International Journal of Engineering & Technology, *7 (4.36) (2018) 338-349*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

End-Point Information Security in the Healthcare Industry: A Critical Review

Arif Uzzaman

MS in Cyber Security, MBA, Webster University
**Corresponding author E-mail:au.uzzaman@gmail.com*

Abstract

The ability of the healthcare industry to keep abreast with the evolving trends in endpoint information security depends on combinations of measures. In the current literature, some of these measures include the development of analytics capable of spotting intruders on time, embracing quick reactions to potential or detected intrusions, and the decision to employ robust system defenses. In this paper, the main aim was to review the current literature regarding the subject of endpoint information security, with critical insights gained from the case of the healthcare industry. Findings suggest that the healthcare industry forms one of the most attractive arenas for security attackers. Some of the healthcare organizations that have been victims of recent security attacks include the Californian Hollywood Presbyterian Medical Center that experienced a data breach in February 2016 and MedStar Health Inc. (in the same month). In the following month, San Diego’s Alvaro Hospital Medical Center was also targeted for cyber attack. Hence, some algorithms have been proposed to counter these attacks; including the use of SOA-based EHRs, the implementation of the RBAC model, the use of *k*-anonymity, *k*-unlinkability, and the SQL searching mechanisms that target the patients’ encrypted data. Also, some strategies have been proposed as best practices in endpoint information security. These strategies include the management of identity lifecycles, the establishment of risk-aware cultures, the management of third-party security compliance, and securing healthcare firms’ devices in terms of design. Overall, it is evident that the complexity of endpoint information security in the healthcare industry (due to the evolution of applications such as virtualization and cloud computing) implies that the ability to survive from future security attacks will depend on the firms’ ability to keep abreast with industry demands.

Keyword: *End-Point, Information Security, Healthcare Industry*

1.Introduction

Given the increasing use of web-based services and the emergence of e-Health in the healthcare industry, success in service provision is likely to be determined by the effectiveness with which health-related information is obtained and managed by patients securely [1]. Endpoint security entails methodologies seeking to protect corporate networks, especially those that are accessed through remote devices. Examples of these devices include mobile devices, laptops, and other wireless devices [1, 2]. Therefore, it can be inferred that endpoint security refers to a technique aimed at protecting computer networks, especially those that have been remotely linked to the client devices. It is also evident that the linkage of corporate networks to the mobile phones, tablets, laptops, and related wireless devices tends to create attack paths that pose security threats [2]. In the current healthcare industry, the cost of endpoint security attacks stretches to about $1.3 billion in each year [2, 3]. In 2017, the average healthcare organization lost about five million dollars and the losses were attributed to endpoint attacks. Other studies have documented some of the common costs incurred by healthcare industry players relative to the aspect of endpoint security. The common costs include regulatory actions, fines, and lawsuits. These costs account for about four percent of the loss, reputation damage associated with about eight percent of the loss, and damage to infrastructure, which accounts for about 10 percent of the losses. Other costs include theft of information assets (23 percent), system downtime (25 percent), and end user and IT productivity loss; with the latter accounting for 30 percent of the costs incurred [2-4, 6]. The figure below provides a summary of these healthcare costs associated with endpoint attacks.

