nrtc
Member driven. Technology focused.

Navigating NIST Compliance to Elevate Your Cybersecurity Posture

May 16th, 2024

1

Introductions

Scott Watts
Director, Product Management & Strategy
NRTC Managed Services

nrtc SILVERSKY

2

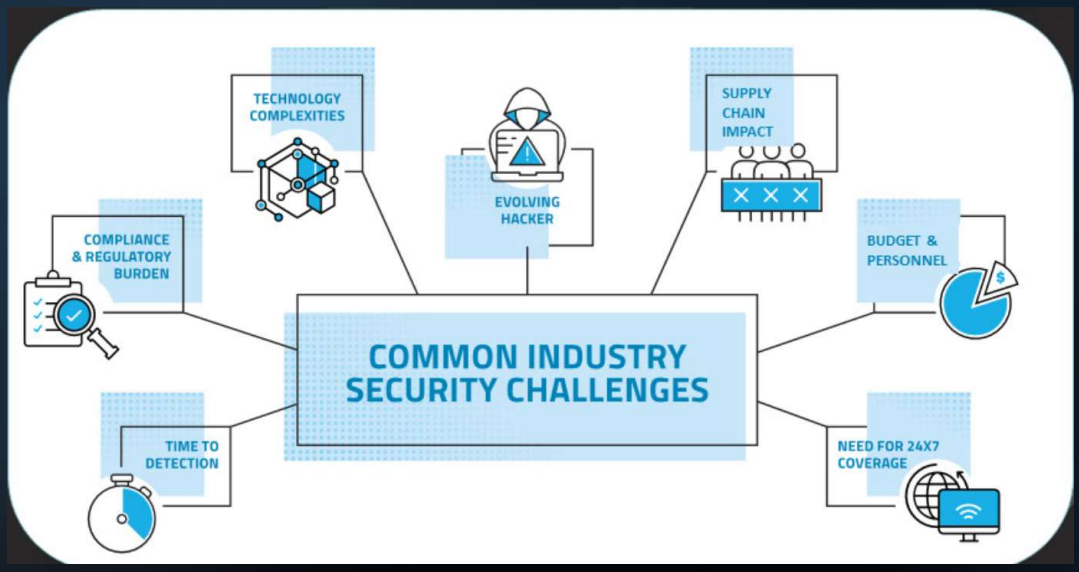
Topics

- Challenges Facing Most Organizations
- Current Cybersecurity Landscape
- Building a Cyber Resilient Program
- Final Words of Advice
- Q&A

nrtc

3

Cybersecurity Challenges in 2024



4

Cyber Threat Landscape:

The Evolving Hacker and Dwell Time

Opportunistic Hacker:

Independent Actors, No real goal but notoriety

Spray and prey attacks
After school hackers

2000-2006

2006-2012

Criminal Gangs:

Well Funded, Targeted, Goal: Monetary Gain

2006 Onset of Zeus

Nation-state Actors

Military Focus, High Value Targets, Critical Infrastructure Goal: Destructive, Disruptive

2012-2019

2019-present

Hybrid Hacker

Cyber warfare

Nation-states combining with cyber criminals

5

Cyber Threat Landscape:

Protecting the Crown Jewels

SENSITIVE TOXIC DATA

NAMES HOME ADDRESS
DATE OF BIRTH CREDIT CARD NUMBER
PASSWORDS SOCIAL SECURITY NUMBER
SECURITY QUESTIONS ANSWERS
EMAIL ADDRESS PHONE NUMBERS
ACCOUNT NUMBERS
FINANCIAL INFORMATION

VS.

CORPORATE SECRETS

CORPORATE TRADE SECRETS
COMPANY FINANCIALS
MERGER AND ACQUISITION DATA
R&D AND PRODUCT DOCUMENT
PATENTS/TRADEMARK DATA
BLUEPRINTS/DESIGN PLANS

