Technology and Health Care 25 (2017) 1–10
DOI 10.3233/THC-161263
IOS Press

Invited Review Article

Cybersecurity in healthcare: A systematic review of modern threats and trends

Clemens Scott Kruse*, Benjamin Frederick, Taylor Jacobson and D. Kyle Monticone
Texas State University, San Marcos, TX, USA

Received /Accepted 19 August 2016

Abstract.
BACKGROUND: The adoption of healthcare technology is arduous, and it requires planning and implementation time. Healthcare organizations are vulnerable to modern trends and threats because it has not kept up with threats.
OBJECTIVE: The objective of this systematic review is to identify cybersecurity trends, including ransomware, and identify possible solutions by querying academic literature.
METHODS: The reviewers conducted three separate searches through the CINAHL and PubMed (MEDLINE) and the Nursing and Allied Health Source via ProQuest databases. Using key words with Boolean operators, database filters, and hand screening, we identified 31 articles that met the objective of the review.
RESULTS: The analysis of 31 articles showed the healthcare industry lags behind in security. Like other industries, healthcare should clearly define cybersecurity duties, establish clear procedures for upgrading software and handling a data breach, use VLANs and deauthentication and cloud-based computing, and to train their users not to open suspicious code.
CONCLUSIONS: The healthcare industry is a prime target for medical information theft as it lags behind other leading industries in securing vital data. It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentially of patient information from unauthorized access.

Keywords: Cyber attack, cybercrime, cybersecurity, cyber threats, health, healthcare, ransomware

1. Introduction

The Patient Protection and Affordable Care Act (ACA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) are shifting the landscape of healthcare technology. Legislation is encouraging healthcare providers to demonstrate “meaningful use” by becoming network-integrated in providing services [1]. As healthcare organizations transition to electronic-based systems, many are left vulnerable to cybercrime.

Cybercrime emerged in the late 1970s as the computer information technology (IT) industry took shape [2]. What began as spam eventually transitioned into viruses and malware. The technology is becoming more sophisticated and coordinated. The health industry is an attractive target for cybercriminals as health data contains sensitive personal and financial information.

*Corresponding author: Clemens Scott Kruse, 601 University Drive, College of Health Professions, rm 254, Texas State University, San Marcos, TX 78666, USA. Tel.: +1 512 245 4662; E-mail: s_k97@txstate.edu.

In order to circumvent the breach of healthcare data, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) implemented physical and technical safeguards to ensure sensitive information is protected from cybercriminals [3]. Physical safeguards include workstation use and security, device and media controls, and facility access controls. Technical safeguards include a unique user identification number, emergency access procedure, automatic logoff, encryption, and decryption [3]. However, cybercriminals are finding ways to breach these safeguards.

The adoption of healthcare technology is an arduous process that requires major planning and implementation time. After implementation, the software needs to be consistently updated to keep up with the recent advances and security holes that cybercriminals have exposed. Organizations are spending large amounts of funding to become more integrated, but are not spending enough time or money in keeping software updated [4]. An example of a recent threat – ransomware – crippled a California hospital [5].

Ransomware is the process of breaching networks and encrypting files to restrict access, and then ransoming the files for a fee [4]. Dr. Joseph Popp created ransomware in 1989 [6]. Popp used code to prey on organizations that held interest in introductory research on Acquired Immunodeficiency Syndrome (AIDS). Although authorities apprehended Popp, his creation resulted in many derivatives that serve as a framework for cybercriminals. Ransomware exposes and exploits the vulnerabilities of 21st century information technology (IT) infrastructure [6]. Hollywood Presbyterian Medical Center in Los Angeles, California had no choice but to pay a $17,000 payment to obtain a decryption key to regain access to their files, after it was held for ransom [5]. However, this does not account for 10 days of lost revenue while the hospital's systems were inaccessible nor does it account for a damaged reputation in patient data security [5].

