Adopting the NIST Cybersecurity Framework in Healthcare

WHITE PAPER

Symantec™

It's no secret; the healthcare industry is a lucrative target for hackers. Healthcare groups host and share a large amount of personal information – from basic data such as names and addresses to more sensitive information such as medical records, financial and account information, to insurance and Social Security numbers. Additional information of interest includes business data like contracts, personnel and HR data, as well as research and intellectual property. Hackers want this information to resell on the black market, making healthcare the most attacked industry[1].

These frequent attacks, coupled with an industry that traditionally has underinvested in security, have placed healthcare organizations in a very unhealthy situation. In fact, the U.S. Department of Health and Human Services (HHS) recently said that healthcare organizations are "severely flawed[2]" when it comes to protecting this information.

While many healthcare organizations are starting to increase their cybersecurity investment, just purchasing and implementing security technologies alone won't advance an organization's need for a true and effective information risk management program. It is paramount that these organizations put in place a strategic yet dynamic approach for identifying the most critical risks and mitigate them on an ongoing basis.

To better address these challenges, many healthcare organizations are adopting the NIST Cybersecurity Framework (CSF) and its five core functions – Identify, Protect, Detect, Respond and Recover. This framework, developed by the federal government in partnership with major cybersecurity leaders, including Symantec, serves as the security roadmap for federal agencies, academia and other major industries. In fact, the most recent HIMSS Cybersecurity Survey (Aug. 2017) indicates mature organizations with a senior-level information security leader, such as a Chief Information Security Officer or other senior information security leader, have a wide-spread adoption of the NIST CSF, with 95% of respondents using it.

While the framework consists of best practices and industry recommendations around managing cybersecurity risks, the NIST CSF is not a simple checklist of security controls to implement. Its purpose is to help organizations assess their current security maturity and then develop and implement a risk management program that provides visibility and insight into systems, networks, and data on a continual basis.

As adoption of the NIST CSF continues to increase, there are considerations that healthcare technology professionals, and other stakeholders across the business, must understand when it comes to leveraging this framework and the benefits it can provide.

Compliance vs. Security Risk Management

When it comes to information security, there are already a number of regulations in place for healthcare organizations. The most well-known is the Health Insurance Portability and Accountability Act, better known as HIPAA, and specifically the HIPAA Security Rule.

Although the HIPAA Security Rule defines the basic requirements a healthcare provider needs to comply with, it does not provide any guidance on how to actually do that. HIPAA merely defines the objectives and baseline for information security. But simply being in compliance with HIPAA does not equate to an organization having a strong security posture. Information security must go beyond HIPAA, looking beyond just passing a compliance audit, to strengthening all aspects of the enterprise to protect against today's sophisticated and targeted attacks.

The NIST CSF can help healthcare organizations plot their path to a more secure state, and identify the appropriate technologies that can improve their overall security. The NIST CSF also gets to the core of risk management, providing a comprehensive guide for organizations to improve different aspects of security from technology to employee training to data controls.

Inside the NIST CSF

The NIST CSF provides a common structure for managing cybersecurity risk that is flexible and adaptable, and should be used by healthcare organizations as a baseline, even if they already use other frameworks such as COBIT, ITIL or HITRUST.

The NIST CSF is organized in five core functions:

- **IDENTIFY** physical and information assets and establish a risk management strategy as appropriate for the organization's risk tolerance and business environment;
- **PROTECT** the assets and data from malicious attacks or unintentional compromise;
- **DETECT** and monitor the environment for security events and incidents;
- **RESPOND** to attempted or successful attacks; and
- **RECOVER** from the attack, while using the lessons learned to adjust security policies and fill in any existing gaps

1 - https://www.esecurityplanet.com/network-security/healthcare-industry-hit-most-frequently-by-cyber-attacks.html
2- http://www.healthcareitnews.com/news/hhs-task-force-says-healthcare-cybersecurity-critical-condition

Each of these functions allow healthcare organizations to better understand their security risks and potential consequences. The goal is to shed light on areas that are under-protected or do not meet the larger security objectives of the organization. That could necessitate more training for employees, a new technology or even restructuring governance models.