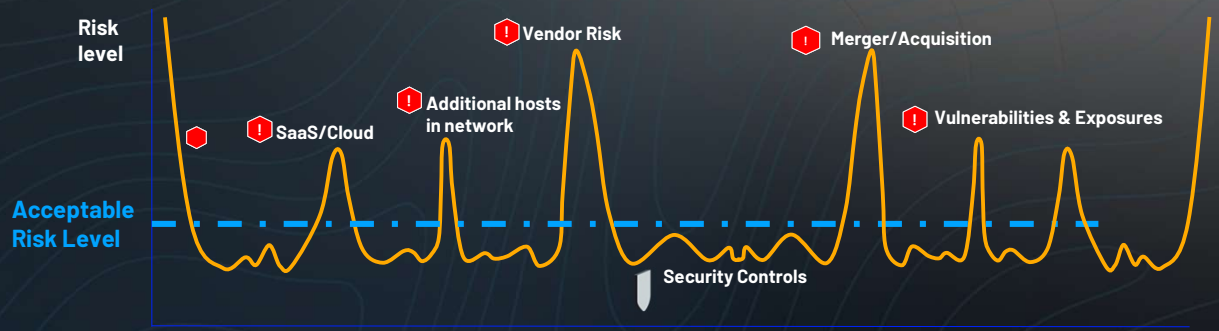
FINANCIAL GAIN

RANSOMEWARE
WIRE FRAUD SCHEMES
EXTORTION
DATA ENCRYPTION
AI DECEPTION

6

Cyber Threat Landscape:

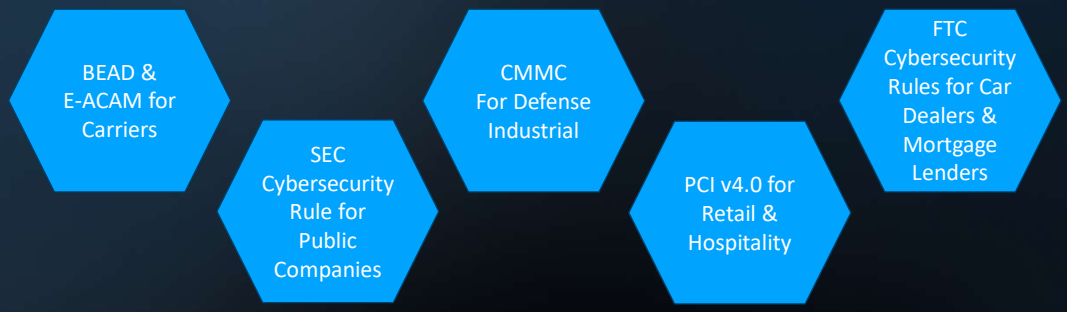
Technology Complexities and Need for 24/7



7

Cyber Threat Landscape:

Increased Regulatory Burden



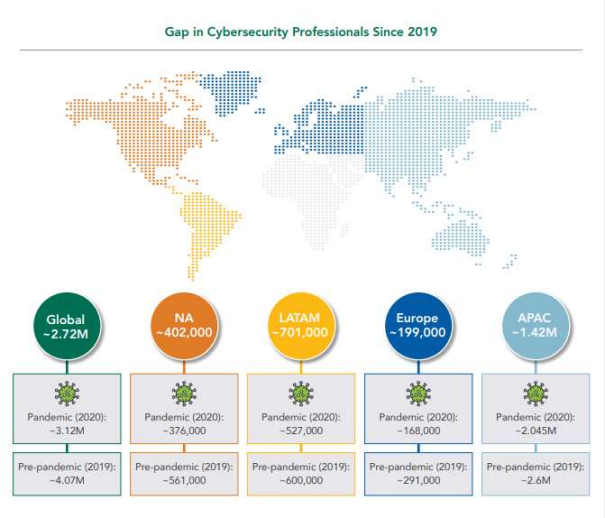
8

Cyber Threat Landscape:

Budget and Personnel Challenges

According to the ISC2 2023 Cybersecurity Workforce Study:

- Security spending still a small portion of overall IT Budgets
- Cybersecurity professionals say the workforce gap remains the number one barrier to meeting their security needs
- Two-thirds (60%) of study participants report a cybersecurity staffing shortage is placing their organizations at risk
- Despite 700,000 new professionals in the cybersecurity workforce, the study shows that global demand for cybersecurity professionals continues to outpace supply
- United States continues to show a shortage of 377,000 unfilled cybersecurity roles.



