Health IT Security Journal

Volume 5, No. 2

A publication of the HITSF

Why healthcare organizations should adopt the NIST Cybersecurity Framework Pg. 2

Ransomware Protection for Healthcare Covered Entities and Business Associates Pg. 5

HEALTH IT SECURITY JOURNAL

Volume 5, No. 2

A PUBLICATION OF THE HITSF

MAY, 2017

Letter from the editor

Dear readers,

This is the fifth year of the Journal and we are very proud to present another issue.

We at the Health Information Technology Security Forum are very excited about health information technology and how to secure it and ultimately, the patient data residing on those systems.

This issue of the Health IT Security Journal offers insight into information security for healthcare practitioners but it is relevant for many other industries as well. We hope you can enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org.

Sincerely,

Hadi Syahrial
Editor in Chief

Why healthcare organizations should adopt the NIST Cybersecurity Framework

Hadi Syahrial

Budi Luhur University

Unlike the millions of other standards out there, the NIST Cybersecurity Framework (CsF) combines the best of existing rules, assessments, regulations and guidelines into a unifying cybersecurity reference guide. The NIST Framework ratifies the move from traditional audit-focused policies toward a more risk-based approach. It is not a checklist, but rather a compilation of industry-leading cybersecurity practices that organizations should consider in building their own cybersecurity programs.

The Framework provides an assessment mechanism that enables organizations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cybersecurity programs.

It comprises three primary components: Profile, Implementation Tiers, and Core.

The Profile component enables organizations to align and improve cybersecurity practices based on their individual business needs, tolerance for risk, and available resources.

The Implementation Tiers help create a context that enables organizations to understand how their current cybersecurity risk-management capabilities stack up against the characteristics described by the Framework.

The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references, and is organized by five continuous functions: Identify, Protect, Detect, Respond, and Recover. The five functions signify the key elements of effective cybersecurity.

Identify helps organizations gain an understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities. Protect helps organizations develop the controls and safeguards necessary to protect against or deter cybersecurity threats. Detect are the steps organizations should consider taking to provide proactive and real-time alerts of cybersecurity-related events. Respond helps organizations develop effective incident response activities. And Recover is the development of continuity plans so organizations can maintain resilience—and get back to business—after a breach.

The Framework breaks down each of these functions into additional categories and then provides helpful guidance. For example, the Identify function has five categories: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy. Under Governance, one of the four subcategories is that an organization should establish an organizational security policy. The subcategory points organizations to standards such as COBIT, ISA, ISO/IEC, and NIST SP 800-53 Rev. 4 for information on how to implement a policy.

NIST released a "final" public draft of the Preliminary Cybersecurity Framework in October of 2013, and the final version was released in February of 2014, which HITRUST formally integrated into the CSF and CSF Assurance Program in April of 2014 with version 6.1.

Based on a collection of cybersecurity standards and industry best practices, the NIST CsF broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication. Whether an organization has a mature risk management program and processes, is developing a program or processes, or has no program or processes, the Framework can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure.

Specifically, the NIST CsF:

- Provides guidance on risk management principles and best practices,
- Provides common language to address and manage cybersecurity risk
- Outlines a structure for organizations to understand and apply cybersecurity risk management, and
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs.

Beyond the stated goals and benefits of the NIST CsF, there are additional potential benefits to healthcare organizations that implement NIST CsF "compliant" information protection programs, such as those based on the HITRUST RMF.

The HITRUST RMF is fully consistent with the recommendations of the NIST CsF, and it will likely be recognized by the Federal Government under the Partner Program. Organizations that receive HITRUST CSF or SECURETexas certification would subsequently benefit from this recognition.

Organizations that correctly implement a NIST CsF-based information protection program can demonstrate a minimal, recognizable level of due care and due diligence for the protection of protected health information (PHI).

There are three key elements that must be addressed to ensure an organization implements a robust and comprehensive cybersecurity program: threat modeling, threat intelligence, and collaboration. Threat modeling may be accomplished either through a traditional risk analysis or the selection of a control baseline from an appropriate security framework. Threat intelligence is essential for an organization to understand and proactively address active and emerging cyber threats, and collaboration with other

public and private sector entities allows an organization to address cyber threats more efficiently and effectively than it otherwise could.

The NIST CsF provides the structure needed to ensure these three key elements are addressed by industry sectors and organizations while providing the flexibility needed to implement the framework.