In order to keep health information protected, healthcare providers must be aware of cybersecurity trends and threats as they emerge. Approximately 90 percent of healthcare providers were faced with data breaches in the last two years [5]. Cyber attacks are up 125 percent since 2010 and are the leading cause of health data security breaches [5]. As technology is constantly evolving, this systematic literature review is an update to "Cyber Threats to Health Information Systems: A Systematic Review" published in January, 2016 [7].

The purpose of this systematic review is to identify cybersecurity trends, including recent threats in regards to ransomware, and its relationship to the healthcare industry through academic literature.

2. Methods

2.1. Protocol and eligibility crtieria

The researchers derived the structure of this systematic review from the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Articles were eligible for this review if they were published in the last 10 years, if the full-text version of the manuscript is with PubMed (MEDLINE), CINAHL, or ProQuest, and if the publication is a peer-reviewed or scholarly journal.

2.2. Information sources

Three separate databases were queried to gather appropriate literature related to cybersecurity and recent trends. Databases chosen by the researchers included the Cumulative Index of Nursing and Allied Health Literature (CINAHL) and PubMed (MEDLINE complete) via the Ebson B Stephens Company (EBSCO Host), and the Nursing and Allied Health Source via ProQuest. The search string used in all three research databases was (Cybersecurity AND Healthcare) OR Ransomware. The literature search process is illustrated in Fig. 1.

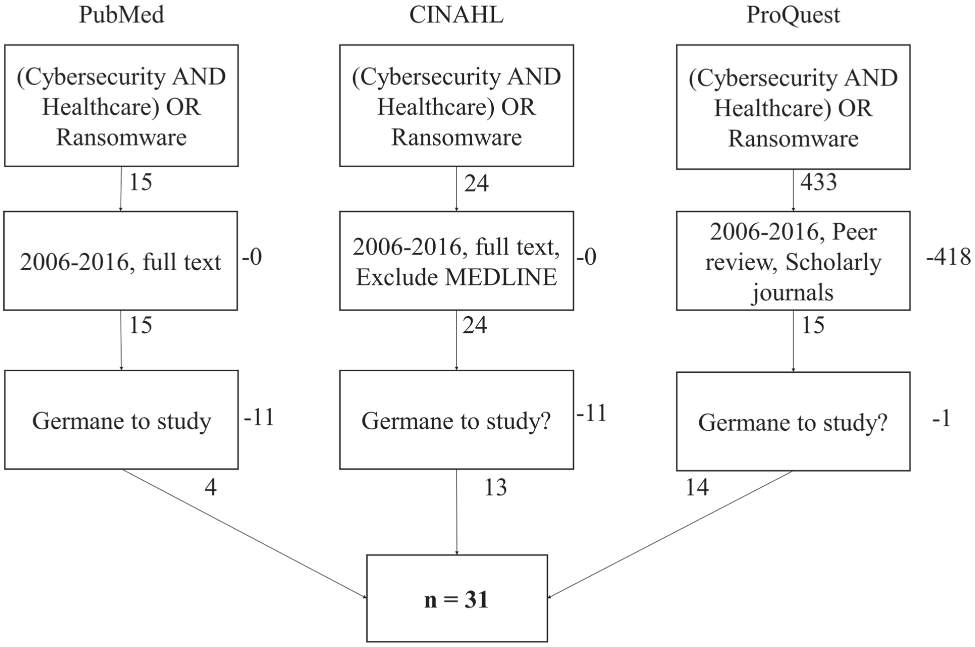
PubMed
CINAHL
ProQuest
(Cybersecurity AND Healthcare) OR Ransomware
(Cybersecurity AND Healthcare) OR Ransomware
(Cybersecurity AND Healthcare) OR Ransomware
15
24
433
2006-2016, full text
-0
2006-2016, full text, Exclude MEDLINE
-0
2006-2016, Peer review, Scholarly journals
-418
15
24
15
Germane to study
-11
Germane to study?
-11
Germane to study?
-1
4
13
14
n = 31

Fig. 1. Literature search process with inclusion and exclusion criteria.