9

Building a Cyber Resilient Program

10

Regulation vs. Framework

Regulations

- A host of laws and requirements that directly and indirectly govern the various cybersecurity requirements for any given business or industry segments

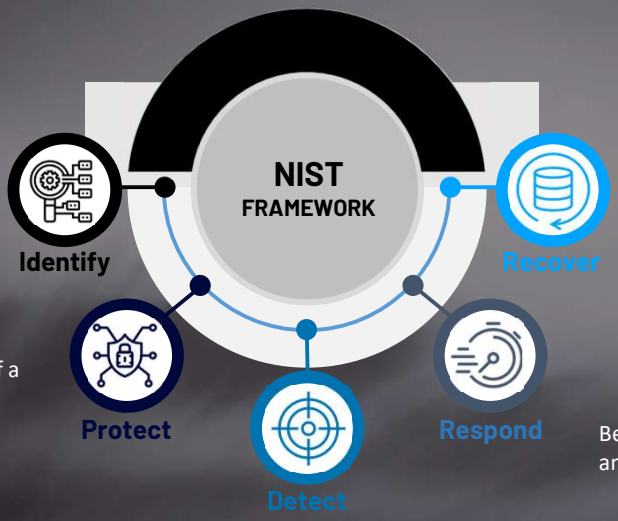
Frameworks

- A security framework is a series of documented processes that define a recommended implementation and ongoing management of information security controls.
- These frameworks are a blueprint for managing risk and reducing vulnerabilities.

PCI-DSS (Retail, Hospitality)	ISO 27000
FEDRAMP/TAC202 (Gov./State Regs)	NIST 800-53
CMMC (Defense Industrial Base) →	NIST 800-171
HIPAA (Healthcare) →	HITRUST
BEAD/E-ACAM (Carriers) →	NIST CSF
GLBA/FACTA (Financial) →	CIS Critical Controls

11

What is NIST Cyber Security Framework?



Understanding your risk and regulations

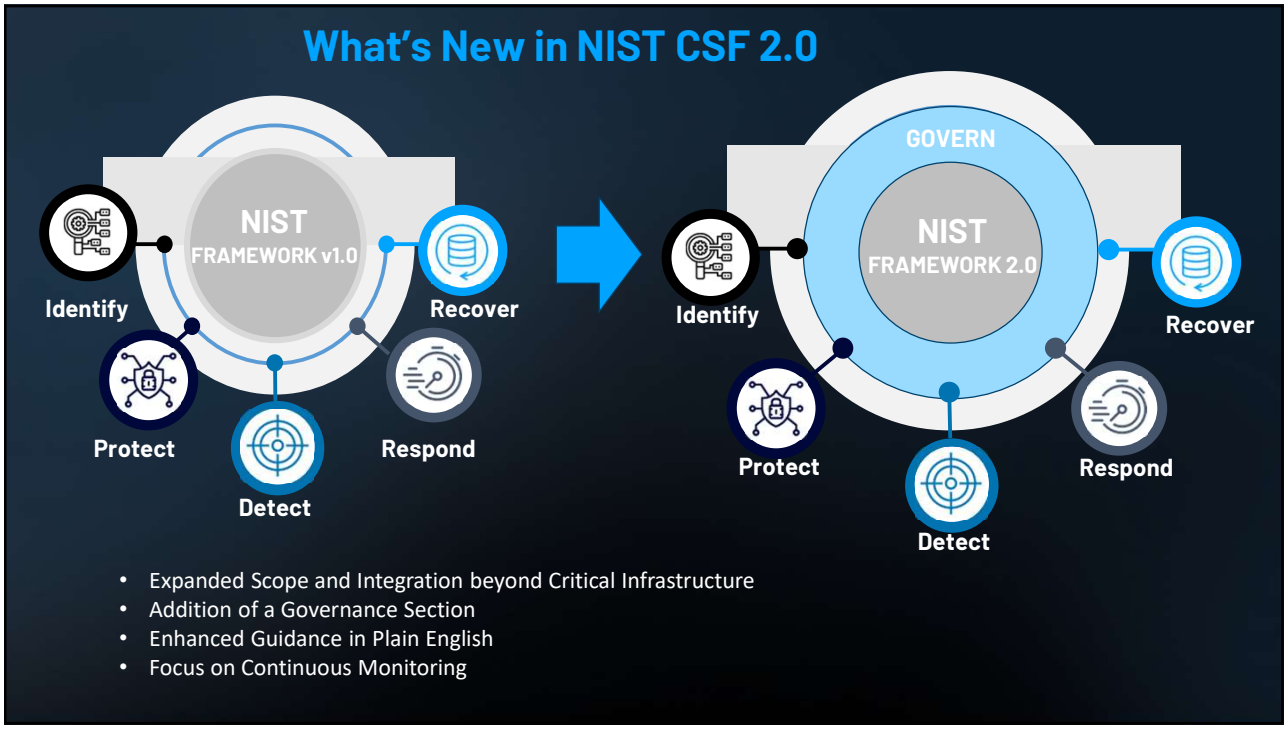
Maximize the ability to recover from a cyber incident

