November 2016

THE KOSCIUSZKO INSTITUTE

THE KOSCIUSZKO INSTITUTE POLICY BRIEF

Aaron Ostrovsky

Digitalized Healthcare Sector – A New Frontline of Cybersecurity

author

Aaron Ostrovsky is Systems Analyst Specialist at a major Hospital in New York City. Aaron holds a BA in Russian Studies from Bates College, a MA in Central and Eastern European History from Central European University, a Health Information Technology Graduate Certificate from Weill Cornell Medical College and a MPH in Public Health from the George Washington University. Aaron is currently pursuing his PhD in Biomedical Informatics from Rutgers University.

Cybersecurity has changed the digital landscape forcing a multitude of industries to assess their abilities to protect and secure sensitive data, evaluate newer forms of technology and implement security measures to enforce securer IT environments. The healthcare industry in the United States, in particular, has had a drastic shift over the last ten years as both physician offices and hospitals adopt electronic health records (EHR).

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17th, 2009, as part of the American Recovery and Reinvestment Act (ARRA), with the goal of promoting the adoption of health information technology. The Act seeks to improve health care delivery and patient care by offering financial incentives to healthcare providers that demonstrate meaningful use of electronic health records (EHR). The Office of the National Coordinator for Health Information Technology (ONC) leads the charge, as mandated by HITECH, of incorporating the use of health information technology (IT) into the U.S. healthcare system. This push for utilizing information technology as a platform to better assist in the management of patient care, reduction of medical errors and streamlining clinical workflows requires that this technology truly aim to improve care through meaningful use.

Meaningful use is defined, by HITECH, as “the use of certified EHR technology in a meaningful manner; ensuring that the certified EHR technology is connected in a manner that provides for the electronic exchange of health information to improve the quality of care; and that in using certified EHR technology the provider must submit to the Secretary of Health

& Human Services (HHS) information on quality of care and other measures."[1] The fundamental goals of meaningful use and health outcomes policy priorities are the following:[2]

- Improve quality, efficiency, safety and reducing health disparities;
- Improve population and public health;
- Ensure adequate privacy and security protection for personal health information;
- Improve care coordination

In order to accomplish these priorities, meaningful use was established through a phased approach, which is divided into three pivotal phases: data, advanced clinical processes and improved/expected outcomes. To qualify and receive incentive payments the following criteria must be achieved under meaningful use:

1. The use of a certified EHR in a meaningful manner, such as electronic medication prescribing
2. The use of certified EHR technology for electronic exchange of health information to improve quality of health care.
3. The use of certified EHR technology to submit clinical quality and other measures

Serving as the primary piece of legislation, the HITECH Act directs federal health IT policies and programs. The Congressional Budget Office (CBO) predicts that roughly $37.2 billion will be spent in Medicare and Medicaid through HITECH from 2009-2019.[3] The HITECH Act has $2 billion in grant programs to fund the following: health IT infrastructure, resource centers, workforce programs, privacy and security programs and research projects. In addition, HITECH provides grants to states to offer low-interest loans to assist providers in the financing of their health IT initiative. Currently, as of March 1st, 2013, about $1.985 billion of the $2 billion has been distributed.[4] Medicare incentive payments for those providers or hospitals that adopt and use EHRs are funded through HITECH. Eventually, the incentive program will be replaced with penalties for those not meeting and satisfying the meaningful use standards. Certain Medicaid providers, under the HITECH Act, receive 100% funding from the government to adopt a certified EHR system; as of recently, $12.7 billion in total has been provided to nearly 388,593 providers or hospitals.[5]

The volume increase of digitalized medical data has unfortunately placed a target on the healthcare industry.

The volume increase of digitalized medical data has unfortunately placed a target on the healthcare industry. The Workgroup for Electronic Data Interchange (WEDI) estimates that between 2010 and 2014, roughly 37 million healthcare records have been compromised by cyber attacks.[6] In addition to the growing adoption of EHRs, other technologies such as medical devices and wearable's have become an increasingly valuable source of patient data.

According to Fortinet, a cyber security solutions company, the first four months of 2015 saw 93 separate attacks that impacted nearly 99 million healthcare records.[7] Unfortunately the evolution of technology in the healthcare industry has provided a lucrative landscape that has become vulnerable to cyber attacks.

