Right-Sizing a Cybersecurity Strategy

Pamela Passman
President and CEO
CREATe Compliance
Today’s Discussion:

Today’s complex cybersecurity environment:
- Multifaceted risk environment
- More sophisticated cyber threats
- Rising regulations
- Corporate governance

Early learning from the front lines
- Why companies manage cyber risk
- What is working and not working
- How to think about managing third party risk
- Who to involve

Opportunities for Enterprises to take a risk-based approach:
- NIST Cybersecurity Framework and CREATe Leading Practices for Cybersecurity

Opportunities for Small Companies to Get the Basics
CREATe Compliance works with enterprises to better manage internal and third party global risk for key issues – cybersecurity, intellectual property and trade secret protection, and anti-corruption.

CREATe Compliance’s services – CREATe Leading Practices – provide a practical and scalable way to measure, benchmark, improve and monitor compliance and risk programs:

• CREATe Leading Practices for Cybersecurity – Aligned to the NIST Cybersecurity Framework
• CREATe Leading Practices for Intellectual Property Protection
• CREATe Leading Practices for Trade Secret Protection
• CREATe Leading Practices for Anti-Corruption – Aligned to leading international guidance and the ISO 37001 Anti-Bribery Management Systems Standard
Complex Risk Environment
Top Risks for Corporations

Top 10 Risks:
• Rapid speed of **disruptive innovation**
• Corporate resistance to change
• Managing **cyber threats**
• Regulatory change and heightened **regulatory scrutiny**
• **Culture** may not encourage timely escalation of risk issues
• Ability to attract and retain **talent**
• Ensuring privacy/identity management and **information security**/system protection
• Economic conditions in markets where selling products/services
• Inability to utilize data analytics and big data
• Meeting performance expectations related to quality, time to market, cost, innovation and competition
Breaches: a Constant Today…and Tomorrow

Under Armour app users exposed to major data breach

As Atlanta Seeks To Restore Services, Ransomware Attacks Are On The Rise

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

Cyber espionage: China wants Japanese firms’ intellectual property

Cyber groups within China are targeting Japanese companies involved in heavy industry and national infrastructure as part of a multifaceted effort to create the Chinese strategic playbook.
# Cyber Risk Threat Landscape

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Objectives</th>
<th>Methods</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Insiders</td>
<td>Competitive advantage, financial gain, national goals</td>
<td>Blunt force hacking</td>
<td>People</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social Engineering</td>
<td>Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trojan Horse</td>
<td>Technology</td>
</tr>
<tr>
<td>Nation States</td>
<td>Military technology, help national companies</td>
<td>Spear phishing</td>
<td></td>
</tr>
<tr>
<td>Competitors</td>
<td>Competitive advantage</td>
<td>Watering Hole Exploits</td>
<td></td>
</tr>
<tr>
<td>Transnati’l Organized Crime</td>
<td>Financial gain</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Political/social goals</td>
<td>Co-opted Credentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical/Non-technical</td>
<td></td>
</tr>
</tbody>
</table>
“Domains” of Cyber Vulnerability
What’s Most at Risk?

What information matters most to your business, and what matters most to your adversaries? They may not be the same thing.

- Know what your company’s most valuable and sensitive information assets are and where they are located in the business ecosystem.
- Prioritize and allocate resources to effectively protect the “crown jewels” today and into the future.
- Know that your company may be targets as the “means to an end” – gaining information about or access to the systems of others.

Regulatory Environment

New, Expanded Regulation
- Financial, health, other critical infrastructure sectors
- Government procurement
  - DOD
  - Civilian
  - State and Local
- Securities regulation and enforcement
- Shareholder and customer lawsuits

Contractual Requirements
- Government bids
- Global value chain requirements
Questions from the Board

How would you answer these questions?

- Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
- What are the company’s cybersecurity risks?
- How is the company managing these risks?
- Who are our likely adversaries?
- How will we know if we have been breached? How will we find out?
- Do we have a systematic framework, such as the NIST Cybersecurity Framework, in place to address cybersecurity and assure adequate cybersecurity hygiene?
Early Learning from the Front Lines
Why a Company Implements an Information Security Management System

As part of an enterprise risk management strategy - reviewed by senior management and/or the Board of Directors

As required by “critical infrastructure” laws and regulations

To meet customer contractual requirements related to cybersecurity and the protection of specific data

As required by a cybersecurity insurance policy

As required by government procurement regulations for providers of products/services, and in some cases for supply chain partners
Early Days for Managing Cyber Risk

Organizations are weak at risk assessment
- What are the key threats?
- What are the assets?
- Where are they located?
- Who has access?