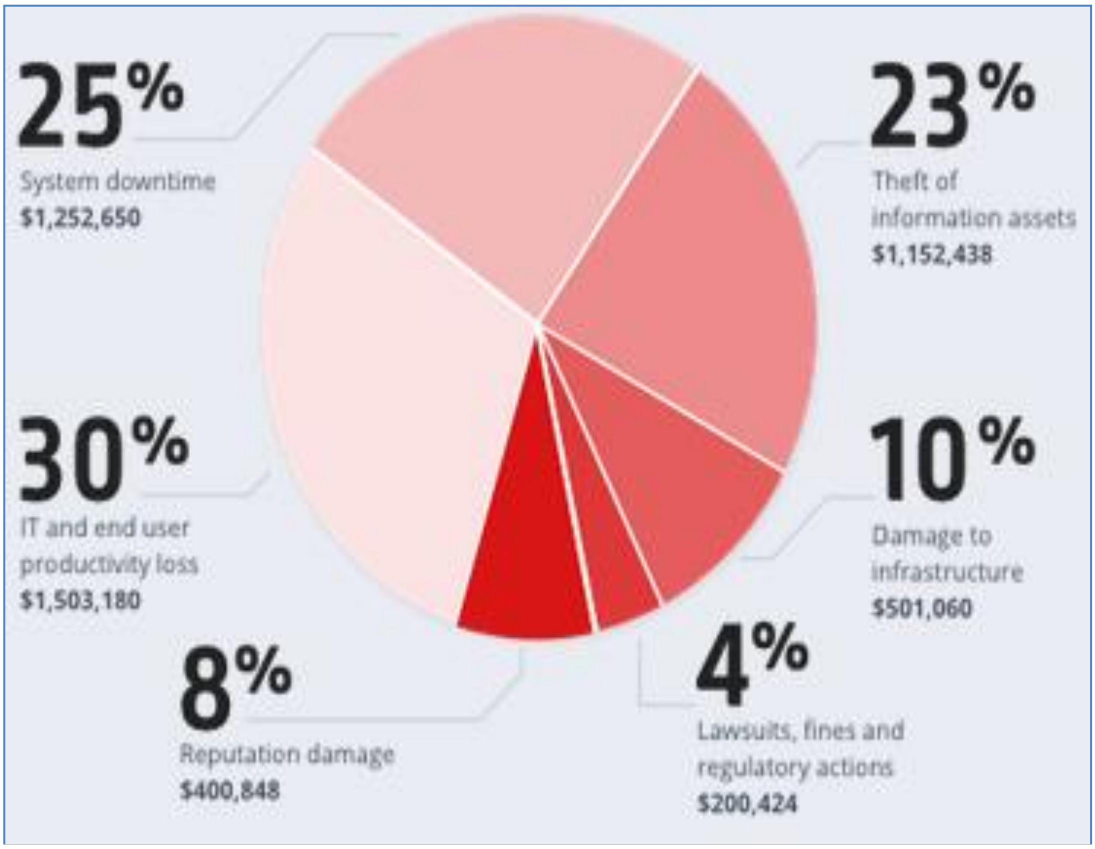

Figure 1: Costs incurred due to endpoint attacks in 2017

With the information obtained from security and IT leaders, the figure above suggests that today's healthcare industry continues to struggle to secure the endpoints. Additionally, the trends above indicate that most of the healthcare firms incur steep costs for the various attacks; with the situation compounded when the attacks target large organizations. This paper focuses on some of the previous scholarly studies that have investigated the subject of endpoint security to provide a critical review, with particular emphasis on the healthcare industry.

2.State of Research in Information Security in the Healthcare Sector

In most of the previous studies, the common research methodologies that have been employed relative to the subject of endpoint information security in the healthcare sector include quantitative research, qualitative research, and design research. Indeed, the focus on design research has been to establish artifacts that include frameworks, prototypes, algorithms, and models responsible for solving information system challenges in the industry [4]. On the other hand, qualitative research seeking to give an insight into the selected subject has seen scholars examine endpoint information security via instruments such as the researchers' observations and impressions, participant observation, the use of documents, and the decision to conduct interviews. Some of the quantitative approaches that the previous scholarly studies have embraced include statistical modeling, econometric analysis, and survey-based research [5, 6]. Therefore, this sub-section reviews some of these scholarly contributions, with the critical review poised to pave the way for the prediction of future trends in endpoint information security.

