ASA

Annie Searle & Associates LLC

Research Note

Mandatory Cybersecurity Risk Management Framework in Healthcare Sector

Andy Herman

December 2016

Keywords: cybersecurity; healthcare; risk management; electronic health records

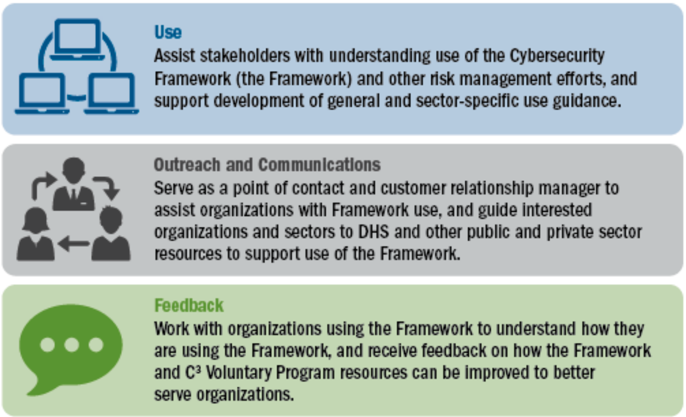
Abstract: This paper explores the gap in the current healthcare cybersecurity approach – that there is no mandatory risk management framework for healthcare organizations. The current method of control for protection of patient information has been through the enforcement of Title 2 of the HIPAA governance. The author suggests introducing a mandatory implementation of a full cybersecurity framework with monitoring systems before receiving the incentives guaranteed by the meaningful use clause associated with electronic health records. While recognizing that the healthcare sector is already burdened with heavy compliance requirements, the key point is that a cybersecurity framework should be considered an operational necessity, not simply a voluntary option.

Breaches in the continuously evolving cyberspace atmosphere have contributed to financial and reputational loss for many organizations across all industries. Of the sixteen critical infrastructure sectors, the healthcare sector has become a sector of increasing interest by both cybersecurity professionals and hackers trying to protect and gain access to the valuable patient health information. Stolen healthcare information including personal identifiable information and insurance numbers has led to identity thefts and painful problems for victims. Research has shown that stolen electronic patient health information is sold on the black market at a rate of $50 per record.[1] Though healthcare data breaches in 2014 were primarily caused by the negligence of physicians (losing devices containing personal identifiable information), "98 percent of data breaches in healthcare in 2015 were a result of hacking and other IT-related incidents."[2] Improvement and maintenance of cybersecurity is one of the main Healthcare and Public Health sector goals. It is imperative to determine the root cause of the breaches and develop mitigation plans to minimize the damage. There are many possible reasons to explain the increase in data breaches this past year, but I feel that the Meaningful Use clause, part of the American Recover and Reinvestment Act of 2009 (ARRA), has contributed the most to creating an atmosphere where hospitals are unprepared. The clause "promises stimulus incentives to physicians using EMR/ medical practice software that meet some still *unspecified* criteria," which exposes them to potential data breaches in the pursuit of compliance driven by a desire for financial gains.[3] The HITECH Act proposed incentive payments to accelerate "the adoption of HIT and use of qualified EHR."[4] The intent of the massive overhaul to electronic health records was to improve the quality of care that physicians could provide patients. Though the benefits of shifting to new technology increases the potential for improved quality of care, there are vulnerabilities with the implementation of this program that creates a risk to one of the most important infrastructures in our country. Therefore, the sector would benefit from an additional requirement for electronic health records - meaningful use (EHR-MU) requiring that institutions under HIPAA implement a cybersecurity program that uses the NIST Cybersecurity Framework. Understanding that healthcare organizations are already under a lot of pressure to maintain compliance to HIPAA, mandatory cybersecurity risk assessment programs should be considered if the goal of the EHR-MU is to improve the quality of care.

The Office of the National Coordinator of Health Information Technology (ONC) is located within the Office of Secretary of the U.S. Department of Health and Human Services (HHS). One of the missions of the ONC is to "[coordinate] nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information."[5] The ONC should be concerned about this issue of cybersecurity because of the risk for loss of electronic health records, which pose an operational risk to the mission of healthcare organizations. The ONC recommends that healthcare organizations conduct a risk assessment to reduce the likelihood of these events happening.[6] They provide a toolkit that is not required by the HIPAA security rule, but provides a method of being vigilant and compliant with the guidelines of HIPAA. Furthermore, the ONC's program (SRA Tool) asks 156 Boolean logic questions that align with HIPAA requirements.[7] The SRA Tool provides merely a statistical outline of what areas are currently at risk but does not offer controls and metrics to monitor improvement. The ONC has published and released numerous flyers and information packets to help healthcare organizations become more informed about healthcare cybersecurity. The ONC has done a great job in increasing awareness of cybersecurity. The next step is to implement health information technology with the proper establishment of cybersecurity frameworks and mitigation plans *before* the complete transition by hospitals to electronic health records in both private and public sectors of healthcare.