Reducing the likelihood of a damaging cyber intrusion

Be prepared to respond if an intrusion occurs

Developing the ability to quickly detect a potential intrusion

12


What's New in NIST CSF 2.0
NIST
FRAMEWORK v1.0
Identify
Recover
Protect
Respond
Detect
GOVERN
NIST
FRAMEWORK 2.0
Identify
Recover
Protect
Respond
Detect
• Expanded Scope and Integration beyond Critical Infrastructure
• Addition of a Governance Section
• Enhanced Guidance in Plain English
• Focus on Continuous Monitoring

13


Goal 1: Understanding Your Risk
IDENTIFY
I Have Limited Budget. How Do I know I am spending wisely?
Frame Risk
• Aligns the key business processes/technology to the mission/business objectives it supports
• Establishes Risk Tolerances around strategic, operational, reputational, financial, technology, external, and legal
Identifies Who and What?
• Identifies the "Who" by analyzing the threats actors and tactics they may use
• Identifies the "What by identifying what business process and systems are likely targets
• Understand your attack vector including third parties
Operationalizes Risk
• Aligns technology assets to business processes and criticality
• Drives operational process through a risk prioritized approach
• SOC Operations
• Vulnerability Management

14

Goal 2: Reducing the likelihood of a damaging cyber intrusion

PROTECT

Align Protections with Risk Mitigation

- Develop a roadmap of protections starting with high risk, largest maturity gain, or based on critical systems.

Build Processes with Risk in Mind

- Risk Prioritized approach can be applied to most processes in a Cyber Program

Key Protection Elements Every Resilient Program Needs

- Multi-factor authentication
- Back-ups
- Email Protection
- Security Awareness
- Vulnerability and Patch Management

15

Goal 3: The Ability to Quickly Detect a Potential Intrusion

DETECT

Assess

People:
- Build vs. Outsource
- Train users to report events

Process:
- Develop detections based on threat profiles
- Risk based response

Technology:
- Find the right technology for you (SIEM, SOAR, SOCaaS, MDR)

Visibility

- Detection mechanism should cover key telemetry points.
- Ability for a SOC to piece together an attack - Email, Perimeter, Endpoints, Users
- Periodically test the the effectiveness of your detections

Coverage

- Coverage must be 24x7x365 due to changing Threatscape
- Monitoring is not a check the box activity - All assets and systems should be covered
- Review environment periodically and implement a process to incorporate new devices

16

Goal 4: Be prepared to respond if an intrusion occurs

RESPOND

Plan

- Develop an IR plan with playbooks for common risk scenarios
- Include Third Parties and Service Providers in Plan
- Build out roles and responsibilities
- Establish internal and external communication plans

Prepare

- Don't assume your MSSP covers incident response
- Establish a relationship with an Incident Response Firm
- Cyber Insurance is not a replacement for a Cyber Program
- Designate a crisis-response team

Practice

- Practice your Incident Response Plan with Tabletop exercises of plan to test scenarios
- Incorporate practice with backup scenarios in your DR/BCP Plan
- Include Service Providers and Third Parties in plan walkthroughs

17

Goal 5: Maximize the ability to recover from a cyber incident

RECOVER

Maintain Good Backups

- Test backup procedures to ensure that critical data can be rapidly restored
- Ensure that backups are isolated from network connections
- Cloud Backups to Alternate Zones

Recovery Plans

- Practice your Incident Response Plan with Tabletop exercises of plan to test scenarios
- Practice backup scenarios in your DR/BCP Plan
- Include Service Providers and Third Parties in plan walkthroughs

18

Goal 6: Test and Validate Controls

IDENTIFY

Continuous Monitoring of a Security Program

Continuous monitoring **enables you to review cyber processes for adherence to and deviations from their intended performance and effectiveness levels**.

Test, Test, Test

- Validate your control by implementing a continuous monitoring program or IT Controls reviews
- Test your program – Penetration testing, Social Engineering, Red Team Simulations, Backups
- Program Improvement – Use Test Results to strengthen controls and re-assess Risk Profiles

19

Final Words of Advice

1. **There is no finish line!**
   - Security threats are changing everyday
2. **There is no Silver Bullet!**
   - Build a program with layers of protection
3. **Build a Cyber Culture from the top down!**
   - It starts with BOD and Executive buy in
4. **Don't take the Journey Alone!**
   - Find a good partner and resources to help

20

Questions?

Scott Watts
Director, Product Management

21

Thank You!

For more information visit: www.nrtc.coop

Or email: managedservices@nrtc.coop

22