Cyber Attacks

In a 2016 report by Ponemon Institute, cyber attacks have nearly doubled over the last five years. Ponemon Institute estimates that an average data breach costs a hospital roughly $2.1 million; nationally it has been estimated that cyber attacks targeted towards hospitals and doctors has cost the healthcare system in

[1] Meaningful Use (Internet) 2016, September 3rd – Available from: http://www.cdc.gov/EHRmeaningfuluse/introduction.html

[2] Meaningful Use (Internet) 2016, September 3rd – Available from: http://www.cdc.gov/EHRmeaningfuluse/introduction.html

[3] Senators Thune, Alexander, Roberts, Burr, Coburn, Enzi. Reboot: Re-Examining the Strategies Needed to Successfully Adopt Health IT. United States Senate, April 16th, 2013

[4] Senators Thune, Alexander, Roberts, Burr, Coburn, Enzi. Reboot: Re-Examining the Strategies Needed to Successfully Adopt Health IT. United States Senate, April 16th, 2013

[5] Ibid

[6] WEDI, "WEDI Releases Perspectives on Cybersecurity in Healthcare Primer" (Internet) September 6th, 2016. Available from – http://www.wedi.org/news/press-releases/2015/06/22/wedi-releases-perspectives-on-cybersecurity-in-health -care-primer

[7] Ibid

the U.S. around $6 billion a year.[8] The healthcare sector has become a treasure trove of sensitive data that can be exploited for large amounts of money.

In 2013, Executive Editor of Healthcare Information and Management Systems Society (HIMSS) Media Tom Sullivan commented on the transition from a paper-based to an electronic one, "it's harder to steal millions of paper records than electronic ones. But as more EHRs create a digitalized health system where health information exchanges (HIEs) and health insurance exchanges are the norm, electronic health data is widely shared and an increasing amount of it stored in clouds and other central repositories, from where it can be accessed by a variety of mobile devices, well that is already changing. Add to it the rocket-like proliferation of mobile devices, easily-lost and frequently unencrypted."[9]

According to a 2015 Breach Level Index report issued by Gemalto, a digital security company, the healthcare industry in the United States experienced 187 breaches occurred in the first half of 2015, which accounts for roughly 21.1% of all data breaches in that year. According to this report, the U.S. Government and the Healthcare Industry collectively have suffered the most in terms of data breaches; both these industries account for roughly two-thirds of compromised data records.[10] The Verizon Data Breach Report (DBIR) of 2016 estimated that the Healthcare industry experienced roughly 166 security incidents in 2015; 115 of these security incidents have confirmed instances of data loss.[11] While these reports provide some insight into the breach activity within the healthcare sector it's likely that numbers are actually higher, either because attacks are going unreported or undetected.

As of June 2016, nearly 632 health IT vendors have supplied 337,432 ambulatory primary care physicians, podiatrists, medical specialist, surgical specialists and dentists with certified EHR software to facilitate and streamline patient care.[12] This government-sponsored transition to an increasingly electronic ecosystem has contributed greatly to improving patient care including reducing errors and streamlining complicated workflows. However, this transition has also created a dependency on technology, which unfortunately exposes a new form of sensitive data to risk.

According to a 2015 Pricewaterhouse Coopers (PwC) report, by 2020, healthcare products with Internet connection are expected to grow in value by an estimated $285 billion.[13] This economic value projection, however, will potentially increase targeted attacks. In 2014, roughly 85% of large healthcare organizations experienced, at varying levels, a data breach; nearly 18% of these breaches costs more than $1 million to correct.[14] Retired U.S. Army Colonel Jeff Schilling, currently Chief Security Officer at Armor Inc., commented that protecting health data "comes down to network architecture and design." Schilling additionally stated, "Medical devices need to be segmented apart from other devices on a hospital's network. This is one of the very few cases where a cyber actor could take action and hurt someone very quickly."[15] It was not until 2015 that the first ever government warning surrounding medical devices was issued. The U.S. Food and Drug Administration (FDA) on May 13th, 2015, the FDA released communication surrounding the vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems.[16] Security Researcher Billy Rios identified vulnerabilities within the infusion pump models, which could be targeted remotely by infiltrating a hospital's network. Common security exploits, which include gaining unauthorized remote access, have been