Another government entity whose operational risk can be mitigated by the proper implementation of a mandatory cybersecurity framework is the Center for Disease Control (CDC). The CDC and the ONC have collaborated to modernize medicine through the implementation of electronic health records (EMR). They have spearheaded the movement towards ERM adoption and have held workshops to inform and create awareness about the benefits that ERM can provide to the healthcare sector. In 2007, the CDC and ONC held their first EMR workshop. At this event, they stated that "privacy, security, medical legal issues, cultural change, and workforce" would be relevant issues to the topic of "improving health-care statistics through EMR and health information exchange."[8] This initiative by the CDC illustrates that the CDC and ONC were concerned about the security of the electronic patient information gathered in the pursuit of increased quality of care. Unfortunately, an analysis of the events at the EMR workshop showed no further evidence that addressed how organizations could secure information or what protocols should be considered. The CDC has worked with other organizations to continue to increase participation of healthcare organizations in the transition to electronic health records. On October 16, 2012, the CDC collaborated with the Association of Public Health Laboratories to publish the "Clarification Document for EHR Technology Certification." This document is intended to document the requirements to be considered properly certified as an ELR (Electronic Lab Record) compliant technology.[9] While scanning this document, it became evident that there is no clarification on this document regarding the requirements for a risk assessment or mitigation plan to protect health information. Recall the mission of the HITECH ACT was to improve the quality of care by implementing technology to make the delivery of healthcare efficient. The lack of emphasis on the implementation of a cybersecurity framework as an important aspect of the transition to electronic health records will act as an operational risk because the potential for breaches that threaten personal identifiable information of patients. This operational risk could potentially lead to the decrease in the quality of care.

The current method of control for protection of patient information has been through the enforcement of Title 2 of the HIPAA governance. Title 2 of HIPAA has five rules: Privacy Rule, Security Rule, Transactions and Code Set Rules, the Unique Identifiers Rule, and the Enforcement Rule. The Privacy and Security rule will be the focus points of this paper, particularly as it relates to protecting electronic healthcare information. The Privacy Rule establishes the standards that are associated with "giving patients the right to access and request amendment of their PHI [Protected Health Information] as well as requesting restrictions on the use or disclosure of such information."[10] The Security Rule sets a "national set of security standards for the confidentiality, integrity and availability of EPHI."[11] The HIPAA provides a guideline, rules, and regulation for healthcare organizations to follow to ensure patient information is protected. Cybersecurity compliance to these rules and regulations can be generally met using the cybersecurity frameworks established by NIST. Hospitals generally adapt the cybersecurity framework as the foundations to their cybersecurity programs before adapting parts of the program to fit the needs of their own



Use
Assist stakeholders with understanding use of the Cybersecurity Framework (the Framework) and other risk management efforts, and support development of general and sector-specific use guidance.

Outreach and Communications
Serve as a point of contact and customer relationship manager to assist organizations with Framework use, and guide interested organizations and sectors to DHS and other public and private sector resources to support use of the Framework.

Feedback
Work with organizations using the Framework to understand how they are using the Framework, and receive feedback on how the Framework and C³ Voluntary Program resources can be improved to better serve organizations.

organization.[12]

Another control that is currently in place is the Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which was signed by President Obama on February 12, 2013.[13] This executive order was established to address the concerns of our nation's cyber infrastructure. It consists of three main areas: "(1) information sharing, (2) privacy, (3) the adoption of cybersecurity practices."[14] The President tasked the Department of Homeland Security to develop a voluntary program to help promote the cybersecurity framework that NIST was ultimately able to create. This voluntary program is called the "C^3 Voluntary Program." C^3 Voluntary Program was launched in 2014 alongside the final version of the NIST cybersecurity framework. The purpose of the C^3 Voluntary Program is to "assist stakeholders with understanding use of the [Cybersecurity] Framework and other cyber risk management efforts, and support the development of general and sector-specific guidance for framework implementation."[15] The benefits of having a voluntary range from less pressure and more flexibility, but the disadvantages of a voluntary implementation of a cybersecurity framework is the potential for a lackadaisical attitude towards security. Organizations will see the word "voluntary" and it may suggest a lower importance in implementing. In 2014, the Healthcare Information and Management Systems Society (HIMSS) has been noted as accurately saying that "HIPAA compliance is not equal to security" and that the NIST cybersecurity framework is critical in the bridging of the gap between compliance and security.[16] The irony is that though HIMSS understood the importance of security of healthcare information, they recently wrote a letter to NIST to request that the NIST Cybersecurity Framework remain voluntary. HIMSS "acknowledges that healthcare organizations can benefit from improving their risk management process and better address cybersecurity risks."[17] However, the argument for the necessity of the cybersecurity framework to be voluntary was based on the following reason:

Figure 1: C3 Voluntary Program Graphic (Source: https://www.us-cert.gov/ccubedvp)

> "To 'prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes' as required by the Cybersecurity Enhancement Act of 2014, the NIST Cybersecurity Framework should continue to be voluntary, consistent with Section 405 of CSA."[18]

This helped me understand the argument presented by HIMSS to allow the NIST cybersecurity to remain voluntary. Since the healthcare sector is already burdened with having to comply with HIPAA and HITECH Act, it is understandable that they may not want to be forced into compliance with another form of governance. However, it is important to understand that the mandatory cybersecurity framework should not be seen as a nuisance and especially if the physicians are seeking to gain some financial incentives through the EHR–MU incentive program, it is imperative that the organizations are prepared to protect the patients.

The EHR-MU is currently divided into three stages: stage 1, stage 2, and stage 3. Stage 1 requires that the provider meet a set of fifteen core requirements and five from the optional list to receive the incentives that "range from $44,000 (through Medicare) to $63,750 (through Medicaid)."[19] The organization must be in each stage for at least two calendar years before they can qualify for the next stage. Upon reading through a detailed core requirements form, there were no mentions of the voluntary cybersecurity framework. The requirements did mention the use of EHR certified technology. If the hospital could prove that they were able to use the EHR certified technology they were considered to have fulfilled the requirements for that task. As mentioned earlier, even the process of certification of the EHR-enabled technology does not include a clear procedure to ensure cybersecurity.

An example of when the lack of proper implementation of cybersecurity in the public sector of healthcare had negative effects can be demonstrated by one of the biggest HIPAA violations at St. Joseph Health System in Bryan, Texas. On December 2013, St. Joseph Health System "experienced a three-day long data security attack" which resulted in hackers gaining access to the protected health information of 405,000 patients at the hospital.[20] The technology that was used at St. Joseph Health System was "certified EHR technology" using the guidelines provided by the CDC. Furthermore, a review of the financial statements showed that the St. Joseph Health System received $1,954,000 in 2013 and $5,103,000 in 2014 upon "demonstration of compliance with the criteria for meaningful use incentives" from the Centers for Medicare and Medicaid Services.[21] The evidence revealed in the financial reports indicated that St. Joseph's Health System is participating in Stage 1 of the Meaningful Use Incentive program. Furthermore, this meant that the core objectives were being met. Though there was evidence of an electronic system to maintain patient information, an analysis of the organizational chart of the hospital indicated that the management of this system was not by a CISO but the only IT staff member who carried the title of "site director." [22] From this example, we can see the risks that are associated with the promotion of Meaningful Use Incentive Program without proper implementation of cybersecurity can potentially lead to huge breaches. It is difficult to jump to conclusions that a better cybersecurity program will have prevented this information breach, however, when looking at the history of third-party hackers gaining unauthorized access to servers, some of these cases can be deterred by a simple implementation of a cybersecurity framework.

There are many hazards that are associated the rush that physicians are going through to gain financial incentives of the meaningful use clause. Rushing to fulfill the meaningful use clause of the ARRA, which "promises stimulus incentives to physicians using EMR/ Medical practice software that meet some still unspecified criteria" can result in negligence in security of valuable information.[23] Dr. Steven Waldren, an information technology expert from the American Academy of Family Physicians, proposed that "the meaningful-use program [has] pushed some medical practices to implement EHRs even though they weren't exactly ready to."[24] As we saw with the example of St. Joseph Health System, the incentive program can present huge operational risk because the lack of controls and preparedness to handle the security of EHRs. Financial gains are often the critical factor in leading to negligence and overlooking the importance of preparing the proper infrastructure and cybersecurity environment before implementation. Acknowledging that there is great potential for improvement of the quality of care with a well-organized electronic health records system, I have proposed the idea of having a "Step 0" which would remove the *voluntary* cybersecurity framework implementation suggestion and *enforce* the implementation of a full cybersecurity framework with monitoring systems before receiving the incentives guaranteed by the EHR-MU. As mentioned by HIMSS, mere compliance to governance such as HIPAA will never guarantee complete security. Having electronic health record systems that merely comply with the rules and standards for HIPAA should not be the minimum requirement to increase the use of IT systems in healthcare. I believe it is critical to not lose focus on the importance of improvement of quality of care over the opportunity for financial gains. From my personal experience being with physicians, this distinction is frequently overlooked.