Healthcare Sector organizations leveraging the HITRUST RMF should use the following seven-step process for implementation.

Step 1: Prioritize and scope organizational components for framework adoption

Step 2: Identify systems and existing risk management approaches within the scope

Step 3: Create a desired risk management profile based on the organization's factors (Target Profile)

Step 4: Conduct a risk assessment

Step 5: Create a current risk management profile based on assessment results (Current Profile)

Step 6: Develop a prioritized action plan of controls and mitigations (Action Plan)

Step 7: Implement the Action Plan

In general, conducting cybersecurity activities based on the NIST CsF enhances the resiliency of the Healthcare Sector organization, but implementation may involve certain challenges.

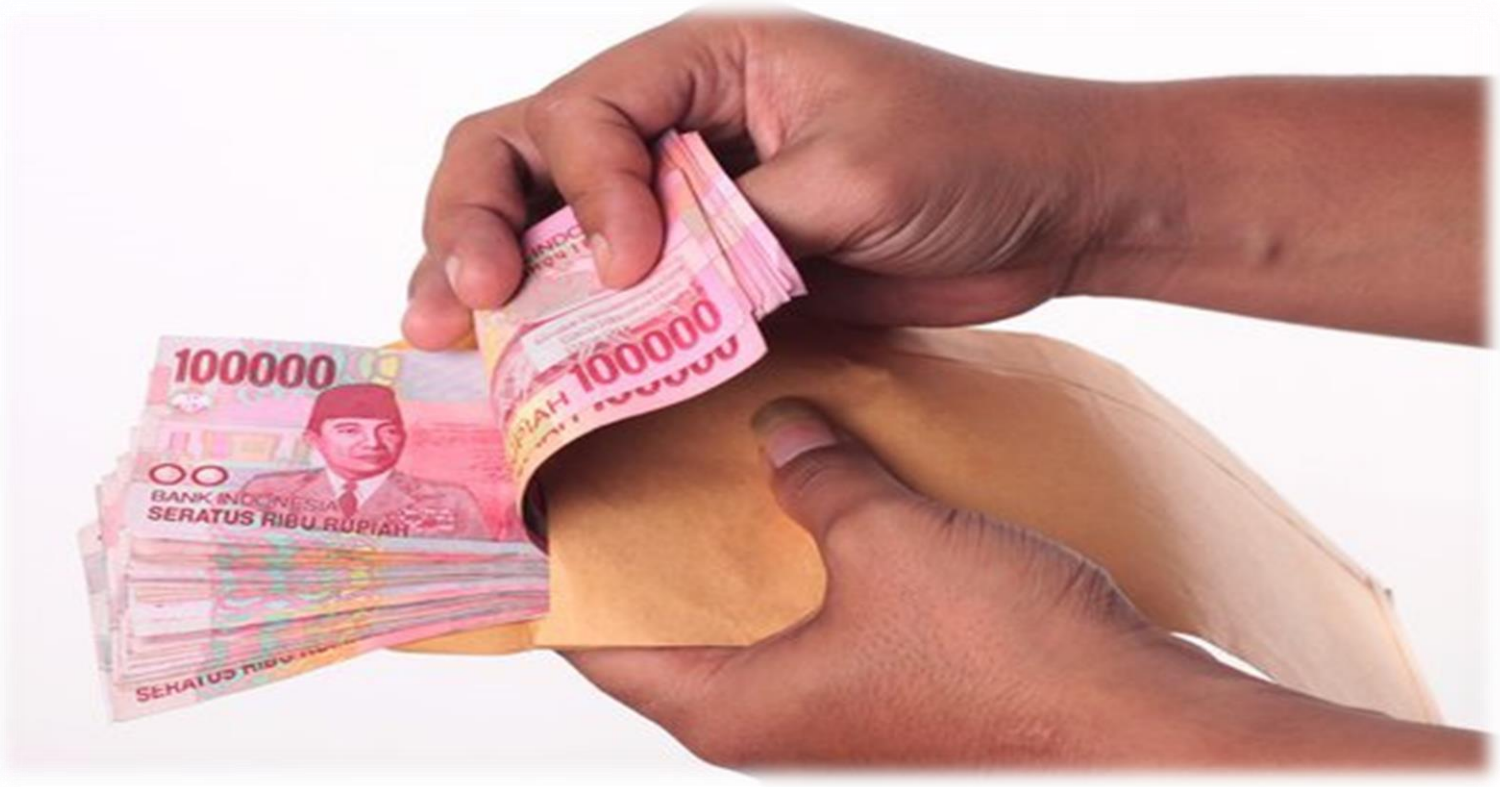
About the Author:

Hadi Syahrial

Hadi Syahrial is a Lecturer and Researcher at Budi Luhur University, Jakarta, Indonesia.