[8] Pettypiece, Shannon "Rising Cyber Attacks Costing Health System $6 Billion Annually," Bloomberg Technology, May 7th, 2015. Available from – http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually

[9] Sullivan, Tom. "Are providers ripe for massive medical records heist? Government Health IT, January 14th, 2013. Available from – http://www.healthcareitnews.com/news/are-providers-ripe-massive-medical-records-heist

[10] Gemalto, "Findings from the Breach Level Index" (Internet) September 3rd, 2016. Available from – http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx

[11] Verizon, "2016 Data Breach Investigations Report" September 17th, 2016. Available from – http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

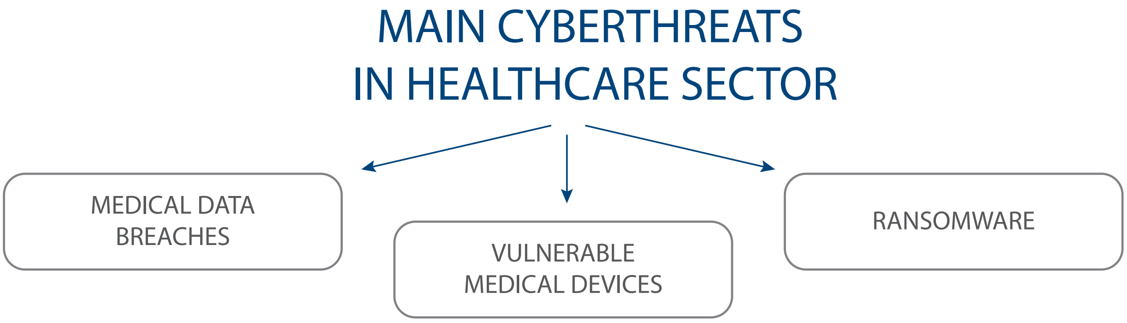
[12] The Office of the National Coordinator for Health Information Technology, Health IT Dashboard, 2016 September 3rd. Available from – http://dashboard.healthit.gov/quickstats/quickstats.php

[13] PwC Cybersecurity Report (Internet) September 3rd, 2016. Available from – http://www.pwc.com/us/en/health-industries/top-health-industry-issues/cybersecurity.html

[14] Ibid

[15] Ibid

[16] U.S. Food & Drug, Medical Devices & Cyber Security (Internet) September 3rd, 2016. Available from – http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm



MAIN CYBERTHREATS IN HEALTHCARE SECTOR

MEDICAL DATA BREACHES

VULNERABLE MEDICAL DEVICES

RANSOMWARE

associated with the use incorrect use of protocols such as hypertext transfer protocol (HTTP), anonymous file transfer protocol (FTP), exposed remote desktop protocol (RDP), SSH, telnet, etc. In addition, coding flaws in the systems, applications, and medical devices used by healthcare organizations can lead to compromises and breaches due to security exploits like buffer overflows, cross-site scripting (XSS), SQL injection, and cross-site request forgery (CSRF).

Vulnerable medical devices are not the only security threats faced by healthcare organizations. Ransomware, a form of malicious software (or "malware") designed to restrict users from accessing their systems or files, has hit the healthcare industry particularly hard over the past couple of years This type of malware is typically sent through "phishing", intended to trick unsuspecting users into opening malicious attachments.[17] Ransomware has grown to such a threat that in March 2016, the U.S. Department of Homeland Security (DHS) issued an alert about the proliferation of two variants of Ransomware, Locky and Samas, which were targeting healthcare organizations and hospitals.[18]

In May 2016, the Kansas Heart Hospital fell victim to a Ransomware attack. Kansas Heart Hospital paid the initial ransom but refused to pay the second request; this was the second hospital to publicly admit to paying a ransom. Hollywood Presbyterian in February of the same year paid $17,000 to their attackers.[19] Vice President of Fortinet Ryan Witt stated that "Demands for funds are soaring, and the problem is organizations are paying. Ransomware will get worse before it gets better… you don't want to think of return on investment as it pertains to criminal activity, but there is a strong ROI, and these attackers are quite sophisticated and know where there is money to be made."[20]

As cyber-attacks occurrences continue to threaten the healthcare industry new preventive security mechanisms and standards must be enforced in order to safeguard medical data.

