Choosing an Information Risk Management Framework: The Case for the NIST Cybersecurity Framework (CSF) in Healthcare Organizations

CLEARWATER COMPLIANCE

> *"The question becomes: Am I going to spend my cybersecurity budget on somebody else's list of 'good things to do?' Or am I going to spend it on the basis of my organization's assets, my exposures, my business goals and objectives?"*
>
> **Bob Chaput,** CEO, Clearwater Compliance

The healthcare industry is quickly becoming the number one target of cyberattackers. The value of protected health information (PHI), combined with the industry's struggle to afford and implement cybersecurity best practices, makes the healthcare industry an irresistible target. Gone are the days when a network firewall and anti-virus software provided adequate protection. Because of changes in the scope and intensity of the threat landscape, the healthcare industry needs a more sophisticated approach to information risk management (IRM).

"Information security in healthcare today is characterized by being tactical and technical. It involves a lot of spot-welding and firefighting," said Bob Chaput, CEO, Clearwater Compliance. "But that approach doesn't work anymore. Healthcare organizations require a strategic, risk-based approach to cybersecurity in order to protect patient safety and business assets. That approach is exactly what a cybersecurity framework provides."

Why Healthcare Organizations Need a Cybersecurity Framework

Until now, many healthcare organizations have taken a fragmented, reactive approach to cybersecurity. First they installed a network firewall, then they purchased and installed antivirus software, and then maybe a malware detection system or encryption. "The problem with this approach is that it isn't strategic," said Chaput. "It emphasizes the technical aspects of cybersecurity and ignores the organization's business context, goals and desired outcomes."

Adoption of a cybersecurity framework flips the piecemeal approach on its head. Instead of starting with the purchase of point solutions, a true cybersecurity framework starts with an inventory of the organization's information assets. In other words, a cybersecurity framework changes the game from defense to offense. Adoption of a cybersecurity framework helps an organization establish the foundation for an overall information risk management program, rather than focusing on specific technology tools.

"The single biggest decision a healthcare organization will make regarding cybersecurity and information risk management is how the organization will approach this task," said Chaput. "This one decision will have long-term effects on the organization's ability to establish, implement and mature an information risk management process that transcends time and assets. To be effective in today's constantly evolving threat landscape, healthcare organizations must adopt an approach that goes beyond the threats, vulnerabilities and controls du jour."

What a Cybersecurity Framework Is – And Isn't

A cybersecurity framework – as the word 'framework' implies – provides an organization with an architectural approach to information risk management. The framework methodology is grounded in an initial inventory of the organization's information assets and exposures, considered in the context of the organization's business goals and objectives. "The framework provides a way for the organization to think seriously and deeply about the desired outcomes of their information risk management program," said Chaput. "The framework is not about how. The framework is about what you are trying to achieve."

This focus on high-level architecture in the context of specific business outcomes is what differentiates a cybersecurity framework from a controls checklist. "A framework is broad and it's high-level," said Rob Suárez, Director of Product Security, BD (Becton, Dickinson and Company). "A framework is applicable

> *"The NIST CSF is designed to be agile and adaptable over time, so that it can keep pace with the evolving threat landscape."*
>
> **Matt Barrett,** NIST Program Manager, Cybersecurity Framework

to a wide range of scenarios and technologies, while a controls checklist is typically prescriptive to one stakeholder group or to specific types of technologies. A controls checklist can't replace the role of a framework, but it can't replace the role of a framework in an organization's information risk management program."

The controls checklist approach skips over the question of what an organization's information risk management program is trying to achieve, and goes straight to the how. It's a one-size-fits-all approach to cybersecurity. For example, a controls checklist might ask, 'Do you have a firewall in place? Yes or No. Have you implemented anti-malware? Yes or No. Have you implemented an intrusion detection system? Yes or No.' The framework approach starts with a different question, i.e., "What are your information assets and what are their specific vulnerabilities?"

