory filings
- DDoS and hactivism
- Employee PII data
- Broker accounts
- Financial information
- Medical device access
- System access

- Peer-to-peer networks
- Search engines
- Social networking
- Job sites
- Understand operations
- Understand technology used
- Understand supply chain and business partners
- Research available exploits
- Target information of value
- Target systems
- Target employees/non-employees
- Anonymization
- Obfuscation
- Schedule

**Attack sequence**

**Goals**
- Denial of service
- PHI and identity theft
- Espionage
- System and network access

**Common Attack Vectors**
- M&A data
- Hedge positions
- Investment client data
- Pre-regulatory filings
- DDoS and hactivism
- Employee PII data
- Broker accounts
- Financial information
- Medical device access
- System access
Despite more complications, security and privacy investments by companies in some industries fall behind others.

IT Security Spend per Employee by Sector/Industry

<table>
<thead>
<tr>
<th>Sector/Industry</th>
<th>IT Security Spend per Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Publishing</td>
<td>$1,152</td>
</tr>
<tr>
<td>Government-NW/Intl</td>
<td>$1,100</td>
</tr>
<tr>
<td>Professional Services</td>
<td>$889</td>
</tr>
<tr>
<td>Insurance</td>
<td>$761</td>
</tr>
<tr>
<td>Banking/FSI</td>
<td>$400</td>
</tr>
<tr>
<td>Health Care Providers</td>
<td>$191</td>
</tr>
</tbody>
</table>

IT Security Spend as a Percent of Total IT Spend by Sector/Industry

<table>
<thead>
<tr>
<th>Sector/Industry</th>
<th>IT Security Spend as a Percent of Total IT Spend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Publishing</td>
<td>11%</td>
</tr>
<tr>
<td>Government-NW/Intl</td>
<td>11%</td>
</tr>
<tr>
<td>Professional Services</td>
<td>10%</td>
</tr>
<tr>
<td>Insurance</td>
<td>8%</td>
</tr>
<tr>
<td>Banking/FSI</td>
<td>6%</td>
</tr>
<tr>
<td>Health Care Providers</td>
<td>4%</td>
</tr>
</tbody>
</table>

The increasing risk gap

Information security risks increase as the industry transforms

Trends in the market

- Proliferation of data through the use of mobile devices
- Excessive access rights and management of privileged accounts
- Externalization and sharing of data with individuals, organizations, etc.
- Move to cloud-based solutions (salesforce.com; Workday, SaaS, PaaS, IaaS)
- Advanced persistent threats and other advanced cyber attacks (hacking as a business; cyber espionage)
- The Affordable Care Act of 2010 presents the need for strategic planning due to its complexity
- Shortened product development life cycles and rush to market for drugs and medical devices
- Genetic testing ties patient identities to drug profiles and presents greater need for PHI protection

The “risk gap” is growing faster than the industry is prepared to adapt to it.
Correlation between information security maturity and spending

Security spending will likely uptick during program evolution phases that focus on become aware of capability gaps and performing remediation activities. As the program enters operational sustainability, average security spending will decrease and capabilities will improve risk management and the organization’s security posture. Average security spend for 2011 as a percentage of IT spend is 5.2%*.

Information security and privacy programs are typically structured to support “run, grow, transform” activities, enabling capability maturity evolution, accountability, service delivery, and continuous improvement.

*Source: Gartner IT Key Metrics Data 2012: Key Information Security Measures: Multiyear
Cyber issues for CFOs
Cybersecurity – What do CFOs need to know?

Planning and Management

• How do we identify our critical assets and associated risks and vulnerabilities?
• How do we meet our critical infrastructure operations and regulatory requirements?
• What is our strategy and plan to protect our assets?
• How robust are our incident response and communication plans?

