Implementing Cybersecurity using the National Institute of Science and Technology (NIST) Framework at Small and Medium Businesses (SMB)

By

Isaac Stephenraj

Student – M.S in Cybersecurity

Katz School of Science and Health at Yeshiva University

Implementing Cybersecurity using the NIST Framework at Small and Medium Businesses

Small and medium sized businesses (SMB) are prime targets for cyber criminals because many of these organizations typically don't have large cyber security budgets, the security of their systems, data and networks is not their highest priority, SMB's are unaware of the vulnerabilities in their systems, and also do not have do not have adequate preventative measures in place. Some common threats for SMB's include data breach, ransomware, an employee stealing or selling proprietary information, hackers using the SMB network to piggyback that access into larger, more secure systems, betraying the trust between the SMB and the larger organization. A Cybersecurity incident at an SMB can be devastating to the SMB's business, finances, and operational viability. According to the Verizon 2018 Data Breach Investigations Report, small businesses are 58% of data breach victims. Unlike the breaches impacting large, publicly traded companies, when a small business is hit with a breach, it may not become public knowledge or get reported in the local news. The National Institute of Standards and Technology (NIST) has developed a risk-based, voluntary, flexible cybersecurity framework that helps SMB's better understand, manage, and reduce their cybersecurity risk and protect their networks and data.

The NIST framework consists of three parts: Framework Core, Implementation Tiers, and Framework Profiles. The Framework Core represents industry standards, guidelines, practices, and consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond, Recover. The five functions provide a holistic, strategic view of an organization's management of cybersecurity risk. The Implementation Tiers provide context into an organization's views of its cybersecurity risk and the processes to manage those risks. The Tiers characterize an organization's practices from informal, reactive responses (Tier 1) to approaches that are agile and risk-informed (Tier 4). Framework Profiles are used to conduct

self-assessments and identify opportunities for improving cybersecurity posture by comparing a "Current" profile ("as is" state) with a "Target" profile ("to be" state). The Profiles enable an SMB to establish actionable cybersecurity risk reduction plans that reflect the SMB's business and strategic priorities and satisfy legal and regulatory requirements and industry best practices. The following paragraphs provide a high-level overview on implementing the NIST framework at an SMB, and briefly describe the five functions of the Framework Core at an SMB.

Implementing a new or improving an existing NIST cybersecurity program at an SMB consists of the following seven steps. An SMB can repeat the seven steps as needed to continuously assess and improve its cybersecurity program. In step 1 the SMB identifies its business objectives and organizational priorities and uses this information to make strategic decisions on the scope of its cybersecurity program. In step 2 the SMB identifies systems, assets, threats, vulnerabilities, and regulatory requirements that fall within the scope of its cybersecurity program. In step 3, the SMB creates a "current profile" using the categories and subcategories of the Framework Core to accurately represent the cybersecurity measures currently adopted or cybersecurity outcomes currently being achieved at the SMB. In step 4, the SMB conducts a risk assessment to identify existing and emerging risks, and gain a better understanding of the likelihood and impact of cybersecurity events. In step 5, the SMB creates a "target profile" using the categories and subcategories of the Framework Core to accurately identify the SMB's desired cybersecurity outcomes. The SMB may also consider the requirements of other entities, customers, and business partners when creating the target profile. In step 6, the SMB does a gap analysis to identify gaps between the current profile and target profile. Following the gap analysis, the SMB creates a prioritized action plan that addresses the identified gaps, and achieves outcomes identified in the target profile. The prioritized action plan is used by the SMB to determine workforce, and funding resources necessary to address the gaps. In step 7, the SMB implements the prioritized action plan

identified in step 6. In step 7, the SMB also determines the necessary standards, guidelines, and practices to implement the action plan.

The following section describes the five functions of the Framework Core, and lists some example measures an SMB can implement for each function. During “Identify” an SMB develops an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. “Identity” function activities are foundational for the effective use of the framework. Some example “Identify” measures include, creating and maintaining an inventory of purchased and/or installed software, collected and/or processed data, and bought and/or leased equipment (includes laptops, smartphones, printers, tablets, point-of-sale devices, etc.). An SMB may also create and share a cybersecurity policy document that covers roles and responsibilities for employees, contractors, vendors, and anyone else with access to sensitive data. An SMB may also conduct background checks for its employees, contractors, and require individual user accounts for each employee and contractor.