2.1 Privacy Concerns in Relation To Endpoint Information Security

Special classes of patients have been the target population from whom most of the past research has strived to examine perceptions of privacy. Some of these classes of patients include adolescents, seekers of HIV testing, and mental health patients [7]. For the surveys that have examined the subject of healthcare confidentiality in relation to endpoint information security, four major conclusions have been made. Firstly, most of the patients examined concur that the information provided only needs to be shared with individuals charged with their care. For patients who are keen to have their health information shared among physicians, the current literature contends that seekers of HIV testing are unlikely to approve that their health information is shared. Thirdly, the studies indicate that the majority of patients who are willing to have their information shared among physicians are less likely to release the same data to third parties such as family members and employers. Lastly, the scholarly affirmations hold that most of the patients who undergo genetic testing prefer an option that restricts the responsibility of sharing health information to at-risk members of the family to the patients themselves [7-9]. Based on these results, mixed observations arise regarding the patients' privacy concerns. The relative perception of security and privacy concerns among patients has also been documented to increase with increasing levels of technology [10]. The implication is that as technology in the healthcare industry advances, information security and privacy concerns among patients increase 7-10].

2.2 Proposed Algorithms That Promise Information Access Control

Large networked systems characterize most of the modern healthcare systems [11]. The role of these systems concerns the management of patient data. However, the health data continues to be accessed by multitudes of users; with the access arising from various contextual purposes that the users hold of the data [12, 13]. To assure information access control, one of the algorithms that have been proposed entails Role Based Access Control (RBAC). Reported as an effective tool through which the patients' data access could be managed, RBAC has gained increasing adoption in the healthcare industry. The main reason for this increasing use of the tool is that it can manage and implement a wide range of control policies, proving responsive to the healthcare industry's growing complex role hierarchies [14]. Overall, the model promises improvements in transparency regarding access control management among healthcare systems. The figure below illustrates the functionality of the proposed RBAC algorithm as a tool seeking to support information access control in the healthcare industry.

