NAVEX GLOBAL®
The Ethics and Compliance Experts

Cyber Security and Inside Threats: Turning Policies into Practices

Presented by

Ingrid Fredeen and Pamela Passman

Presented By

Ingrid Fredeen, J.D.

VP and Senior Product Manager, NAVEXEngage
NAVEX Global

Pamela Passman

President and CEO
CREATe Compliance

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

CREATe Overview

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.

CREATe.org
Center for Responsible Enterprise And Trade

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

CREATe Compliance

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

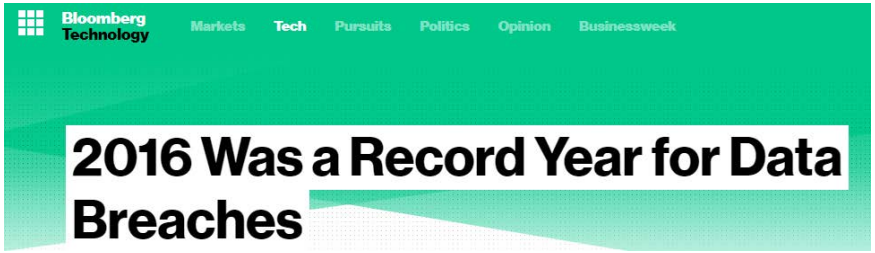
- CREATe Leading Practices for Cybersecurity
- CREATe Leading Practices for Anti-Corruption
- CREATe Leading Practices for Intellectual Property Protection
- CREATe Leading Practices for Trade Secret Protection

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."

--Identity Theft Resource Center Data Breach Report (2016)

- 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

CREATe Compliance

Threat Actor	Objectives	Methods	Vulnerabilities
Nation States	Military technology, help national companies	Blunt force hacking Social Engineering Trojan Horse Spear phishing Watering Hole Exploits Malware Co-opted Credentials Physical/Non-technical	Processes People Technology
Malicious Insiders	Competitive advantage, financial gain, national goals		
Competitors	Competitive advantage		
Transnati'l Organized Crime	Financial gain		
Hacktivists	Political/social goals		

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

CREATE Compliance

Government contracts now regularly require:

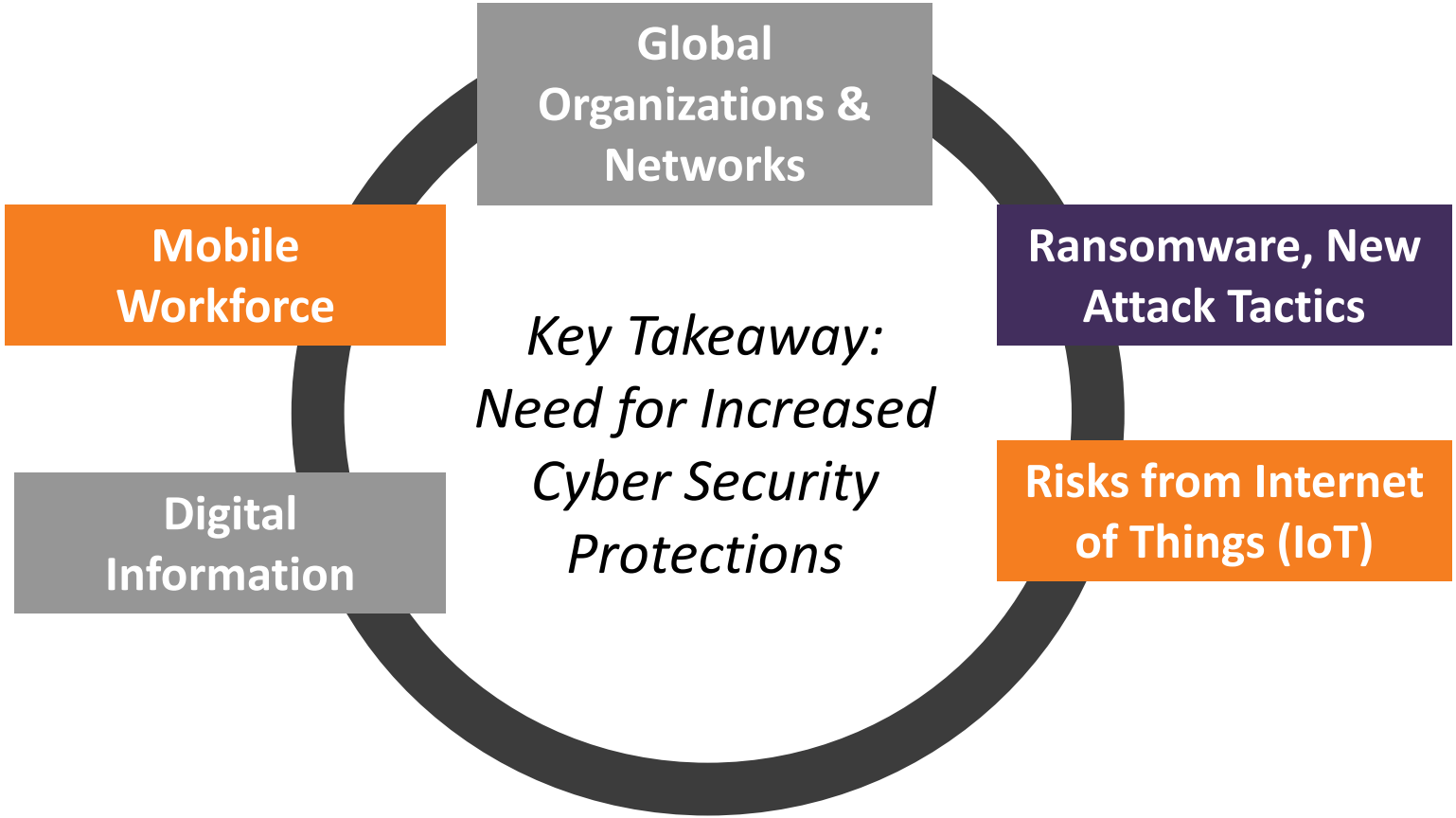
- Particular cyber security controls
- Compliance with particular standards
- Risk assessment and risk management
- Reporting and remediation of breaches