2.3. Search

The review team experienced some initial difficulties with the search, but through the use of Boolean expressions, and some trial and error, the final search was successful. A common search string was used in all three research databases: (cybersecurity AND healthcare) OR ransomware. The searches in PubMed and CINAHL yielded very small results, even with filters, however the result from the search in ProQuest used filters to those with a better chance of meeting our objective. We used two of the three filters available: Peer reviewed and scholarly journals. All literature included in the study was independently read by at least three researchers and summarized. Before the researchers accepted the literature, it was evaluated to ensure it was relevant to the study. Literature was only rejected and excluded if at least two researchers agreed it was not relevant.

2.4. Study selection

A total of 472 articles were identified in the cybersecurity OR ransomware search. As ransomware is a relatively new topic, most of the literature was in the form of news articles, while cybersecurity articles were journals. The final sample size was 31.

2.5. Data collection process and synthesis of results

The reviewers used a series of consensus meetings to discuss their progress and observations. For instance, once the researchers had the results from the search after filters, they had 54 articles. The abstracts for these articles were divided among all group members in a way that each articles was reviewed by at least two reviewers. The team used a shared spreadsheet to record their recommendations on whether to keep the article in the analysis or reject it. When reviewers disagreed on recommendations, we went through a "why" session allowing each reviewer to present his case for why it should or should not be included. Consensus was reached when both agreed. The final group of articles was 31. The reviewers then divided these up between group members in a way that all articles were analyzed by at least two reviewers. The same shared spreadsheet was used to record observations. A consensus meeting was called when disagreement existed.

2.6. *Risk of bias*

Because of the relatively young age of ransomware in healthcare, very little has been studied in a randomized control trial. As a result, publication bias would restrict the availability of data for analysis.

3. Results

3.1. *Study selection and characteristics*

The initial search produced a total of 472 articles relating to the search topics "cybersecurity" OR "ransomware." After the researchers filtered the search criteria and perused the abstracts for information germane to the review's objectives, there were 31 articles that met the objective of the review. We selected English-only restriction and a date range limited to year 2006 to current, but the results were already limited in PubMed and CINAHL to the point that additional filters did not change the results. ProQuest used the similar filters as PubMed and CINAHL but required an additional filter of academic articles. We also selected the filter of peer reviewed, but that did not change the results. Each researcher examined every article to identify common themes. The researchers came to a consensus regarding major themes of the articles as well as their summaries. Table 1 provides a list of all the articles relevant to the study in the systematic review as well as a brief synopsis of their content.

3.2. *Results of individual studies*

The review team used the shared spreadsheet to record their observations, then the observations were reviewed collectively in another consensus meeting. The list of observations for each study in the sample is detailed in Table 1.

3.3. *Synthesis of results*

All of the articles analyzed are in agreement in acknowledging the growing threat of cyber attacks in healthcare and the systematic unpreparedness in dealing with cyber threats. There are two primary drivers that result in the increased exposure of healthcare organizations to cyber threats.

First, there is an ever-changing technological landscape. New technologies are implemented faster than security systems can be created or updated to protect them. Medical devices, which were traditionally stand-alone systems, are becoming network-integrated within hospital IT systems and are no longer immune to traditional cyber attacks [8]. As of recent, medical device manufacturers are implementing and expanding networked medical devices, while failing to maintain a pace to circumvent the possible cybersecurity threats posed by network integration [9,27]. Many IT experts are concerned that recent trends will convince cybercriminals to target medical devices such as pacemakers or Intensive Care Unit (ICU) respirators [33].