Silos still dominate
- Cybersecurity viewed as IT issue
- Different metrics and terminology
- A cross-functional approach typically not employed

Lack of understanding of the cybersecurity controls in place
- Depth, breadth and maturity of controls
- How approach aligns with the NIST Framework and other guidelines

Third party risks are high; engagement is low
- Most typical: ‘contractual’ approach - yet no insight into actual practices
- Lack of monitoring to ensure obligations are being met
Cybersecurity in Value Chains

Where we are Now
- Assessing cybersecurity risk of third parties is at an early stage

Why it is Important
- Digital supply chain means companies are interdependent and critical information is shared

Where we are Headed
- Independent verification of third parties will be required - not practical to rely on self-assessments

Ongoing Challenges
- Verification: how to make it scalable, yet gain credible information to achieve verified trust
## Embedding Cybersecurity into Business

### Board Oversight

### Executive Level Decision-Making

### Cross-Functional and Incident Response Team

<table>
<thead>
<tr>
<th>Legal</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Compliance Officer (CCO)</td>
<td>Communications/PR</td>
</tr>
<tr>
<td>Risk</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>Supply Chain</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>Customer Support</td>
</tr>
<tr>
<td></td>
<td>Human Resources</td>
</tr>
</tbody>
</table>

### Stakeholders

<table>
<thead>
<tr>
<th>Employees</th>
<th>Shareholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers</td>
<td>Regulatory agencies</td>
</tr>
<tr>
<td>Vendors/Suppliers</td>
<td>Law enforcement</td>
</tr>
<tr>
<td>Partners</td>
<td>Media (formal and informal)</td>
</tr>
<tr>
<td>Lenders</td>
<td></td>
</tr>
</tbody>
</table>
A Risk-Based Approach: The NIST Cybersecurity Framework
Approaches Companies Take Today: Align with Leading Guidance

**Goal:** Demonstrate that a company has a risk and information security management system in place

**Two leading approaches:**

- ISO 27001 (certification)
- NIST Cybersecurity Framework (voluntary approach)

**NIST Cybersecurity Framework enables you to:**

- Measure the maturity of an information security system against the standards referenced and processes identified in the framework
- Choose a Target Profile – a level of maturity aligned to an organization’s risk profile
- Determine gaps between system maturity and its Target Profile for each control in the Framework, creating an actionable plan for maturing its practices
The NIST Cybersecurity Framework

“By 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from 30% in 2015.”

Gartner: Best Practices in Implementing the NIST Cybersecurity Framework
January, 21, 2016

“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.”
Elements of the NIST Framework

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

Five main Functions

22 Categories & 98 Subcategories of Controls

Providing an analysis of technical and management capabilities
Another View of the NIST Framework

People & Process

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

Technology

Cybersecurity Capability Performance:
- Vulnerability Management
- Cyber Resiliency
- Threat Management
- Identity & Access Management
- Event Management
- Incident Management
- Configuration Management
- Perimeter/Network Defense
- Communication
- Data Security
CREATe Leading Practices for Cybersecurity
Enhancing use of the NIST Framework

• Enable organizations to operationalize the NIST Framework internally & with third parties

• Develop a calibrated maturity scale
  - Descriptive answers describing maturity for each sub-category

• Provide guidance to clarify intent and definitions of sub-categories

• Offer an alternative view for taking the assessment or viewing results
  - Operationally meaningful
  - Link to information security budget
  - Informative for reporting and decision-making
Assessment Aligned to the NIST Framework

- **Five-level maturity scale** aligned to the NIST Cybersecurity Framework’s 98 controls
- **Enables calibration and identification of gaps**
- **Answers and guidance ensure consistent benchmarking** across an enterprise and among third parties
Easy Access to References and Documentation

- Enables references to standards and guidance included in NIST Cybersecurity Framework
- Uploading of documentation for record-keeping and verification
- Subsequent assessments can leverage prior data and documentation
Report Options for Different Audiences

- Ability to pull data and develop reports to share maturity of programs to diverse audiences
- Different views of data based on requirements
Two Views for NIST Framework Controls
CREATe Compliance View
Operationalizing the NIST Framework

**People & Process**

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

**Technology**

Cybersecurity Capability Performance:
- Vulnerability Management
- Cyber Resiliency
- Threat Management
- Identity & Access Management
- Event Management
- Incident Management
- Configuration Management
- Perimeter/Network Defense
- Communication
- Data Security
The Basics for Small Companies
Insights into SMB Cybersecurity

Figure 8. What challenges keep your IT security posture from being fully effective?

- Insufficient personnel: 67%
- Insufficient budget: 54%
- Insufficient enabling security technologies: 44%
- No understanding how to protect against cyber attacks: 39%
- Lack of in-house expertise: 36%
- Not a priority issue: 32%
- Management does not see cyber attacks as a significant risk: 11%
- Lack of collaboration with other functions: 11%
- Lack of clear leadership: 6%

Source: Ponemon Institute - 2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)
The Cyber Readiness Institute is a non-profit organization convening senior leaders of global companies and their value chain partners from across sectors to share cybersecurity best practices and to develop content and tools to improve the cyber readiness of small and medium-sized businesses.
This Autumn, the Cyber Readiness will Launch:
A Self-Driven Cyber Readiness Program

- Enabling small and medium-sized companies to be more cyber resilient
- Addressing top risks – phishing, patching, identity authentication, and USBs – and providing guidance for going to the cloud
- Providing a web-based guided set of content, resources, and tools
Get Involved!