Healthcare organizations don't have unlimited dollars to spend on information risk management and cybersecurity. "The question becomes: am I going to spend my cybersecurity budget on somebody else's list of 'good things to do?' Am I going to spend it on the basis of my organization's assets, my exposures, my business goals and objectives?" said Chaput. "If I have articulated my business goals through a framework, I can make business decisions that are specific to my organization's goals. For example, encryption may not be my number one issue. I may need to prioritize a firewall instead. Adopting a framework as opposed to just marching down some controls checklist puts the organization in a far better position to make intelligent and informed decisions."

The Case for the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

Once a healthcare organization decides to adopt a framework approach to information risk management, the next question becomes: which framework? There are many to choose from, including publicly available frameworks, industry-specific frameworks and commercial frameworks. Chaput believes there is only one cybersecurity framework worth considering: the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). NIST CSF Version 1.0 was released in February 2014 in response to a 2013 Executive Order aimed at improving cybersecurity across the Nation's critical infrastructure.[1] Since its initial release, the NIST CSF has emerged as the frontrunner within healthcare, across industries, and even across national boundaries. "The NIST CSF is far superior to every other framework available to healthcare organizations," Chaput said. Here are a few of the reasons why:

- **The NIST CSF was developed using an open, inclusive process.** "We used a 'come-one, come-all' approach to developing the NIST CSF," said Matt Barrett, NIST Program Manager, Cybersecurity Framework. The year-long process leading up to the release of NIST CSF Version 1.0 included many opportunities for stakeholder participation and public input including an initial Request for Information (RFI); three public workshops; the publication of a first draft with the opportunity for public comment; and two additional public workshops. "More than 2,000 people participated in the series of five initial workshops," said Barrett. "Stakeholder participation was important for the initial development process, and that is the process we are using to this day, for the continuing evolution of the framework."

- **The NIST CSF uses accessible language that all stake holders – from C-suite executives to IT specialists – can understand**. The NIST CSF is built around five core functions: identify, protect, detect, respond and recover. "The value of those five functions cannot be overstated," said Barrett. "Those five words are critical for two reasons. First, they describe the

[1] Exec. Order No. 13636, 3 C.F.R. 11737-11744 (2013). Retrieved from https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

> *"The NIST model involves everyone, from the technical people operating at a tactical level, to the leadership at the highest level, who are crafting policies and procedures."*
>
> **David Finn,** former Health IT Officer, Symantec

entire breadth of cybersecurity, whether it is applied to the cyber, physical, or personnel domain. Second, they are purposely accessible, eighth-grade level words. The reason that's important is because cybersecurity is such a massive challenge that cybersecurity experts alone cannot solve the problem. We need all parties to participate, to understand how cybersecurity affects them, and to understand how they can impact cybersecurity. Using those five words means that whether a person is on a hospital's Board of Directors, or a clinician, or an IT specialist, or a front-desk clerk, they can understand and participate in the conversation about cybersecurity. That feature of the NIST CSF is incredibly important."

- **The NIST CSF facilitates information governance.** "The healthcare industry doesn't do information security governance, or even information governance, very well," said David Finn, former Health IT Officer, Symantec. "The NIST CSF has governance built into it, because it calls for both a top-down and a bottom-up response. Under the CSF, the organization's technical people may be collecting data, and explaining what is working and what is not working; but at the same time, it is up to the leadership to look at that data and decide how it will change the organization's approach to security. The NIST model involves everyone, from the technical people operating at a tactical level, to the leadership at the highest level, who are crafting policies and procedures."

- **The NIST CSF leverages current standards, guidelines and best practices from a number of internationally recognized sources.** Although security controls, in and of themselves, don't constitute a cybersecurity framework, they can provide important guidance in the tactical implementation of a cybersecurity program. The NIST CSF includes cross-references to the CIS CSC, COBIT 5, ISA 62443, ISO/IEC 27001, and NIST SP 800-53.[2] "The NIST CSF provides a guide for a more robust security program by cross-referencing these standards," said Suárez.