Table 1
Summary of observations

Author(s)	Synopsis
AHC Media (Apr) [5]	Introduces the high profile cyber attack on Hollywood Presbyterian Medical Center as well as the true costs ransomware imposes on providers.
AHC Media (May) [8]	Details four previous healthcare related ransomware attacks and how healthcare IT systems are not keeping up with the current cyber threats.
Wu et al. [9]	Introduces the topic of new wireless applications of medical devices left vulnerable to cyber attacks and how safety risk management in manufacturing is being redefined to address growing cybersecurity threats.
HCPro.com [10]	Explains how new strands of ransomware target backup files will render some hospital security measures inert and how some healthcare providers will be negatively impacted by declining consumer satisfaction with cybersecurity.
Conn (July) [11]	Discusses a taskforce of healthcare professionals assembled by Health and Human Services (HHS) to identify best practices in cybersecurity and how these best practices can lend themselves to the healthcare industry. The authors also mentions how the taskforce is hesitant to release some of their findings as it may detail vulnerabilities within the industry and insight further cyber attacks.
Rowe [12]	The article covers how the ACA and the HITECH Act's meaningful use are shifting providers towards greater network integration without having adequate cybersecurity to accompany the increased technological integration of healthcare services.
Blanke & McGrady [13]	Discusses the emerging threat of cyber attacks and how they could affect HIPAA and the HITECH act. The article provides a useful checklist tool to assess and monitor common risks.
Hagland [14]	Provides information on why the healthcare industry is being targeted in cyber attacks and why providers are unprepared to deal with these attacks.
American Health Information Management Association [15]	Introduces statistics on ransomware attacks.
Streger [16]	Details the cyber threats facing healthcare providers and four main points for protection.
American Association of Critical-Care Nurses [17]	Describes how successful cyber attacks in healthcare primarily stem from employees or human error.
Van Alstin [18]	Reports that cybercrime is going to increase as cybercriminals become more sophisticated.
Post [19]	Discusses how hospitals try to cope under a cyber attack and mentions that 3 percent of hospitals pay a ransom and do not disclose that fact to the broader public.
Goedert [20]	Outlines the reasons why ransomware ransoms are relatively inexpensive and stresses the importance of having well-trained staff on cybersecurity threats.
Conn [31]	Covers an attack on a hospital in Indiana that infected an entire hospitals' network and how many medical devices are at-risk of being compromised as well.
Hospitals become major target for ransomware [22]	Describes how stolen administrative credentials can be used to infect IT servers and stresses the importance of having backups of data as ransomware evolves.
Tuttle [23]	Analyzes the three criteria hackers consider when selecting a healthcare target as well as the value of cyber insurance policies.
Valach [24]	The article gives tips for organizations who are victims of a ransomware attack.
Koppel et al. [25]	Discusses cybersecurity issues and why some overly burdensome cybersecurity rules and regulations are prompting physicians to work around cyber safety measures to complete their work.

Table 1, continued

Author(s)	Synopsis
Page et al. [26]	Analyzes cybersecurity within Telehealth technologies and how end-to-end encryption methods could make cloud storage and access of Protected Health Information (PHI) compatible with HIPAA requirements.
Rios [27]	Great oversight of medical devices in cybersecurity as medical devices become increasingly networked and wireless. There is the possibility of knowing the motivations for attacks and what attackers will be targeting.
McNeil [28]	Details cybersecurity threats and how 26 billion devices will be integrated into the "internet of things" as well as how medical devices need to be prepared for this shift in terms of their cybersecurity.
Welch [29]	Article discusses the dangers of cybersecurity and details five essential areas of importance for providers. Essential areas include preparation, prevention, long-term strategies, and resources.
McDermott [30]	Analyzes the three prominent types of ransomware and what IT personnel are doing to prevent attacks.
McGuire [31]	Introduces the threat of increasing network integration of medical devices and provides ransomware statistics.
Coronado et al. [32]	Explores the idea of cybersecurity of medical devices and how increased integration of medical devices into healthcare IT systems leaves new networked medical devices exposed to cyber threats in ways they have not been in the past. The author goes on to provide steps hospitals can take to prevent attacks.
Loughlin et al. [33]	Provides information on a group of executives who voice their concerns with growing cyber threats and how acute care operations can be disrupted by unsecured off-the-shelf software products that are left vulnerable to cyber attacks.
Bangs [34]	The article talks about basic methods (six ways) of protecting your organization against ransomware attacks.
Fu & Blum [35]	Reports on what medical devices must do to stand up to cyber attacks and how there is no reporting system that tracks patient death or injury as a result of cybersecurity breaches.
Luo & Liao [36]	Details the importance of university curriculum to include courses that focus on protecting data and IT systems.
Mueller [36]	The article goes into great lengths to detail ways to prevent "webjacking" and ransomware. Ways to tackle on the problem include: a change of mindset, perimeter monitoring, remote investigation, and remote remediation.