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



How Companies Address Cyber Security

CREATE Compliance

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

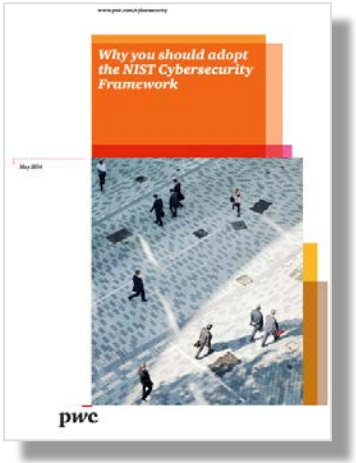
The NIST Cybersecurity Framework

CREATE Compliance

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

"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."

Bringing Consistency to Cyber Security Efforts

CREATE Compliance

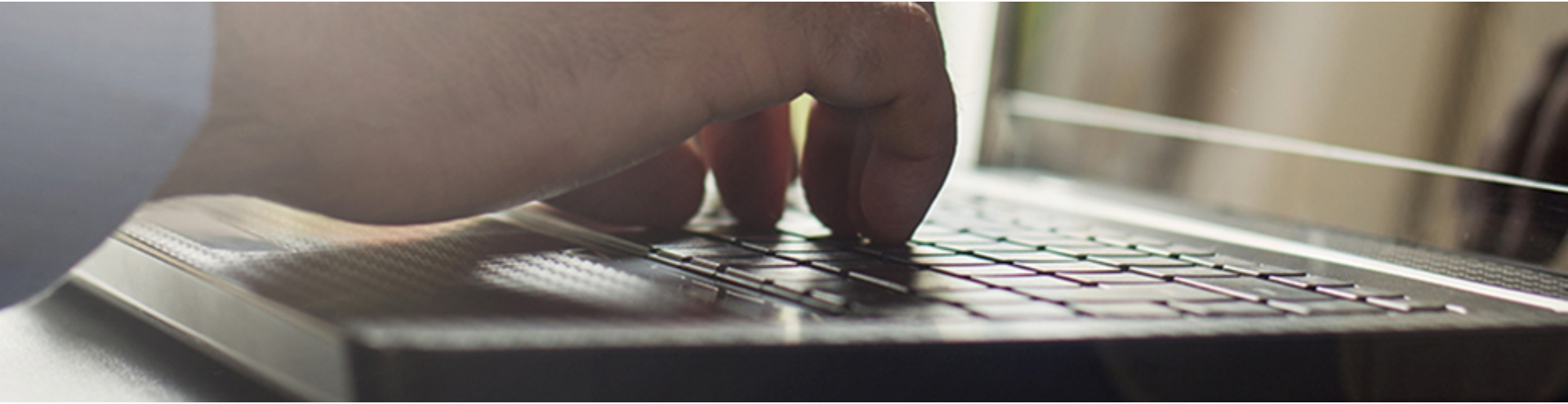
OVERVIEW OF NIST CYBER SECURITY FRAMEWORK	
IDENTIFY (ID)	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT (PR)	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT (DE)	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND (RS)	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER (RC)	Recovery Planning
	Improvements
	Communications

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]

- O During onboarding
- O Once a year
- O Multiple times a year
- O I don't know
- O 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

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

Bringing Consistency to Cyber Security Efforts

CREATE Compliance

OVERVIEW OF NIST CYBER SECURITY FRAMEWORK	
IDENTIFY (ID)	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT (PR)	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT (DE)	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND (RS)	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER (RC)	Recovery Planning
	Improvements
	Communications

- 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

CREATe Compliance

How CREATe Gauges Maturity

CREATe Compliance

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

Resource: CREATe › Leading Practices *for Cyber Security*

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

- Report: 2016 Ethics & Compliance Training Benchmark Report
- 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]

- O Schedule a guided tour of our Cyber Security training course
- O Discuss our full online training library
- O 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
- O No thanks

Questions?

Thank You