- **The NIST CSF has been endorsed by healthcare industry heavyweights, including the Healthcare Information Management and Systems Society (HIMSS).** In September 2016, the HIMSS North America Board of Directors approved a HIMSS Cybersecurity Position Statement. HIMSS stated that the framework adopted by the health sector should align with Section 405 of the Cybersecurity Act of 2015, specifically addressing the "voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes."[3] In light of those criteria, HIMSS recommended the NIST CSF as the best fit for the health sector.[4]

- **A majority of the healthcare organizations who have adopted a security framework use the NIST CSF.** A study by HIMSS Analytics, conducted on behalf of Symantec, found that of those healthcare organizations that had adopted a cybersecurity framework, the majority (56 percent) had adopted the NIST CSF.[5] "Adopting the NIST CSF gives you a common language you can speak with your peers," said Finn. "Just like when a specialist in medicine calls for a referral or consult with another specialist. They have a common language and common tools they can talk about. The NIST CSF makes it possible for the chief information security officer (CISO) at Hospital A to call the CISO at Hospital B and to share

[2] "Framework for Improving Critical Infrastructure Cybersecurity," Feb. 12, 2014. National Institute of Standards and Technology (NIST). Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[3] Section 405 of the Cybersecurity Act of 2015 is codified at 6 U.S.C. §1533 (2016).

[4] "HIMSS Cybersecurity Position Statement," Sept. 30, 2016. Retrieved from http://www.himss.org/sites/himssorg/files/hna-cybersecurity-position-statement.pdf

[5] "IT Security Strategy," 2016. Study conducted by HIMSS Analytics, on behalf of Symantec.

a common language when they talk about what to do about a particular cybersecurity problem."

- **The NIST CSF has become the standard for the U.S. Government.** The NST CSF as originally released in 2014 was voluntary. An Executive Order issued in May 2017 by President Donald Trump changed that.[6] All agencies of the U.S. Government are now required to use the NIST CSF to manage cybersecurity risk.[7] "If you are in healthcare, you are tied to a lot of federal agencies," said Finn. "If you accept Medicare or Medicaid, even if they are administered by the state, the funding is federal. At some point, those NIST CSF requirements will trickle down. So there are a lot of reasons for healthcare to be at the front end of that, adopting and using the NIST CSF before it becomes a requirement."

- **The NIST CSF is emerging as a national standard across industries.** A 2016 study of U.S. information technology and security professionals across industry sectors found that 30 percent of U.S. business across industry sectors already use the NIST CSF.[8] "The reason this is important for healthcare is that the healthcare sector is dependent on the other sectors," said Barrett. "For example, healthcare is dependent upon the energy sector, the financial services sector, the information technology sector and the emergency services sector. Communication about cybersecurity needs to be precise and efficient not only within sectors, but across sectors. So if the energy sector and the financial services sector and the healthcare sector all adopt the NIST CSF, there is not going to be a lot of wasted time and effort trying to align communications around cybersecurity."

- **The NIST CSF is customizable**. "The NIST CSF provides a template for your organization's cybersecurity framework," said Suárez. "The rest is up to you. It's like having a palette of colors to paint a canvas. The colors are what you combine to create your painting; and your painting is going to be what cybersecurity looks like for your specific organization. The NIST CSF gives you that palette to start with."

- **The NIST CSF is scalable**. There are enormous variations in organization size within the healthcare industry, from one-physician practices to large, multi-national corporations. The NIST CSF is flexible enough to accommodate organizations at both ends of the spectrum. "Everything in the NIST CSF is scalable," said Barrett. "For example, there is one subcategory of the framework that requires you to establish and communicate your business objectives and business priorities. Some well-resourced organizations will fulfill that subcategory with a 100-page business plan. But a smaller organization might capture that in a page, or a paragraph. The extent to which you fulfill a given subcategory is not prescribed, and therein lies a lot of the scaling capability of the framework."

- **The NIST CSF is affordable.** Unlike commercial frameworks, all of the resources an organization needs to adopt and implement the NIST CSF are available for free. The Framework itself, as well as supporting documentation, video presentations, FAQs, industry-specific resources and implementation guides, are available at: https://www.nist.gov/cyberframework. Some organizations may choose to hire an outside vendor to assist in conducting an initial, Office of Civil Rights (OCR)-compliant risk assessment, or to assist in implementing the framework across a large, complex enterprise, but this is not required.

