January 5, 2016

Cybersecurity, Where Do We Begin? Measuring Your Organization's Security with NIST Cybersecurity Framework

CYBERSECURITY, LARGE COMPANIES
BY SCHNEIDER DOWNS PROFESSIONAL

The concept of cybersecurity can be a daunting thought. The world of information technology alone is filled with complexity, then you add in business requirements and expanding user requirements. The next thing you know, your IT manager's hands are pretty full. Let's face it, most organizations today are so focused on keeping the lights on and keeping systems up and running that security is often an afterthought. The challenges that the average information technology professional face in today's ever-growing interconnected world have never been greater. The internet revolution has provided great resources for business and personal use alike; however, it has also made it much easier for a nefarious individual halfway around the world to hack into your organization's network.

The security world is filled with shiny new products and expensive solutions, none of which are a panacea for all security issues. It also seems like there are new critical security vulnerabilities identified in enterprise systems on a daily basis. To make things even more complicated, you add in the human element and how cyber attackers are targeting your everyday employee in order to circumvent or bypass that shiny new firewall you just purchased. So, you may be wondering, where do I start to ensure that my company's systems are secure? How do we know if we are doing enough? You are not alone.

While there is no foolproof formula to make sure your organization is secure, we recommend that you start with a tested and recognized framework to see how your organization stacks up. The NIST Cybersecurity Framework, which was drafted by the National Institute of Standards and Technology (NIST) in response to President Obama's February 2013 Executive Order titled "Improving Critical Infrastructure Cybersecurity," is an example of such a framework. The framework does not introduce many new technical standards or concepts; rather, it references and provides organization and structure to industry-leading and proven security best practices from organizations such as ISO, NIST, ISACA and others. The framework was developed over a ten-month period with collaborative input from more than 3,000 security professionals. It was designed to provide an assessment mechanism to allow organizations to determine their current state of security and define a plan of action to achieve a more desirable state.

The NIST Cybersecurity Framework Core defines and organizes standardized security activities, desired outcomes and applicable references. The Framework Core is organized by five core functions that are further broken down into categories (See

Table 1). The Framework Core essentially defines the critical security processes to be followed on a continuous and improving basis to constitute an effective cybersecurity posture.

NIST CYBERSECURITY FRAMEWORK CORE FUNCTIONS

Table 1

Function	Definition	Categories
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.	Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response Planning; Communications; Analysis; Mitigation; and Improvements.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery Planning; Improvements; and Communications.

KEYS TO A SUCCESSFUL CYBERSECURITY FRAMEWORK IMPLEMENTATION

- Ensure cybersecurity is aligned with the business mission and objectives.
- Gain senior management support.
- Assess the current security posture against the industry recommended best practices and guidelines.
- Determine where you would like to be in the short and long term.
- Develop an actionable plan to get you there.
- Continuously monitor, reassess and communicate results.

While implementing a framework such as this is completely voluntary, we view it as a necessary means of effectively evaluating an organization's cybersecurity measures in order to protect your most valuable information assets. Using a proven framework not only gives your organization advanced regulatory and legal standing, it establishes a proactive risk management approach that tackles a very complex problem. Adopting a framework such as this should ultimately shift your organization's security mindset from a reactive one, into a proactive risk-based driver of solutions.

Contact us with your cybersecurity questions and visit the Schneider Downs blog for similar articles.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.