Cyber attacks are not limited to hospitals and provider organizations. Healthcare insurance companies, for example, have also fell victim to such attacks. On February 4th, 2015, Anthem, Inc., publicly admitted that nearly 78.8 million current and former members and employee's information was compromised by a cyber-attack. Ken Dort, a cybersecurity professional, at Drinker Biddle & Reath, commented that the "insurers have probably so many different legacy systems bolted onto older systems… they may not be quite as synchronized as much as they should be."[21] The long-term impact of this attack has yet to be fully realized. Similarly, on January 29th 2015, Premera Blue Cross, an insurance company located in the Pacific Northwest, revealed that nearly 11 million records had been comprised by a cyber-

[17] United States Computer Emergency Readiness Team, Alert (TA16-091A) Ransomware and Recent Variants (Internet) September 3rd, 2016. Available from – https://www.us-cert.gov/ncas/alerts/TA16-091A

[18] Gendre, Andrien. "Hospitals and Ransomware: Phishing and Healthcare," *VadeSecure*, April 21st, 2016. Available from – http://blog.vadesecure.com/en/hospitals-ransomware-phishing-healthcare/

[19] Siwicki, Bill. "Ransomware attackers collect randsom from Kansas hospital, don't unlock all the data, then demand more money," *Healthcare IT News*, May 23rd 2016. Available from – http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom

[20] Ibid

[21] Herman, Bob "Details of Anthem's massive cyberattack remain in the dark a year later," *Modern Healthcare*, March 30th, 2016. Available from – http://www.modernhealthcare.com/article/20160330/NEWS/160339997

attack through unauthorized access to their information technology systems. As a means of appeasing angered customers, Premera issued two years of free credit monitoring and identity theft protection for those affected;[22] Despite the offer of identity protection, since the breach, Premera has been hit with multiple class action lawsuits by patients reporting attempted fraud.[23]

As cyber-attacks occurrences continue to threaten the healthcare industry new preventive security mechanisms and standards must be enforced in order to safeguard medical data.

Defense Mechanisms:

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, serves as the current national standard for protecting the security and privacy of particular health information. The U.S. Department of Health and Human Services (HHS), under title II of HIPAA that focuses on the procedures and standards for ensuring the security and privacy of identifiable health information, published the HIPAA Privacy Rule and HIPAA Security Rule. Although not a defined security standard model, HIPAA requirements could be interpreted as the following:[24]

- Transport encryption – electronic protected health information (ePHI) must use encryption for transmitted and must securely exchange data via SSL/TLS

- Storage encryption – HIPAA controls outline the encryption of data "at rest." This required encryption does not specify how an organization might define their internal processes for storage encryption

- Integrity – Data integrity is assured through the consistency and accuracy of the data. The data cannot be maliciously or accidently modified

- Disposal – If needed, an entities' data can be permanently purged; this includes data that is identified for archiving.

- Authorization – Access to sensitive data is only granted to authorized personnel. Hosting providers, as stated by HIPAA compliance, must agree to a Business Associate Agreement (BAA)

- Backup – ePHI should be effectively backed up so that data recovery and restoration is available in the case of emergency

The Security Rule, specifically, "establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[25] This rule in conjunction with the Privacy Rule strive to safeguard how electronic protected health information is used but also how organizations like "covered entities*" interact with such sensitive data. In addition to the administrative, technical and physical safeguards outline under the Security Rule, risk analysis is a required capability that must be performed by an organization's security management processes.

