LeveL5Cyber

Secure Delaware 2021

Building an Adaptable Security Strategy

Presenters: Marianne Swarter & Anthony Morrone

What Are We Talking About?

- Methodology to develop a Security Strategy
  - Pick an industry standard to measure cyber maturity
  - Define the scope
  - Understand current state
  - Identify business specific threats & gaps
  - Determine risk tolerance
  - Develop a plan

- How to apply the methodology to develop a Third-Party Risk Management Strategy

What is NIST?

The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and non-regulatory agency of the US Department of Commerce.

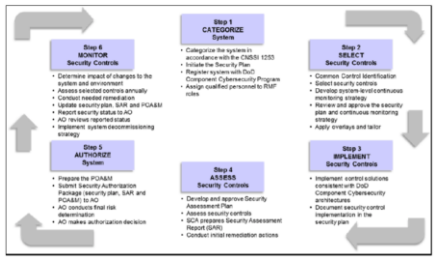
Its mission is to promote American innovation and industrial competitiveness.

NIST CSF

Cybersecurity Framework

NIST 800-30

Guide for Conducting Risk Assessments



NIST 800-53

Security and Privacy Controls for Information Systems and Organizations

NIST 800-82

Guide to Industrial Control Systems (ICS) Security

NIST 800-171

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Define the Scope

- Identify business process / mission objective
  - Third-Party Management, Supply Chain, Strategic Vendor Management
  - Intellectual Property Protection
  - Operational Integrity

- Identify systems and assets
  - Regulatory requirements
  - Threats
  - Vulnerabilities

Measure Current State Capabilities

Scope → Orient → **Current Profile** → Risk Assess → Target Profile → Prioritize Gaps → Develop Plan

- NIST CSF 5 Core Functions
- Choose an ***Informative Reference*** that is right for your business and develop objective scores for each ***Category.***
- Typically requires interviewing SMEs
- Developing the questions and scoring are the challenges – don't need to go to extremes the first time!
- Using 3rd parties to provide independent and objective reviews
- Rotate 3rd parties and ensure they follow an industry standard scoring methodology, or you may need to map to prior year's assessments.

Figure 1: Framework Core Structure

Identify Business Specific Threats & Gaps

- How to identify company risks
  - Company Risk Register
  - Board Risks
  - Interview C-level
  - 10K Reports
  - Cyber Information Sharing groups for your business
  - National ISAC's like InfraGard

- Common risks
  - malware/ransomware/BEC, IP loss, operational disruption, insider, regulatory, environmental, reputation, theft

Determine Risk and Tolerance

- Perform risk assessment
  - Align stakeholders on threats and impact
  - Align technical team on vulnerabilities, controls and likelihood
  - **Assets, threats → probability of threat being exploited → impact → controls → risk**
- What can you do with risk?
  - Mitigate risk to an acceptable level
  - Avoid the risk
  - Accept the risk
  - Transfer the risk
- Develop a plan of action
- Companies will choose different paths based on business models, regulatory drivers, culture, state of the business, and many other drivers.

It's critical to tailor the solution to meet the business needs!

Here's What We Covered!

- We have identified a scope and all the related assets
- We have documented the cyber capabilities supporting those assets
- We have identified the threats and performed a risk assessment against supporting assets
- Identified how the risks will be addressed
- Developed a plan of action to address gaps

Now Develop the Strategy!

- Key points to a successful strategy
  - Clearly defined current, and end state with business value
  - KPIs and multi-level metrics can be measured
  - Leadership buy-in on costs, timing, resourcing and impact to user and culture
  - Communication Plan
  - Brand the strategy
  - Use of Innovation

Develop a Third-Party Risk Management Program (TPRM)

- Methodology to develop a TPRM Program
  - Pick an industry standard to measure cyber maturity → **NIST CSF & NIST SP800-30** (what about CMMC and 800-82?)
  - Define the scope → **TPRM**
  - Understand current state → **Identify all in scope assets/processes and measure their capabilities using NIST CSF**
  - Identify business specific threats & gaps → malware, IP loss, compliance
  - Determine risk tolerance → what will the business accept (cost, effort, impact)?
  - Develop your Strategy
    - Focus on remediations that will drive the most business value
    - Plan and sell the high-value remediations that have higher cost and effort – those will be foundational to the strategy

About LeveL5Cyber

LeveL5Cyber is a veteran-led organization forged by a group of diverse and experienced leaders highly skilled in the protection of critical infrastructure, highly sensitive data, regulated environments, and those many organizations that are at the very heart of keeping our nation running. With decades of hands-on experience, LeveL5Cyber is committed to providing the highest caliber cyber consulting services that were built with people, processes, and solutions in mind. Our solutions are designed to reduce the risk and exposure of organizations to help ensure they can effectively defend against today's advanced threat actors and can continue to operate effectively. We are proud of our valued team members and the culture that we have built, which is why our employees are at the foundation of all that we do.

Learn more about us at
www.LeveL5Cyber.com

"Define the Risks, Defend the Assets"

Social media accounts

Who is LeveL5Cyber?

- **Our Heritage:** Former Lockheed Martin, DuPont and military personnel
- **Our Mission:** Addressing the critical market void by providing **right-sized solutions** hands-on, real-world expertise at a **competitive price point**

- LeveL5Cyber is a **veteran-led** organization with a **daily passion** for cybersecurity
- Our industry leaders have over **116 years** of collective cybersecurity experience

- We bring **right-sized** solutions for your business with **fixed outcomes** and **flexible terms** while reducing the risk and exposure to your organization
- We bring a **practical** and **cost-effective** approach to the market

Marianne Swarter – Senior Director

Marianne Swarter is a results-driven Risk Management Leader with over 23 years' experience building and strengthening information security processes world-wide. Throughout her 30-year tenure with DuPont, Marianne has built a reputation for developing strategies, producing new business models, and building out essential program. For the past seven years, Marianne built and led an Information Security Risk Management team. She was responsible for developing, organizing, directing and leading the global security risk management program. She has focused her career on strengthening the corporation's information security posture.

Anthony Morrone – EVP Corporate Strategy

Anthony is co-founder and EVP of Strategy at LeveL5Cyber (L5C). Prior to this, he spent 33 years in IT with the last 25 years focused on information security. Anthony has led many teams at DuPont, including as the Global CISO where he was accountable for risk management, cyber defense, education and awareness, infrastructure security, and others. He attended the University of Delaware with a BA in Math and a minor in Computer and Information Sciences and serves on University of Delaware's Cybersecurity Initiative Advisory Board. Anthony was also a member of the Phi Kappa Tau fraternity.