Risk Intelligent Governance in the Age of Cyber Threats

Deloitte & Touche LLP
Raj Mehta, CISA, CISSP, CIPP
Partner

December 2013
The threat landscape is evolving…

Attack sophistication continues to outpace many organizations’ current capabilities.

<table>
<thead>
<tr>
<th>Unsophisticated attackers</th>
<th>Sophisticated attackers</th>
<th>Corporate espionage</th>
<th>State-sponsored attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations are under attack because they are on the internet</td>
<td>Organizations are under attack because they have information of value</td>
<td>Organizations are under attack because employees/third parties seek financial gain from selling their intellectual property (IP)</td>
<td>Organizations are targeted because of who they are, what they do, and the value of their IP</td>
</tr>
<tr>
<td>Organizations have lost time and money with attacks from hobbyists</td>
<td>Skimming and phishing losses show that organizations are an ongoing target</td>
<td>Loss of intellectual property, but more goes undetected</td>
<td>Most recent attacks show that this level of threat is real</td>
</tr>
</tbody>
</table>

Combined attack vectors
- Zero-day attacks
- External consultant stealing IP
- Hacktivism
- Customer data bought by governments

Rapid change in attack sophistication

Monetization
- Spear Phishing
- ZeuS trojan

Experimentation and notoriety
- Website vulnerability
- Search contest
- Website defacement
- Website malfunction
- Phishing
- Skimming

Copyright © 2013 Deloitte Development LLC. All rights reserved.
Cyber security threat landscape

The cybercrime landscape has evolved into a set of highly specialized criminal products and services that are able to target-specific organizations, regions, and customer profiles by using a sophisticated tools, which routinely evade present-day security controls.
So what is Cyber Security?
Cyber attack trends

Types of cyber attacks experienced by 56 benchmarked companies

- The percentage frequency defines a type of attack categories experienced.

- Viruses, worms, and Trojans: 100%
- Malware: 95%
- Botnets: 71%
- Web-based attacks: 64%
- Stolen devices: 46%
- Malicious code: 38%
- Malicious insiders: 38%
- Phising and social engineering: 38%
- Denial of service: 32%

Source: 2012 Cost of Cyber Crime Study: United States by Ponemon Institute
Many attacks are not “Advanced”

While the sophistication of attacks is growing, most breaches could still be easily prevented.

And while perpetrators are upping the ante — trying new techniques and leveraging far greater resources — less than 1% of the breaches in this year’s study used tactics rated as ‘high’ on the VERIS difficulty scale for initial compromise. In fact, 78% of the techniques we saw were in the ‘low’ or ‘very low’ categories (Figure 3). The barriers to entry for becoming a hacker are pretty low.

The simplicity of attacks doesn’t take anything away from their effectiveness or impact. Even well-known techniques can be used to devastating effect.

Videos

Advanced Example:

https://www.youtube.com/embed/l_XOrcBxy-E?rel=0
Using Social Engineering to Compromise a User

**Sequence of Fraud**

1) Miscreant profiles organization and chooses an employee target.
2) Miscreant finds a business relationship from profile data and decides to spoof an email.
3) Spoofed email is sent to target employee.
4) Target employee opens email and clicks on obfuscated malicious link.
5) Fraudulent web site installs malicious code on target employee workstation.
5a) Target employee logs into HR systems to enter Personally Identifiable Information.
6) User name and password for information system are sent to miscreant key logger server.
Common vulnerabilities

- Default credentials
- Misconfiguration of systems
- Limited protection of end-user devices (mobile phones, laptops)
- Unaware users
- Third parties/business partner weaknesses
- Defective applications, programs (lack of secure software development lifecycle) – especially web applications
- Lack of asset management
- Lack of event detection capability
- Ineffective patch management process
- Improper disposal
### Frameworks for Assessing Cyber Security

#### NIST Cybersecurity Framework (http://www.nist.gov/itl/cyberframework.cfm)

<table>
<thead>
<tr>
<th>MATURITY TARGET</th>
<th>Category</th>
<th>Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>0 (Partial)</td>
<td>1 (Risk Informed)</td>
</tr>
<tr>
<td><strong>IDENTIFY</strong></td>
<td>Asset Management</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>Blue</td>
</tr>
<tr>
<td><strong>PROTECT</strong></td>
<td>Access Control</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Awareness &amp; Training</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Information Protection</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Processes and Procedures</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>Blue</td>
</tr>
<tr>
<td><strong>DETECT</strong></td>
<td>Anomalies and Events</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>Blue</td>
</tr>
<tr>
<td><strong>RESPOND</strong></td>
<td>Response Planning</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>Blue</td>
</tr>
<tr>
<td><strong>RECOVERY</strong></td>
<td>Recovery Planning</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>Blue</td>
</tr>
</tbody>
</table>
SANS 20 Critical Security Controls - Version 4.1

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

http://www.sans.org/critical-security-controls/
Frameworks for Assessing Cyber Security (cont.)