Second, the United States (U.S.) government has shifted its policy in promoting the increased use of technology in healthcare institutions [12]. Specific federal initiatives such as "meaningful use" in the HITECH act and the expansion of electronic healthcare information exchanges in the ACA are pushing for healthcare entities to become increasingly network reliant [12,13]. Organizations hoping to comply with federal initiatives are spending around 95 percent of their IT budgets on implementation and adoption, while less than 5 percent of their IT budgets are spent on security [5].

Technological advancements and federal policy initiatives have dramatically expanded the healthcare industry's exposure to cyber attacks. Healthcare is one of the leading industries targeted by cybercriminal organizations [14]. While the exposure and frequency of cyber attacks has changed, the motive and target of the cybercriminals has not. Research suggests that an individual's medical information is 20 to 50 times more valuable to cybercriminals than personal financial information [5,12]. Access to medical information enables cybercriminals to commit identity theft, medical fraud, extortion, and the ability to illegally obtain controlled substances. The utility and versatility of medical information, extensive centralized storage of medical information, relatively weak IT security systems, and the expanding use of healthcare IT infrastructure all contribute to an increase in cyber attacks on healthcare entities [5,15,35].

In fact, cyber attacks which target medical information is increasing 22 percent a year with 112 million compromised records in 2015 alone. An attack costs organizations around 3.7 million dollars to clean up [15].

3.4. Additional analysis

Despite enduring efforts by healthcare organizations and the government to protect sensitive health information, new forms of cyber attacks continue to make a lasting impact. Hospitals have recently been targeted by a type of cyber attack known as “ransomware.” The first major case took place at Hollywood Presbyterian Medical Center in Los Angeles, California [17]. There has also been growing concern for the security of medical devices which have demonstrated security flaws and make them vulnerable to cyber attacks [32]. Cyber attacks can be a costly annoyance but healthcare entities cannot afford to have their operations disrupted. As healthcare entities increase reliance on IT infrastructure for their operations, patient care is more exposed to cybercriminals [25]. When these critical information systems are held hostage by cyber attackers, it creates a sense of urgency for healthcare entities. Lack of access to healthcare data can be detrimental to operations and patient safety [20].

4. Discussion

4.1. Summary of evidence

The U.S. government has recognized the growing problem of cyber attacks in new security requirements to HIPAA and the HITECH act, which require healthcare entities to strengthen their cybersecurity practices [13]. HIPAA’s security rule that requires covered entities to safeguard PHI has been updated by the HITECH act to ensure healthcare entities have updated policies to prepare and protect against data breaches [13]. One way healthcare entities are preparing for data breaches is by employing new techniques to fight cyber threats at their facilities. These techniques include: having clearly defined cybersecurity duties for employees, having properly defined software upgrade procedures, using a virtual local area network (VLAN), using deauthentication, having a data breach plan in place, using cloud based computing, and training employees to be more conscientious of cybersecurity [20,36]. The most stressed security technique in the literature is proper employee training. Most security breaches are caused by employees accessing malicious files and most HIT security systems will not stop those kinds of breaches [20,25,26].

4.2. Limitations

There were several limitations the researchers encountered in their study. First, as ransomware is a relatively new topic, there were few academic articles pertinent to the subject. This resulted in limited search results. Second, cybersecurity is a broad topic. In its relation to healthcare, it was difficult to identify all of the external and internal threats and trends. Last, the study focused geographically on the American healthcare system. Only English articles and articles relevant to the U.S. health system were included in the study.

