Cyber Security and Inside Threats: Turning Policies into Practices

Presented by
Ingrid Fredeen and Pamela Passman
Agenda

• The rise of cyber risks: The threat landscape
• Elements of an effective enterprise-wide cyber security program: Address people, process and technology
• Addressing insider threats: Mitigating risks from employees, contractors and third parties
• Emerging trends: Assessing enterprise cyber security; training your workforce
• Cyber Compliance Training and Measurable Impact
• Q&A
The Center for Responsible Enterprise and Trade (CREATe.org), and its wholly-owned subsidiary, CREATe Compliance Inc: two entities with a mission to promote leading practices to protect IP and trade secrets, advance cyber security and prevent corruption.

Works with leading experts and organizations to develop best practice approaches, resources and tools

Focus: to effectively address corruption prevention, cyber security, trade secret and IP protection

Enabling enterprises to assess, build and strengthen programs via CREATe Leading Practices services:

- CREATe Leading Practices for Cybersecurity
- CREATe Leading Practices for Anti-Corruption
- CREATe Leading Practices for Intellectual Property Protection
- CREATe Leading Practices for Trade Secret Protection
Cyber Security: The Threat Landscape
Who at your organization is the primary owner of cyber risk?

- IT
- Human Resources
- Ethics and Compliance
- Legal Department
- CRO/Enterprise Risk Management Owner
- Multiple Groups Own It
- No One Really Owns It
- Other
Cyber Breaches are Multiplying

“Data breaches in 2016 exposed everything from social security numbers to user account log-in names and passwords.

Attacks known as phishing, in which an employee is tricked into clicking an e-mailed link to give hackers access to a corporate network, accounted for about 56 percent of all breaches last year, according to the center. That’s up from 38 percent in 2015.”


• Employees remain the most cited source of compromise
  - Current Employees: 34%
  - Former Employees: 29%

• Incidents attributed to business partners climbed to 22% (from 18%)

--PwC 2016 State of Information Security Survey
# Cyber Risk Threat Actors

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Objectives</th>
<th>Methods</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nation States</strong></td>
<td>Military technology, help national companies</td>
<td>Blunt force hacking</td>
<td>Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social Engineering</td>
<td>People</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trojan Horse</td>
<td>Technology</td>
</tr>
<tr>
<td><strong>Malicious Insiders</strong></td>
<td>Competitive advantage, financial gain, national goals</td>
<td>Spear phishing</td>
<td></td>
</tr>
<tr>
<td><strong>Competitors</strong></td>
<td>Competitive advantage</td>
<td>Watering Hole Exploits</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td><strong>Transnational Organized Crime</strong></td>
<td>Financial gain</td>
<td>Co-opted Credentials</td>
<td></td>
</tr>
<tr>
<td><strong>Hacktivists</strong></td>
<td>Political/social goals</td>
<td>Physical/Non-technical</td>
<td></td>
</tr>
</tbody>
</table>

Source: CREATe.org – PwC Report: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential thefts, February 2014
Contractual Requirements are on the Rise

**Government contracts** now regularly require:

- Particular cyber security controls
- Compliance with particular standards
- Risk assessment and risk management
- Reporting and remediation of breaches

**Commercial contract requirements** are also on the increase: financial services, healthcare, defense, ICT, etc.
Managing Cyber Risks

AN ENTERPRISE-WISE APPROACH TO CYBER SECURITY
Cyber Security: Increasingly Complex

Key Takeaway:
Need for Increased Cyber Security Protections
How Companies Address Cyber Security

Enterprise Risk Management
• Managing potential financial, operational and reputational risks

Regulatory - Compliance
• Meeting rising regulatory and compliance requirements

Information Technology
• Defending the perimeter; bolstering technical defenses

Trend: Momentum for the NIST Cyber Security Framework
• Voluntary, risk-management approach; way to measure and assess gaps
• Increasingly a reference for contracts and compliance
• Cross-references leading standards and guidelines
“By 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from 30% in 2015.”


“The Framework creates a common language for the discussion of cybersecurity issues that can facilitate internal and external collaboration.”

“Organizations that adopt the Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations.”
Bringing Consistency to Cyber Security Efforts

**OVERVIEW OF NIST CYBER SECURITY FRAMEWORK**

<table>
<thead>
<tr>
<th>IDENTIFY (ID)</th>
<th>PROTECT (PR)</th>
<th>DETECT (DE)</th>
<th>RESPOND (RS)</th>
<th>RECOVER (RC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>Access Control</td>
<td>Anomalies and Events</td>
<td>Recovery Planning</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td>Business Environment</td>
<td>Awareness and Training</td>
<td>Security Continuous Monitoring</td>
<td>Communications</td>
<td>Improvements</td>
</tr>
<tr>
<td>Governance</td>
<td>Data Security</td>
<td>Detection Processes</td>
<td>Analysis</td>
<td>Improvements</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Information Protection Processes and Procedures</td>
<td></td>
<td>Mitigation</td>
<td>Communications</td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Strengths**
- Common framework
- Shared terminology
- Target profiles

**Challenges to Users**
- Defining scope of assessment
- Calibration of results – benchmarking maturity
- Methods of verification
- Operationalizing results
- Scalability to use with third parties
Training Your Employees and Other Insiders
Which statement best describes your organization’s approach to cyber security training?