- NIST 800-53
- Industry specific frameworks (like HITRUST, NERC CIP)
- ISO 27001/27002

Ultimately it does not matter what framework – there is only some many ways one secure an environment!
So where do you begin?

Understand what is the threat profile of the organization? Example questions to consider:

- Has there been trends in the industry sector in which the organization operates in, where the industry has been heavily targeted by Cyber Criminals, Hacktivists, etc.? [test: hearing from peers; seen in publications and articles; FBI feedback, etc.]

- Has the organization been targeted by Cyber Criminals, Hacktivists?

- Social Networking Chatter: Is the organization seeing some level of negative chatter (e.g., environmentalists, PETA, Anonymous, etc.)?
So where do you begin? (cont.)

• Global Footprint: Does the organization have global operations or limited to a specific geographical area (e.g., North America)?

• Assets: Does the organization have information or operational assets that have value and inherent risk from competitors and/or cyber criminals (e.g., highly valued intellectual property that gives the organization a competitive edge; lots of personal and medical information; highly coveted business plans (like bids for exploration), etc.)?

• Business Plan: Are there anticipated changes in the business environment that could impact any of the questions above (e.g., M&A transaction that adds an industry sector that increases the threat visibility)?
Threat Actors

Insiders:
- Employees
- Contractors
- Third-Party Providers

External:
- Hackers
- Activists/Hacktivists
- Competitors
- Nations State

Perceived Level of Concern
- High
- Medium
- Low
Digital Assets

Things that can impact Competitiveness &/or Reputation:

• Business Plans & Strategy (e.g., Merger & Acquisition)
• Pricing
• Customer Lists
• Credit Cards
• Employee and Contractor Personal Information (e.g., Identity Theft) - PII

Things that can impact Operations &/or Reputation:

• System Availability (e.g., bring down system(s) and impacting operations)
# Threat Vectors

<table>
<thead>
<tr>
<th>Threat Vector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>Internet has been one of the ways hackers and other “bad actors” that try to gain access into organizations, e.g., attacking web applications.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Social Engineering (e.g., through calling employees and/or sending “phishing emails”) is one of the current successful ways attackers try to gain access or foothold into the organization.</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Mobile devices such as laptops, USB drives, and PDAs (like iphone, ipads) contain sensitive information and are prone to loss / theft.</td>
</tr>
<tr>
<td>Supply Chain</td>
<td>Supply Chain includes third-parties who have system connections into our organization - “bad actors” can sometimes get a foothold into the organization through supply chain connections.</td>
</tr>
<tr>
<td>Social Media</td>
<td>Social Media such as Facebook can be leveraged to target employees for social engineering and/or employees posting sensitive information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perceived Level of Concern</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
</table>

Copyright © 2013 Deloitte Development LLC. All rights reserved.
So what does the threat profile tell you?
Next Steps

• Decide on a framework
• Leverage experienced resources
• Assess the people, process, and technology component of cyber security capabilities
• Understand the governance and visibility of security
Integrated security model – Key Areas
At the risk governance level, two strong indicators of maturity are:

- Extent of engagement between the board and executive management on cyber threat risk, and
- Sophistication of management’s approach to cyber threat risk metrics.

The risk infrastructure level, owned by executive management, is responsible for implementing and maintaining the people, process, and technology elements needed to make risk management “work.”

The risk ownership level, consisting of a company’s business units and supporting functions, is where many of a company’s actual risk management and monitoring activities occur.
Mature cyber threat risk management
Proactive and preemptive

The goal is to help your organization move its cyber threat risk management practices toward a more proactive, preemptive and mature approach.

Exploring cyber threat risk management with your board and executive team can help to:
• Yield value
• Generate productive dialogue with executives
• Be a springboard to greater engagement between board and management
Other Considerations

• Tools will not solve problems by themselves – there is no magic black box
• Rationalize tools and how effectively are they being used before spending more
• Security team should have a combination of technical, business, and risk acumen
• Security should have proper governance processes, applicable skillsets, connected, etc.
• There should be business oriented security reporting
10 steps to consider when moving toward more effective cyber threat risk governance

1. Keep the board informed
2. Recognize the value
3. Maintain C-level executive accountability
4. Enable, by providing sufficient resources
5. Require regular management reporting
6. Establish continuous monitoring
7. Engage internal audit for periodic assurance
8. Track and report business impact metrics
9. Keep up with legislation and regulations
10. Recognize effectiveness to elevate confidence
Contact info

Raj Mehta
Partner, Deloitte & Touche LLP
rmehta@deloitte.com
+1 713 982 2955
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation 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 shall not be responsible for any loss sustained by any person who relies on this presentation.