4.3. Conclusions

The two primary drivers exposing healthcare to cyber threats include rapid technological advancement and evolving federal policy. As healthcare IT infrastructure struggles with new technology and security protocols, the industry is a prime target for medical information theft. While security companies and the government have made progress to slow the prevalence of cyber attacks, the healthcare industry is lagging behind other leading industries in securing vital data. Healthcare must continuously adapt to the ever-changing cybersecurity trends and threats such as ransomware, where critical infrastructure is exploited and valuable patient data is extracted. It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentially of patient information from unauthorized access.

Acknowledgements

The authors' responsibilities were as follows: BCF, TJ, and DKM conducted the research, analyzed the data, wrote and edited the manuscript, and read all of the articles. CSK directed the research, helped design the review, helped analyze the articles, provided final edits and rewrites, and serves as the corresponding author.

Conflict of interest

There are no conflicts of interest.

Operational definitions

Meaningful use: A program by the Centers for Medicare & Medicaid Services that provides incentives to healthcare entities for the use of certified electronic health record (EHR) technology to: improve quality, safety, efficiency, and reduce health disparities [38].

Funding

There was no funding for this research.

References

[1] Centers for Medicare & Medicaid Services [Internet]. Electronic health records (EHR) incentive programs Baltimore, MD: CMS; 2016. URL:https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms. Accessed: 2016-08-09. (Archived by WebCite® at http://www.webcitation.org/6je8QNlo0).

[2] CW Jobs [Internet]. London, UK: 2016. Cyber crime timeline; URL:http://www.cwjobs.co.uk/careers-advice/it-glossary/cyber-crime-timeline. Accessed: 2016-08-09. (Archived by WebCite® at http://www.webcitation.org/6je8V9cyI).

[3] U.S. Department of Health and Human Services. Security standards: technical safeguards [Internet]. Baltimore, MD: CMS; URL:http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf. Accessed: 2016-08-09. (Archived by WebCite® at http://www.webcitation.org/6je8cfMpZ).

[4] U.S. Department of Health and Human Services. Fact sheet: ransomware and HIPAA [Internet]. Baltimore, MD: CMS; URL:http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. Accessed: 2016-08-09. (Archived by Web Cite® at http://www.webcitation.org/6je8iBYI5).

[5] AHC Media LLC. Hackers target hospitals with "ransomware". ED LEGAL LETT. 2016 Apr; 27(4): 1-4.

[6] Jayanthi A. First known ransomware attack in 1989 also targeted healthcare. http://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html.

[7] Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. Technol Health Care. 2016 Jan 27;24(1): 1-9. Available from: 10.3233/THC-151102.

[8] AHC Media LLC. Ransomware attacks are on the rise, and hackers are getting better. ED LEGAL LETT. 2016 May; 1(4): 1-4.

[9] Wu F, Eagles S. Cybersecurity for medical device manufacturers: Ensuring safety and functionality. Biomed Instrum Technol. 2016 Jan 20; 50(1): 23-33. Available from: 10.2345/0899-8205-50.1.23.

[10] HCPro.com Ransomware a new threat to healthcare sector. Physician Practice Perspective. May 2016; 11-12.

[11] Conn J. Federal task force takes on healthcare cybersecurity. Modern Healthcare. URL:http://www.modernhealthcare.com/article/20160416/MAGAZINE/304169890. Accessed: 2016-08-09. (Archived by WebCite® at http://www.webcitation.org/6jdtejLCt) April 16, 2016.

[12] Rowe K. Healthcare IT transformation: how has ransomware shifted the landscape of healthcare data security? Healthc Inform. 2016 May; 33(3): 44-45.

[13] Blanke SJ, McGrady E. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: a cybersecurity risk assessment checklist. J Healthc Risk Manag. 2016 Jul; 36(1): 14-24. Available from: 10.1002/jhrm.21230.

[14] Hagland M. With the ransomware crisis, the landscape of data security shifts in healthcare. Healthc Inform. 2016 May; 33(3): 41-47.

[15] American Health Information Management Association. Healthcare increasingly targeted by ransomware attacks. J AHIMA. 2016 May; 87(5): 12.