Assets

• How do we track what digital information is leaving our organization and where that information is going?
• How do we know who’s really logging into our network, and from where?
• How do we control what software is running on our devices?
• How do we limit the information we voluntarily make available to a cyber adversary?
Cybersecurity – Key considerations

Cybersecurity “tone at the top,” including awareness and responsibility
Importance of cybersecurity as a corporate priority
Clear governance, policy, and oversight

Critical risk and incident reports
Enterprise resilience
Top-level cybersecurity policies
Independent assessments of cybersecurity programs and controls

Promote Culture
Delegate
Assess and Approve
Oversee

Clear delineation of responsibilities and accountability for cybersecurity programs
Expectations and accountability of management
Adequacy of resources, funding, and focus

Periodic cybersecurity risk reviews
Regulatory compliance requirements
Cybersecurity due diligence and management for third parties
Cybersecurity audits and tests Metrics and reporting structure to filter critical risks

An effective cybersecurity program requires continuous and proactive engagement from CFOs, other executives, and directors
Cybersecurity recommendations for your organization

1. Evaluate the existing cyber incident response plan. Focus on the controls for the “crown jewels” and what we would do in the event of an incident. This team should include senior management from the line of leaders and administrative functions.

2. Work with your CIO to see how finance can help create a culture of security and privacy. Organizations can enhance their security stance by valuing cybersecurity and the protection of privacy and viewing. “Security begins with me.”

3. Require regular reports from senior management on privacy and security risks, based not on project status but on key risk indicators.

4. Many times, security budgets take a backseat to other IT or business priorities and we find companies are not prepared to deal with risks and attacks. We suggest annual review of cybersecurity budgets.

5. Annually, reevaluate the use and need of cyber insurance.
Cybersecurity Executive Order and framework
For the stated goal of strengthening the resilience of critical infrastructure, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, on February 12, 2013.

The executive order calls for the development of a voluntary cybersecurity framework that provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk.

**Key objectives of the framework are:**

- Align cybersecurity practices, guidance, and standards with organizational strategy.

- Promote the consideration of cybersecurity risk as a priority similar to financial, safety, and operational risk, and when examining larger systemic risks inherent to the organization.
Cybersecurity framework program and our national critical infrastructure

Framework goal: To establish a voluntary program to support the adoption of the cybersecurity framework by owners and operators of critical infrastructure.

Currently, there are 16 industry sectors defined as critical infrastructure;

85% of critical infrastructure is in the private sector\(^1\)

Trends exposing industry to increased risk: interconnectedness of sectors, proliferation of exposure points, concentration of assets.

<table>
<thead>
<tr>
<th>Critical infrastructure sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture and Food</td>
</tr>
<tr>
<td>Dams</td>
</tr>
<tr>
<td>Information Technology</td>
</tr>
<tr>
<td>Banking and Financial Services</td>
</tr>
<tr>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Nuclear Reactors, Materials, and Waste</td>
</tr>
<tr>
<td>Chemical</td>
</tr>
<tr>
<td>Emergency Services</td>
</tr>
<tr>
<td>Transportation Systems</td>
</tr>
<tr>
<td>Commercial Facilities</td>
</tr>
<tr>
<td>Energy</td>
</tr>
<tr>
<td>Water and Wastewater Systems</td>
</tr>
<tr>
<td>Communications</td>
</tr>
<tr>
<td>Government Facilities</td>
</tr>
<tr>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td>Health Care and Public Health</td>
</tr>
</tbody>
</table>

Framework impact and questions to consider

The framework may impact your organization in several ways, including:

• Driving greater involvement by the board in overseeing cybersecurity risk.

• Potentially requiring organizations to build information-sharing mechanisms and protocols while protecting customer and employee privacy.

• Lack of adoption of the framework may lead to additional regulation for “critical infrastructure” sectors.

Take-away questions to consider for your organization in light of the framework:

• What are the current difficulties in implementing cybersecurity practices into your business?

• What are the types of questions you ask your management team to ensure that your organization is following best practices when managing cybersecurity risk?
This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2013 Deloitte Development LLC. All rights reserved.