Organizations that leverage the NIST CSF will be able to create a "plan of attack" to address risks and vulnerabilities. They can prioritize the most critical aspects and devote resources to the areas that need it most by developing a long-term plan to address these risks.

By having a better understanding of their environment and their exposure, healthcare organizations will better know how to protect themselves.

How Symantec Can Help

The NIST CSF provides a comprehensive look at information security, but healthcare organizations need a partner with the tools to implement it efficiently and effectively. Symantec offers the most comprehensive set of security tools to prevent, detect and report on unauthorized attempts to penetrate and exfiltrate data from a network, mobile device or the cloud.

Symantec can provide a multi-layered approach that aligns with the NIST CSF, enabling healthcare organizations to have confidence that their cybersecurity program is, and will remain, effective. Our Integrated Cyber Defense Platform helps protect information no matter where it lives, whether in the cloud or on-premise, creating a cohesive security architecture that provides information technology leaders with increased visibility into their data and networks. This platform not only offers solutions across all five functional areas but can help make the necessary correlations across these areas, eliminating the security silos that have traditionally existed, especially with systems that blend on-premise and cloud computing solutions.

Using the NIST CSF as a guide, Symantec can help organizations identify areas of priority while mapping back to solutions already in place as well as identifying the gaps in their architecture that need to be prioritized and addressed.

Based on Symantec's alignment with the NIST CSF, Symantec has the breadth and depth to help organizations address all five functions, including:

NIST Function	Protection Requirement	Leading Symantec Technologies
IDENTIFY	Identify and manage assets	Endpoint Management, Data Loss Prevention (DLP)
	Discover and classify sensitive information	Data Loss Prevention, Cloud Access Security Broker (CASB)
	Define business environment and governance	Compliance Automation
	Risk Assessment and Risk Management	Compliance Automation
PROTECT	Identity Management and Access Control	Multi-factor Authentication, CASB, Proxy
	Awareness and Training	Compliance Automation, Education Services
	Data Security	DLP, Encryption, Proxy, CASB
	Information Protection Policies & Procedures	Compliance Automation, Endpoint Management, DLP, Encryption, Proxy, CASB, Incident Response
	Maintenance	Endpoint Management, Multi-factor Authentication, Endpoint Protection, CASB
	Protective Technology	Advanced Threat Protection (ATP), Multi-factor Authentication, DLP, Endpoint Protection, CASB
DETECT	Anomalies & Events	Security Services, ATP, Email/ Web Gateway, Proxy, CASB
	Security Monitoring	Multi-factor Authentication, Endpoint Protection, ATP, Email/Web Gateway, Security Proxy, CASB
	Detection Process	Compliance Automation, ATP, Security Services, Security Analytics
RESPOND	Response Planning	Incident Response
	Communications	Compliance Automation, Security Services, Incident Response
	Analysis	ATP, Security Services, Incident Response
	Mitigation	Endpoint Protection, ATP, Proxy, Incident Response
	Improvements	Endpoint Management, DLP, Endpoint Protection, ATP, Security Services, Incident Response
RECOVER	Recovery Planning	Compliance Automation, Security Services, Incident Response
	Improvements	Compliance Automation, Security Services, Incident Response
	Communications	Compliance Automation

Conclusion

Across all industries and government, selecting the right security framework is essential to helping define an organization's security posture, identify gaps and provide a strategy for improvement, but also develops a common language to communicate status to all stakeholders from IT Security to the Board. As healthcare organizations continue to fend off a growing number of malicious attacks, alongside taking on new digital transformation projects, they will benefit from leveraging the NIST CSF to help prioritize security efforts.

While the NIST CSF will not protect assets and data by itself, it provides a guide for healthcare organizations to manage their own assets, taking a full view of their enterprise and its vulnerabilities. Using the NIST CSF as a framework and incorporating leading technologies into a comprehensive cybersecurity program will go a long way in locking down the personal and valuable information housed in healthcare systems. Protect systems, data and identities using the NIST CSF combined with an integrated suite of tools, on-premise or in the cloud, on any device, wherever it is located.

To learn how Symantec can help your organization leverage the NIST CSF and for more information about our solutions, visit our webpage at **www.symantec.com/healthcare**.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

SYMC-Healthcare-NIST-CSF-WP-v3