During “Protect” an SMB develops and implements appropriate safeguards to ensure delivery of critical services. “Protect” function activities are intended to limit or contain the impact of a potential cybersecurity event. Some example “Protect” measures include implementing a cybersecurity training program for everyone who uses any of the SMB’s devices, network, and data. Also an SMB may encrypt sensitive data, either at rest and/or during transit, conduct regular data backups, regularly update security software, routinely patch operating systems and applications, implement policies for safe disposal of electronic files and old devices, limit access to sensitive data, install surge protectors and uninterruptible power supplies, secure wireless access points and networks, install and activate firewalls, and setup web and email filters.

During “Detect” an SMB develops and implements appropriate activities to identify the occurrence of a cybersecurity event. “Detect” function activities are intended to enable the

timely discovery of a cybersecurity event. Some example “Detect” measures include installing and regularly updating antivirus, anti-spyware, and other anti-malware programs. An SMB may also maintain and monitor logs, and monitor computers, networks, and sensitive data for unauthorized personnel access, unusual activity, unauthorized users, or connections.

During “Respond” an SMB develops and implements appropriate activities to respond to a detected cybersecurity incident. “Respond” function activities are designed to support the ability to contain the impact of a potential cybersecurity incident. Some example “Respond” measures include, SMB creating a plan to notify impacted customers, employees, and other constituents, a plan to report the attack to law enforcement and other authorities, and plans to keep the SMB’s business operations up and running. As part of “Respond” an SMB may also investigate and contain an ongoing attack, update cybersecurity policy and response plans with lessons learned, and prepare for inadvertent events (ex: weather emergencies) that may put data at risk.

During “Recover” an SMB develops and implements appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. “Recover” function activities are designed to support timely recovery and reduce the impact from a cybersecurity incident. For “Recover” measures an SMB may make full backups of important business operations data and information, schedule incremental backups, improve processes, procedures and technologies, repair and restore network equipment parts that were affected by the cyber incident, and updating employees, customers and other constituents of the SMB’s cyber incident response and recovery activities.

In summary, the NIST Framework Core provides SMB’s with a flexible, broad array of cybersecurity risk management processes, and industry-wide accepted risk based implementation that can be tailored to the SMB’s industry, business and strategic priorities, risk

appetite, regulatory and legal requirements, and funding priorities. The NIST controls can also be used with a broad array of cybersecurity risk management processes (International Organization for Standardization – ISO; ISO/International Electrotechnical Commission – IEC; Electricity Subsector Cybersecurity Risk Management Process – RMP, etc.). Finally, adopting the NIST framework positions an SMB to prioritize cybersecurity activities and make informed decisions on cybersecurity expenditures, quantify and communicate adjustments to their cybersecurity programs, and enables an SMB to use its NIST controls to meet risk management accreditation requirements.

References

- NIST Cybersecurity Framework, https://www.nist.gov/cyberframework
- NIST Cybersecurity, https://www.NIST.gov/topics/cybersecurity
- NIST Manufacturing Extension Partnership (MEP) National Network, https://www.nist.gov/mep/mep-national-network
- NIST Cybersecurity resources for Manufacturers, https://www.nist.gov/mep/cybersecurity-resources-manufacturers
- NIST Small Business Cybersecurity Corner, https://www.nist.gov/itl/smallbusinesscyber
- NIST Computer Security Resource Center, https://csrc.nist.gov/
- FTC.gov | Cybersecurity for Small Business, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- FTC.gov | Understanding the NIST Cybersecurity Framework, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework
- "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1", *National Institute of Standards and Technology* (April 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- "Cybersecurity for Small Business : Understanding the NIST Cybersecurity Framework", https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf
- Small Businesses are a Big Priority for NIST, https://www.nist.gov/blogs/cybersecurity-insights/small-businesses-are-big-priority-nist
- National Cybersecurity Center for Excellence, https://www.nccoe.nist.gov