[16] Streger M. Ransomware: a ticking bomb for public safety. News Network. July 2016: 12.

[17] American Association of Critical-Care Nurses. Ransomware poses major threat to hospitals. AACN BOLD VOICES. 2016 Jun; 8(6): 14.

[18] Van Alstin CM. Ransomware: It's as scary as it sounds. But with security best practices, you can fight back. Health Manag Technol 2016 6;37(4): 26-27.

[19] Post W. LA Hospital Pays Hackers After Ransomware Attack OpenNotes Expands, Shares Lessons. 2016.

[20] Goedert J. Security: the ransomware nightmare. HEALTH DATA MANAGE. 2016 Apr; 24(3): 10.

[21] Conn J. Ransomware scare: Will hospitals pay for protection? Modern Healthcare. 2016 Apr 11; 46(15): 8.

[22] Hospitals become major target for ransomware. Network Security 2016 4; 2016 (4): 1-2.

[23] Tuttle H. Ransomware Attacks Pose Growing Threat. Risk Management. 2016 May 1; 63(4): 4.

[24] Valach AP. What to Do After a Ransomware Attack. Risk Management. 2016 Jun 1; 63(5): 12.

[25] Koppel R, Smith S, Blythe J, Kothari V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? Stud Health Technol Inform. 2015; 208: 215-220. Available from: 10.3233/978-1-61499-488-6-215.

[26] Page A, Kocabas O, Soyata T, Aktas M, Couderc JP. Cloud-based privacy-preserving remot ECG monitoring and surveillance. Annals ofNnoninvasive Electrocardiology. 2015 Jul 1; 20(4): 328-37.

[27] Rios B. Cybersecurity expert: medical devices have 'a long way to go'. Biomed Instrum Technol. 2015 May 20; 49(3): 197-200. Available from: 10.2345/0899-8205-49.3.197.

[28] McNeil M. 2015 will require implementation of thorough security programs. Wired Magazine, 1-28-2015. Found on 8-9-2016 at https://www.mdtmag.com/blog/2015/01/2015-will-require-implementatin-thorough-security-programs.

[29] Welch SS. Five things providers need to know about cybersecurity. Journal of the Medical Association of Georgia. 2015; 104(1): 40-2.

[30] McDermott IE. Ransomeware: Tales from the cryptolocker. Internet Express. Jun 2015: 35-37.

[31] McGuire CF. TIM Lecture Series-The Expanding Cybersecurity Threat. Technology Innovation Management Review. 2015 Mar 1; 5(3): 56.

[32] Coronado AJ, Wong TL. Healthcare cybersecurity risk management: keys to an effective plan. Biomed Instrum Technol. 2014;(Suppl): 26-30. Available from: 10.2345/0899-8205-48.s1.26.

[33] Loughlin S, Fu K, Gee T, Gieras I, Hoyme K, Rajagopalan SR, et al. A roundtable discussion: safeguarding information and resources against emerging cybersecurity threats. Biomed Instrum Technol. 2014; 8-17. Available from: 10.2345/0899-8205-48.s1.8.

[34] Bangs G. New Ransomware and Cyber extortion Schemes Hold Businesses Hostage. Risk Management. 2014 Oct 1; 61(8): 30.

[35] Fu K, Blum J. Controlling for cybersecurity risks of medical device software. Commun ACM. 2013 Oct; 56(10): 35-37. Available from: 10.1145/2508701.

[36] Luo X, Liao Q. Awareness education as the key to ransomware prevention. Information Systems Security. 2007 Jul; 16(4): 195-202. Available from: 10.1080/10658980701576412.

[37] Mueller L. Webjacking, and how to boot it out. Network Security. 2006 Aug 31; (8): 15-8.

[38] Health Resources and Services Administration. Baltimore, MD: HHS; 2016. What is "meaningful use"?; URL:http://www.hrsa.gov/healthit/meaningfuluse/MU%20Stage1%20CQM/whatis.html. Accessed: 201 6-08-09. (Archived by Web Cite® at http://www.webcitation.org/6je785Ed5)