In conclusion, when comparing the impact that this mandatory emphasis on cybersecurity has on healthcare with other critical infrastructure sectors in the United States, we will be able to observe the overall improvement in safety across the different sectors. In this increasingly technologically dependent society, it is important to increase the awareness of the importance of cybersecurity. Cyber crimes and breaches to databases across all industries lead to President Obama signing the Executive Order 13636 to improve critical infrastructure cybersecurity.[25] Estimates from various economic studies have stated that cyber crime "costs the global economy over $400 billion per year."[26] The Executive Order 13636 did not want to make the implementation a mandatory process because the government does not want to be accused of pressuring private sectors into more regulatory laws. The meaningful use clause of the American Recovery and Reinvestment Act hopes to contribute to the improvement of the integration of health information technology for the overall increase in quality of care. This should not be rushed and careful consideration for the NIST cybersecurity framework as a mandatory aspect should be considered. In a field as expansive as healthcare, the successful implementation of a cybersecurity framework has the potential to act as a catalyst for other sectors to follow suit to maintain their security and potentially reduce the number of breaches.

[1] Lowe, H. "Stolen EHR Charts Sell for $50 Each on Black Market". Medscape Medical News, 2014.

[2] Landi, Heather. "Hacking Accounted for 98 Percent of Healthcare Data Breaches in 2015, Report Says - Dolbey Systems, Inc." *Dolbey Systems Inc*. Healthcare Informatics, 04 Feb. 2016. Web. 14 Feb. 2016.

[3] Needle, Sheldon. "How Much Should Doctors Worry About 'Meaningful Use'?" (CTS Medical Blog, December 1, 2012)

[4] Federal Registrer. "Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule". *Department of Health and Human Services*. 28, July 2010.

[5] "About ONC", HealthIT.gov, August 11, 2014.

[6] Ibid.

[7] Health IT. "Security Risk Assessment." *Security Risk Assessment Tool*. 26 June 2015. Web. 15 Feb. 2016.

[8] Center for Disease Control and Prevention. “Improving Health-Care Statistics Through Electronic Medical Records and Health Information Exchange”. EMR Workshop. 29 May 2007. Web. 23 Feb. 2016

[9] Centers for Disease Control and Prevention, Association of Public Health Laboratories. “ELR 2.5.1 Clarification Document for EHR Technology Certification”. 16 October 2012.

[10] “Cybersecurity: A Shared Responsibility”, HealthIT.gov, (January 12, 2015).

[11] Ibid.

[12] Ewell, Cris V., Dr. "Foundations of Organizational Information Assurance." IMT 551A Lecture. University of Washington, Seattle. 5 Oct. 2015. Lecture.

[13] The White House. "Foreign Policy Cyber Security Executive Order 13636." *The White House*. The White House, 12 Feb. 2013. Web. 02 Mar. 2016.

[14] Ibid.

[15] Homeland Security. "Critical Infrastructure Cyber Community C^3 Voluntary Program." *Critical Infrastructure*. 14 Oct. 2015. Web. 18 Feb. 2016.

[16] Hall, Susan D. "HIMSS Seeks Specific Guidance from NIST on Cybersecurity Framework." *FierceHealthIT*. 14 Oct. 2014. Web. 18 Feb. 2016.

[17] Monegain, Bernie. "HIMSS Presses NIST to Keep Cybersecurity Framework Voluntary for Organizations." *Healthcare IT News*. 10 Feb. 2016. Web. 03 Mar. 2016.

[18] Ibid.

[19] HealthIT.gov. "EHR Incentives & Certification." *Information about EHR Incentives and EHR Certification*. 4 Apr. 2014. Web. 04 Mar. 2016.

[20] McCann, Erin. "Hackers Swipe Health Data of 405K." *Healthcare IT News*. 05 Feb. 2014. Web. 25 Feb. 2016.

[21] Ernst & Young LLP. *Consolidated Financial Statements and Supplementary Information*. Rep. Irvine: Ernst & Young LLP, 2014. Print. (Page 27)

[22] St. Joseph Health. "Leadership and Governance." *Leadership and Governance*. 2016. Web. 26 Feb. 2016.

[23] Needle, Sheldon. “How Much Should Doctors Worry About ‘Meaningful Use’?” (CTS Medical Blog, December 1, 2012)

[24] Lowe, H. “Stolen EHR Charts Sell for $50 Each on Black Market”. Medscape Medical News, 2014.

[25] The White House. "Foreign Policy Cyber Security Executive Order 13636." *The White House*. The White House, 12 Feb. 2013. Web. 02 Mar. 2016.

[26] Gabel, Detlav, Bertrad Liard, and Daren Orzechowski. "Cyber Risk: Why Cyber Security Is Important."

Cyber Risk: Why Cyber Security Is Important. 1 July 2015. Web. 03 Mar. 2016.