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Although this line of defense exists, newer technologies and methods of infiltration have forced government agencies, like the Office for Civil Rights (OCR), to address the current gaps in cybersecurity by cross-walking the HIPAA Security Rule and

[22] Premera "Premera Blue Cross Announces Cyberattack, Offers Protection for Affected Individuals" (Internet) September 3rd, 2016. Available from – https://www.premera.com/wa/visitor/about-premera/press-releases/2015_03_17/

[23] Garnick, Coral, "Premera negligent in data breach, 5 lawsuits claim," *The Seattle Times*, March 27th, 2015. Available from – http://www.seattletimes.com/seattle-news/premera-negligent-in-data-breach-5-lawsuits-claim/

[24] Hosting Edge, "A proactive approach to cybersecurity in healthcare: Going beyond HIPAA compliance (Internet) September 5th, 2016 – Available from – https://www.edgehosting.com/blog/2015/11/a-proactive-approach-to-cyber-security-in-healthcare-going-beyond-hipaa-compliance/

[25] HHS.gov, Health Information Privacy (Internet) September 5th, 2016. Available from – http://www.hhs.gov/hipaa/for-professionals/security/index.html

* Covered entities are defined in HIPAA as the following: health care clearing-houses, health plans and health care provides which electronically submit health information (https://privacyruleandresearch.nih.gov/pr_06.asp)

the National Institute of Standards and Technology (NIST) Cybersecurity Framework. NIST, a non-regulatory agency of the U.S. Department of Commerce, "promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."[26] A large part of this mission is the development and use of standards. In February of 2013, President Barack Obama issued Executive Order 13636 (EO) which called for a cybersecurity framework that offers a "prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services."[27] On February 12th, 2014, NIST issued a cybersecurity framework for improving critical infrastructure that would address the needs outlined in the executive order.

The crosswalk analysis performed by OCR serves as a proactive means to identifying gaps that might exist in an organization's security. Both the HIPAA Security Rule and the NIST Cybersecurity Framework provide guidelines for the purpose of assisting entities in the protection of their health data. On December 18th, 2015 President Obama enacted the Cybersecurity Information Sharing Act (CISA). This law promotes the sharing of cyber threat information between businesses and the federal government. [28] Both HITECH and CISA promoted the implementation of NIST security frameworks.

The FDA has issued guidance surrounding cybersecurity risks as it relates to medical device manufacturers; the International Organization for Standardization (ISO) enacted standard ISO 14971:2007, which deals with risk management of medical devices.[29] Even further than guidance, healthcare facilities should ultimately performing the following in order to secure their environments[30]:

- Evaluate and monitor network traffic to ensure that unauthorized access has not breached the network
- Implement and deploy antivirus software and enable and routinely check firewall configurations
- Segment networks which transmit sensitive data i.e. networked medical devices
- Perform periodic evaluations and penetration testing for gaps in security

Mobile technologies, and the increased acceptance of the use of personal devices via "Bring Your Own Device" (BYOD) initiatives, have also introduced a shift in how data is accessed, transmitted and stored. The National Cybersecurity Center of Excellence (NCCoE), part of NIST, issued in 2015 the NIST Cybersecurity Practice Guide SP 1800-1a. This guide focuses on how to secure electronic records on mobile devices and provides guidance on how to achieve security through various cybersecurity standards, architectural designs and technologies.[31] Mobile device management (MDM) software has been implemented by various healthcare organizations to better monitor, manage and secure mobile devices that connect to an organizations network to access internal resources and applications.

Mobile technologies, and the increased acceptance of the use of personal devices via BYOD initiatives, have also introduced a shift in how data is accessed, transmitted and stored

In addition to mobile technologies, the reliance on third-party solutions and cloud-based services, including the use of the Software as a Service (SaaS) model, has dramatically increased over the years and may pose a new area of risk to attacks and breaches.

[26] NIST, NIST Mission, Vision, Core Competencies, and Core Values (Internet) September 5th, 2016. Available from – https://www.nist.gov/about-nist/our-organization/mission-vision-values

[27] NIST, "Framework for Improving Critical Infrastructure Cybersecurity v1.0" *National Institute of Standards and Technology (NIST)*, Feb. 12th, 2014. Available from – https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[28] Norton Rose Fulbright, Data Protection Report (Internet) September 5th, 2016 – Available from – http://www.dataprotectionreport.com/2016/01/federal-cyber security-information-sharing-act-signed-into-law/

[29] ISO, ISO 14971:2007 (Internet) September 6th, 2016. Available from – http://www.iso.org/iso/catalogue_detail?csnumber=38193

[30] Deloitte Report Issue Brief, "Networked medical device cybersecurity and patient safety: Perspectives of healthcare information cybersecurity executives," *Deloitte*. Available from – http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf

[31] NCCoE, Security Electronic Health Records on Mobile Devices Executive Summary (Internet) September 6th, 2016. Available from – https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1a-draft.pdf

According to a Q2 2015 report issued by Skyhigh Networks, a cloud security software company, roughly 928 cloud-based services are on averaged used by a healthcare organization.[32] These cloud services range from collaboration tools to development environments, content sharing, business intelligence, etc. Skyhigh's report suggests that only 7% of the 928 services adhere to industry standards for compliance and security.[33] HIMSS offers a cloud computing toolkit that provides resources to healthcare organizations to better navigate through the cloud landscape; these resources range from guidance on risk management to educational materials.

The reliance on new technologies has forced security departments within healthcare organizations to re-evaluate their ecosystems to ensure their protection from cyber attacks.

Despite federally mandated regulations and national standards, healthcare organizations are still identifying gaps in their security plans. As cyber threats become an increasing reality, organizations are beginning to take a more proactive approach to safeguarding their data. Vice President of Cybersecurity and Special Missions at Raytheon Intelligence Jack Harrington stated that "cybersecurity is not a waiting game, and organizations without the expertise and tools required to identify and respond to skilled adversaries need to understand that…the old approach waited for technology to flag known threats."[34] In addition to Jack Harrington's comment, President of Raytheon Foreground Security, David Amalser stated, "too many organizations today rely on reactive models and automated tools that attempt to detect threats through signature-, rule- or sandbox-driven models."[35]

Adhering to the minimum standards, the Security Rule and Privacy Rule, will at best get an organization compliant with HIPAA, however, it may not equate to a secure environment; this in many ways is the minimum baseline to achieving compliance with federal regulations.

The reliance on new technologies has forced security departments within healthcare organizations to reevaluate their ecosystems to ensure their protection from cyber attacks. The combination of national and industry standards, cybersecurity frameworks, security software and allocated funding for cybersecurity training has helped mitigate threats by deterring attackers.

The combination of national and industry standards, cybersecurity frameworks, security software and allocated funding for cybersecurity training has helped mitigate threats by deterring attackers.

Conclusion:

President Obama this year has created the Cybersecurity National Action Plan (CNAP), with the goal of establishing a long-term strategy of enhancing cybersecurity protections and awareness, protecting and ensuring privacy and authorizing federal agencies to better protect their digital security.[36] This action plan serves as a reminder that cybersecurity and the protection of sensitive data is not limited to just the healthcare industry but to the whole of our digital engagement. This responsibility extends to not only security teams but to individual users of systems and devices, which provide access to sensitive health data; two examples can be seen through the physical security of laptops and mobile devices and safeguard passwords and changing company culture around security.

Both the federal government and private sector have issued tools to better facilitate and implement security frameworks, standardized secure exchange of data, provide easier access to educational materials surrounding cybersecurity and the issuance of

[32] Skyhigh Network, "Cloud Adoption & Risk in Healthcare Report" Q2 2015 published Q3 2015. Available from – http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Cloud-Adoption-Report-Q2-2015-Healthcare.pdf

[33] Ibid

[34] Raytheon, "Business wait for damaging cyber attacks before taking action: study," *Raytheon* (Internet) September 5th, 2016 – Available from – http://raytheon.mediaroom.com/2016-06-06-Businesses-wait-for-damaging-cyber-attacks-before-taking-action-Study

[35] Belliveau, Jacqueline "How a proactive approach improves healthcare cybersecurity," *Health IT Security*, June 6th, 2016. Available from – http://healthitsecurity.com/news/how-a-proactive-approach-improves-healthcare-cybersecurity

[36] General Services Administration (GSA), "Cybersecurity National Action Plan (CNAP) (Internet) September 6th, 2016. Available from – http://www.gsa.gov/portal/content/129694

security standards. However, greater steps towards developing mature standards and encouraging healthcare organizations to invest in their security programs are required to assist in the defense of the healthcare industry from both existing and future cyber attacks. Hopefully these tools will enable the healthcare industry in the U.S. to stay ahead of threats and continue to uphold a level of security and privacy that is required to keep our medical data safe and secure.

Acknowledgement:

I would like to thank Michael Czumak, CISO for his help on this article