Ransomware Protection for Healthcare Covered Entities and Business Associates

Eric Vanderburg



Ransomware is a form of malware currently taking over at an unprecedented rate and is also becoming a mainstream tool hackers use to separate you from your money. Think of ransomware regarding your patient data or other sensitive information being held hostage by a third party. The way the attacker sets up and executes the attack can lead to a total loss of patient data or other sensitive information unless adequate backups are maintained, or the ransom is paid.

In a ransomware attack, the victim hospital's data or patient data is encrypted with a public key and requires a private key to decrypt the data. The hijacker will then provide the private key for a fee, which is only useful for unlocking the victim's patient data or other sensitive information but not necessarily decrypting it. So there is no guarantee you will get your patient data or other sensitive information back even after you pay the ransom.

Ransomware is often put into a computer system by phishing emails, system vulnerabilities, or via other malware such as a Trojan horse. Ransomware continues to dominate the malware landscape, totaling for over 60% of all malware distributed in March 2017. Already, this is up 10% compared to January this year, underlining the continuing threat and growth of ransomware strains.

The number of cyber attacks where malware holds user data "hostage" is expected to grow in 2017. This is due to hackers targeting more healthcare covered entities and business associates, and advances in ransomware allowing it to compromise more types of data.

Apple devices have often been thought to be somewhat immune to some of the most popular forms of malware, but Palo Alto Networks recently reported that ransomware had been discovered on Apple's phone and tablet IOS and desktop and laptop OSX systems.

Keep in mind that there are new types of ransomware coming out each week. For example, there are a variety of ransomware-as-a-service options such as Alpha blocker and Karmen. What makes RaaS disturbing is the price it is going for. You can purchase RaaS for as little as $65 via Bitcoin. That is less than even the lowest ransoms, so extortionists make their money back with a single paid ransom. With the proof of purchase, attackers can get a copy of the actual ransomware, the master decryptor binary, and their administrative panel. The main selling points of this malware are that it encrypts all drives connected to the PC and continues to encrypt when the computer is turned off. Also, the authors can avoid being caught by periodically pushing updates.

Unfortunately, some organizations are treating ransom demands more like bomb threats and less like cybersecurity incidents. Their default action is to pay the ransom because they do not want to take the risk of not paying when the demand real or losing patient data or other sensitive information due to ineffective data recovery solutions. It is important, therefore, to design and test your backup systems so that you can have the assurance that your healthcare information is recoverable in the case of ransomware.

The question many victims ask is what could have been done differently? Is it possible to get the encrypted patient data or other sensitive information back without paying the ransom?

There are a variety of security companies and researchers that look into ransomware trying to identify flaws in encryption methodologies or obtain master keys from command and control servers. When a particular piece of ransomware is broken, researchers design decryption packages for victims. Check and see if there is a decryption package for your particular ransomware before resorting to paying the extortionist.

What is one way you never have to pay the ransom? Simply, back up your files. The patient data or other sensitive information can be recovered from a backup. Now if you are a business the downtime to get back up and running, not to mention the damage to your businesses reputation will be costly. But then again the media is full of healthcare covered entities and business associates recovering from ransomware attacks so that no one will be surprised. Early detection, remediation, and reliable backups will continue to be some of the best defenses against ransomware attacks.

About the Author:

Eric Vanderburg
Vice President, Cybersecurity
TCDI

Eric Vanderburg is an information security executive, thought leader and author known for his insight on cybersecurity, privacy, data protection and storage. Some have called him the "Sheriff of the Internet" since he and his cybersecurity team at TCDI protect companies from cyber threats, investigate data breaches, and provide guidance on safe computing.

Eric is passionate about sharing knowledge of cybersecurity and technology news, insights and best practices. He regularly presents on security topics and maintains a security blog. You can find him throughout the day posting valuable content on his social media channels.

@evanderburg
inkedin.com/in/evanderburg
facebook.com/VanderburgE

HEALTH IT SECURITY JOURNAL

Volume 5, No. 2

HITSF

HITSF Journal

This journal is a publication of the Health Information Technology Security Forum, an international security organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and can be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health. Learn more at www.healthitsecurity.org

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.