- **The NIST CSF does not require certification.** Some cybersecurity framework vendors offer 'certification' services for a fee. The implication is that 'certification' will protect a healthcare organization in the event of a cybersecurity breach or incident. But in fact, the Office for Civil Rights (OCR) has published guidance indicating that external 'certification' does not ensure compliance with the HIPAA Security Rule.[9] OCR's guidance states: "It is important to note that HHS does not endorse or otherwise recognize private

[6] Exec. Order No. 13800, 3 C.F.R. 22391-22397 (2017). Retrieved from https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[7] Exec. Order No. 13800, 3 C.F.R. 22391-22397 (2017). Retrieved from https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[8] "Trends in Security Framework Adoption: A Survey of IT and Security Professionals," March 2016. Study conducted by Dimensional Research, on behalf of Tenable Network Security. Retrieved from https://www.tenable.com/whitepapers/trends-in-security-framework-adoption

[9] U.S. Department of Health and Human Services, Office for Civil Rights (OCR), HIPAA for Professionals. "Are we required to 'certify' our organization's compliance with the standards of the Security Rule?" Retrieved from https://www.hhs.gov/hipaa/for-professionals/faq/2003/are-we-required-to-certify-our-organizations-compliance-with-the-standards/index.html

> *"A controls checklist can't replace the role of a framework in an organization's information risk management program."*
>
> **Rob Suárez,** Director of Product Security, BD (Becton, Dickinson and Company)

organizations' "certifications" regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a "certification" by an external organization does not preclude HHS from subsequently finding a security violation."[10]

- **The NIST CSF is designed to accommodate changes in technology and changes in the threat landscape.** "The NIST CSF is designed to be a living document," said Barrett. "Both technology and cyberthreats move very, very quickly. The NIST CSF is designed to be agile and adaptable over time, so that it can keep pace with the evolving threat landscape." NIST is using the same inclusive process it used to develop the original version of the framework to develop subsequent iterations. "We will continue taking the best practices and lessons learned from across all industries and pulling them into the framework so all parties can get that value," he said.

Why a Framework Alone is Not Enough

Just as the NIST CSF is a living document, so too is the information risk management process within any organization. Adoption of a cybersecurity framework is an important first step for healthcare organizations, but the framework alone is not sufficient in and of itself to ensure information privacy and security.

"There is no framework you can use once and then you are done – unless nothing in your organization ever changes," said Finn. "One of the big myths around information risk management is that you can do a risk assessment once and then you are finished. People change, processes change, technology changes. The intent of any good information risk management approach is that anytime something changes – whether you've replaced your EHR, or whether you have a new VP of revenue cycle who has a different view of risks than the previous person – you have to reassess your risk and consider whether or not you need to modify your program.

"That's really the power and beauty of the NIST CSF's risk-based approach. It's big enough and broad enough that you don't have to redo everything each time a change occurs, but it does help you evaluate the changes in your risks and exposures when those changes occur," said Finn.

Chaput compares a complete information risk management program to a three-legged stool. "You have the framework, which articulates what you are going to do; you have process, which specifies how you are going to do it; and you have a maturity model, which keeps you in the mindset of continuous process improvement," Chaput said. A complete information risk management strategy combines all three of these components to achieve a holistic and effective information risk management program across the healthcare enterprise.

CLEARWATER COMPLIANCE

About Clearwater Compliance

Clearwater Compliance, LLC is a leading provider of critical infrastructure regulatory compliance and cybersecurity management solutions. Its mission is to empower customers to successfully manage the evolving information security risk landscape. Clearwater solutions have been employed by hundreds of customers including the Fortune 100 and federal government. More information about Clearwater Compliance is at: http://www.Clearwatercompliance.com.

[10] U.S. Department of Health and Human Services, Office for Civil Rights (OCR), HIPAA for Professionals. "Are we required to 'certify' our organization's compliance with the standards of the Security Rule?" Retrieved from https://www.hhs.gov/hipaa/for-professionals/faq/2003/are-we-required-to-certify-our-organizations-compliance-with-the-standards/index.html