- We train on both information security and personal behavior related to reducing cyber risks
- Our training focuses on information security practices only
- We don’t currently provide cyber security training in our organization
- I don’t know
- Other
How often is your organization training employees on cyber security? [Select All That Apply]

- During onboarding
- Once a year
- Multiple times a year
- I don’t know
- Other [Please Chat]
Not All Training is Created Equal

• If you want to:
  – Drive a culture of cyber-awareness, understanding and security best practices
  – Inspire ethical employee behavior and reduce cynicism
  – Protect and defend against carelessness, malicious activity, and poor practices

Your training must be engaging and focus on the employee behaviors that can change your risk profile
Cyber Security Training Tools Will Help Accelerate Culture Shift

CYBER SECURITY: PROTECT AND PREVENT & MANAGE AND LEAD
Cyber Security Expertise

• We start with a focus on the human component of cyber risk & most pressing risk areas

• We create engaging content in close collaboration with leading industry experts

• We make the content relevant and engaging with professional actors and scriptwriters

• We produce unique and compelling video scenarios and interactivities
Cyber Security Expertise

We’ve created a solution that:

• Engages your learners
• Raises awareness
• Drives behavior changes
• Helps build a culture of security and resilience
• Help prevent future mistakes
• Creates a more cyber-secure environment
Measuring and Improving Your Cyber Security Approach
### Resource: CREATE › Leading Practices for Cyber Security

Aligns with the NIST Cyber Security Framework

An efficient way to assess cybersecurity at headquarters, business units, by location or function – or with key third parties

Robust reporting capabilities enabling teams to present the ‘state of cybersecurity’ to stakeholders

<table>
<thead>
<tr>
<th>1. Robust Assessment</th>
<th>2. Independent Verification</th>
<th>3. Improvement Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Q&amp;A:</td>
<td>CREATe expert evaluation:</td>
<td>Based on rating:</td>
</tr>
<tr>
<td>Measures maturity of</td>
<td>Questions to evaluate the</td>
<td>Improvement steps to</td>
</tr>
<tr>
<td>systems against the</td>
<td>program</td>
<td>move to next level</td>
</tr>
<tr>
<td>NIST Framework’s 98</td>
<td>Reviews documents</td>
<td>Benchmarking report</td>
</tr>
<tr>
<td>sub-categories of</td>
<td>Generates verified score</td>
<td></td>
</tr>
<tr>
<td>controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rates maturity on a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>scale from 1 to 5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bringing Consistency to Cyber Security Efforts

**OVERVIEW OF NIST CYBER SECURITY FRAMEWORK**

<table>
<thead>
<tr>
<th>IDENTIFY (ID)</th>
<th>PROTECT (PR)</th>
<th>DETECT (DE)</th>
<th>RESPOND (RS)</th>
<th>RECOVER (RC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>Access Control</td>
<td>Security Continuous Monitoring</td>
<td>Response Planning</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td>Business Environment</td>
<td>Awareness and Training</td>
<td>Detection Processes</td>
<td>Communications</td>
<td>Improvements</td>
</tr>
<tr>
<td>Governance</td>
<td>Data Security</td>
<td></td>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Information Protection</td>
<td></td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td>Processes and Procedures</td>
<td></td>
<td>Improvements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anomalies and Events</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Five Functions; 22 Categories and 98 Subcategories/Outcomes
  - One sentence control
  - Overlap on outcomes

• Covers “People, Process and Technology” but not in the manner that reporting is done by leaders in risk management and compliance

• Does not sufficiently address third party risk management

• 1 to 4 level of tiers not aligned to specific maturity levels
CREATe’s Approach to Operationalizing the NIST Cybersecurity Framework

**People & Process**

**Cyber Security Management Systems:**
- Policies, Procedures & Records
- Cyber Protection Team
- Risk
- Third Party Management
- Training
- Monitoring
- Corrective Actions
- Communication

**Technology**

**Cyber Security Capability Performance:**
- Vulnerability Management
- Cyber Resiliency
- Threat Management
- Identity & Access Management
- Event Management
- Incident Management
- Configuration Management
- Perimeter/Network Defense
- Data Security
How CREATe Gauges Maturity

ID.GV.1: Organizational information security policy is established.

1. **Comprehensive assessment** with answers that map to a 1-5 scale of maturity

2. **Independent verification** of answers and further examination of evidence of controls and business processes
Aligns with the NIST Cyber Security Framework

An efficient way to assess cyber security at headquarters, business units, by location or function – or with key third parties

Robust reporting capabilities enabling teams to present the ‘state of cyber security’ to stakeholders

1. Robust Assessment
   - Online Q&A: Measures maturity of systems against the NIST Framework’s 98 sub-categories of controls
   - Rates maturity on a scale from 1 to 5

2. Independent Verification
   - CREATe expert evaluation:
     - Questions to evaluate the program
     - Reviews documents
   - Generates verified score

3. Improvement Plan
   - Based on rating:
     - Improvement steps to move to next level
     - Benchmarking report
Resources From NAVEX Global and CREATe.org

- Toolkit: Cyber Security Awareness Kit
- Article: Compliance Role in Mitigating Cyber Mayhem
- CREATe Resources – Free Downloads Available at www.CREATe.org like:
  - Cyber Risk: Navigating the Rising Tide of Cyber Security Regulation
  - CREATe-PwC Report: Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats
  - Protecting Intellectual Property through Enterprise Risk Management
  - Addressing Corruption Risk through Enterprise Risk Management (ERM)
[Optional] I’d Like to Speak to NAVEX Global Expert About...

[Select All That Apply]

○ Schedule a guided tour of our Cyber Security training course

○ Discuss our full online training library

○ Speak to a CREATe Compliance expert about assessing and aligning your cyber security approach to the NIST framework, leading practices for cyber security or leading practices for protecting trade secrets and other confidential information

○ No thanks
Thank You