• Large companies: Become a member
• Small and medium-sized companies: join the pilot program
• Academics and experts: become an advisor

Learn more at www.CyberReadinessInstitute.org/membership
Top Takeaways

Be Aware of Increasingly Complex Risks:
➢ Cyber threats are increasingly sophisticated and targeting corporate assets; determine what is most important, where it is located and who has access

Take Steps to Avoid Common Areas of Weakness:
➢ Understand your risks and put controls in place; break cybersecurity out of the IT silo

Align with Leading Guidance:
➢ Map to the best-practice approach of the NIST Cybersecurity Framework and standards

Consider the Broader Value Chain:
➢ Put controls in place to protect the confidential information of your customers; determine whether your third parties have the capacity to protect your sensitive data

Right-size your Approach so it is Embedded in Your Business
➢ Get started, be consistent, measure and improve
THANK YOU

Pamela Passman – PPassman@CREATeCompliance.com
Aligns with the NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>1</th>
<th>Robust Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Q&amp;A:</td>
<td>Measures maturity of systems against the NIST Framework’s 98 sub-categories of controls</td>
</tr>
<tr>
<td></td>
<td>Rates maturity on a scale from 1 to 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Independent Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATe expert evaluation:</td>
<td>Review program</td>
</tr>
<tr>
<td></td>
<td>Check documents</td>
</tr>
<tr>
<td></td>
<td>Generate a verified score</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Improvement Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on rating:</td>
<td>Improvement steps to move to next level</td>
</tr>
<tr>
<td></td>
<td>Benchmarking report</td>
</tr>
</tbody>
</table>

CREATe Platform
Federal Contractor Cybersecurity Requirements
Map to NIST Framework and NIST Standards

NIST SPECIAL PUBLICATION (SP) 800-171 ("Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations")

- Applies to: Companies contracting with the US Department of Defense, and their subcontractors.
- Covers: Technical data and computer software with military or space application that is subject to government restrictions on access, use or disclosure.
- Requires: Self-certification of compliance with SP 800-171 organizational and technical security requirements for protecting such data.
- Organizational and Technical Controls: SP 800-171 contains 110 controls in 14 categories. These include risk assessment, technical protections, 72-hour reporting of cyber incidents, and training and other organizational controls. SP 800-171 also incorporates and cross-references requirements from the NIST 800-53 standard (including general non-federal organization controls).
- Consequences of non-compliance: Possible loss of the government contract, civil damages for negligence/contract breach, criminal liability for fraud.
- Effective date: December 31, 2017. At a minimum, a System Security Plan and Plan of Action should have been in place by then.
- Synergies with NIST Cybersecurity Framework: Most SP 800-171 controls map to one or more NIST Framework requirements.
Cybersecurity Advisory Council
Center for Responsible Enterprise And Trade - CREATE.org

Robert Gaston
VP, Operational Risk Management
ADP Global Security Organization

Chris Boyer
Asst VP, Global Public Policy
AT&T Services Inc.

Mark Sutton
VP, Chief Information Security Officer
Bain Capital

John Denning
Sr VP, Operational Policy Integration, Development and Strategy
Bank of America

David Savage
Associate Technical Fellow, Commercial Aviation Services
The Boeing Company

Dr. Ravi Pendse
VP & Chief Information Officer
Brown University

Edna Conway
Chief Security Officer, Global Value Chains
Cisco Systems

Tim Martin
Chief Information Security Officer
ClearObject

Javier Llinas
VP, Risk Management
Colgate-Palmolive Company

Gaspare LoDuca
Chief Information Officer
Columbia University

Mary Dalecki
Associate VP of Internal Audit
Columbia University

George Guzman
Director of Information Security
Universal Service Administrative Company (USAC)

Kent Landfield
Director, Standards and Technology Policy
McAfee

Michael Iwanoff
Chief Information Security Officer
iconectiv

Pravin Rao
Chief Operating Officer
Infosys

Vishal Salvi
Chief Information Security Officer
Infosys

Janet Nasburg
Chief Risk Officer
Intuit Inc.

Alexander Niejelow
Sr VP & Group Head, Global Public Policy
MasterCard

Brian Shea
Sr Director, Governance, Risk & Compliance
Microsoft

Tom Easthope
Director, Enterprise Risk Management
Microsoft

Justine Thompson
Risk Manager
Microsoft

Shinichi Yokohama
Head, Cyber Security Integration
NTT Corporation

Meredith Dickey
Director, Information Security Strategy
PepsiCo, Inc.

Octavio Flores
Supply Chain, BI Associate Director
Procter & Gamble

Bruce Goldstein
Executive VP, Finance and Risk
PVH Corp.

Howard Overdyk
Principal Enterprise Cyber Security Architect
Rockwell Collins

Geovette E. Washington
Sr Vice Chancellor and Chief Legal Officer
University of Pittsburgh