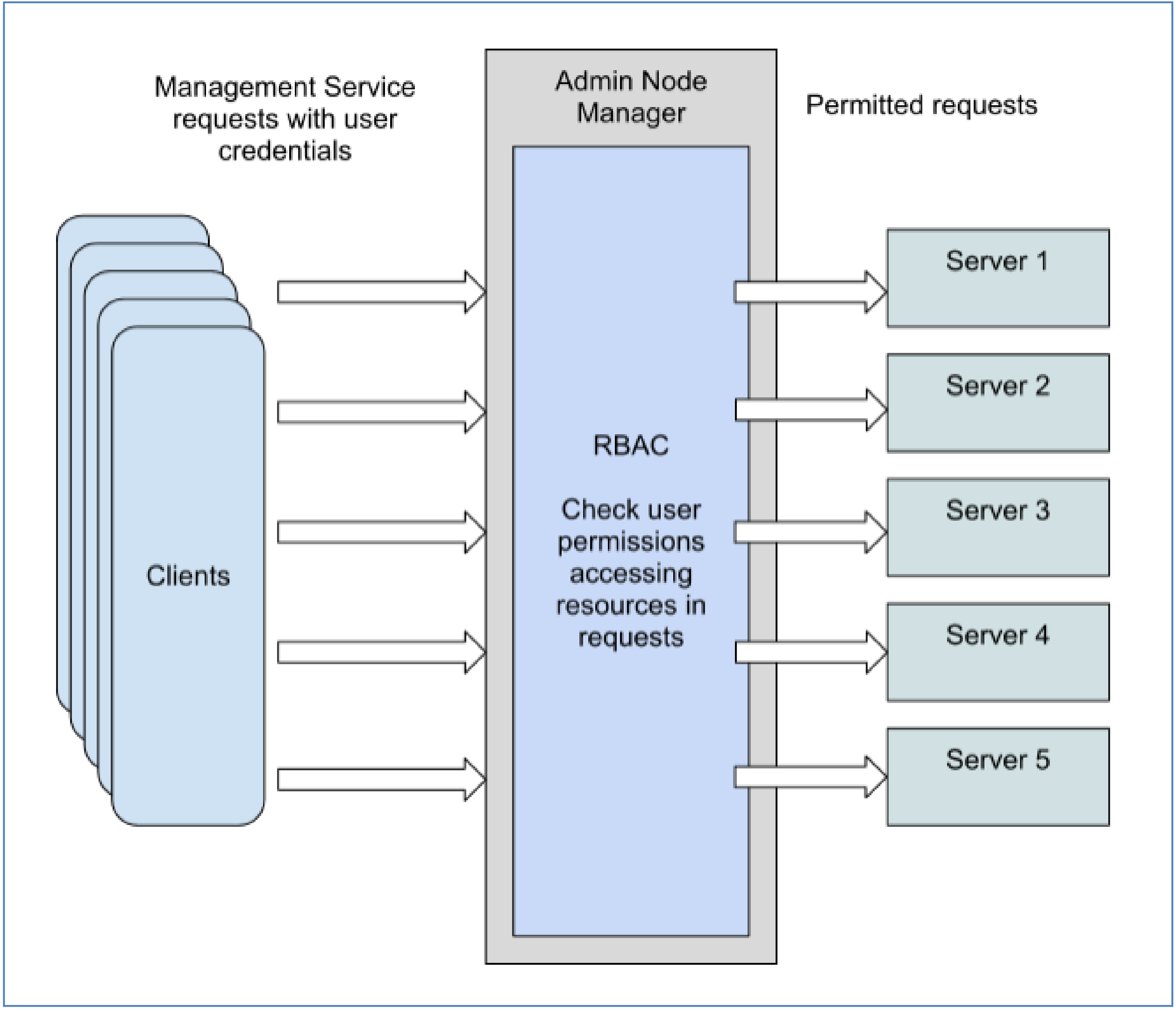
Management Service requests with user credentials
Admin Node Manager
Permitted requests
Clients
RBAC
Check user permissions accessing resources in requests
Server 1
Server 2
Server 3
Server 4
Server 5

Figure 2: The Role Based Access Control model

2.3 Information Security and Data Interoperability in the Healthcare Industry

For some of the provider organizations that have employed healthcare information systems, some of the previous scholarly investigations contend that various proprietary formats have been used to store the health data [15]. Given that the resultant health data formats are diverse, the challenge that emerges concerns the manner in which the patient data could be shared, especially from one provider firm to another [15-17]. The complexity is compounded by situations requiring the patient data to be shared with health policy and medical research specialists [16, 17]. To save the healthcare industry's increasing costs associated with endpoint security attacks, investments in the electronic health records (EHR) interoperability have been proposed [15, 16]. Despite the promising nature of the EHR technique and its perceived contribution to the healthcare industry's endpoint information security, the manner in which fully functional interoperable EHR could be established remains challenging [17]. The technicality has led to the evolution of research studies proposing EHR-specific prototype service-oriented architectures (SOAs) in different settings. The target settings into which the SOA model for EHR has promised to play a contributory role towards endpoint information security include health clinic settings, collaborative medical (mammogram) image analyses, and clinical decision support contexts [18].

The scalability of SOA-based EHRs has also been observed to promote global and national health information networks among inter-enterprise environments. A specific example of a setting in which the model has been observed to gain application is the case of regional health information organizations, as well as their associated alliances [16]. The proposed SOA-based EHRs as algorithms capable of assuring endpoint information security are seen as advanced tools aimed at strengthening privacies assured by the RBAC system. This ability of the SOA-based EHRs is evidenced by the capability of incorporating device ownership and location constraints [19]. The figure below illustrates the manner in which the proposed algorithm could be incorporated into the healthcare architecture, relative to its contribution to the healthcare industry's endpoint information security. Also, the proposed tool is poised to strengthen the privacy achieved by RBAC.

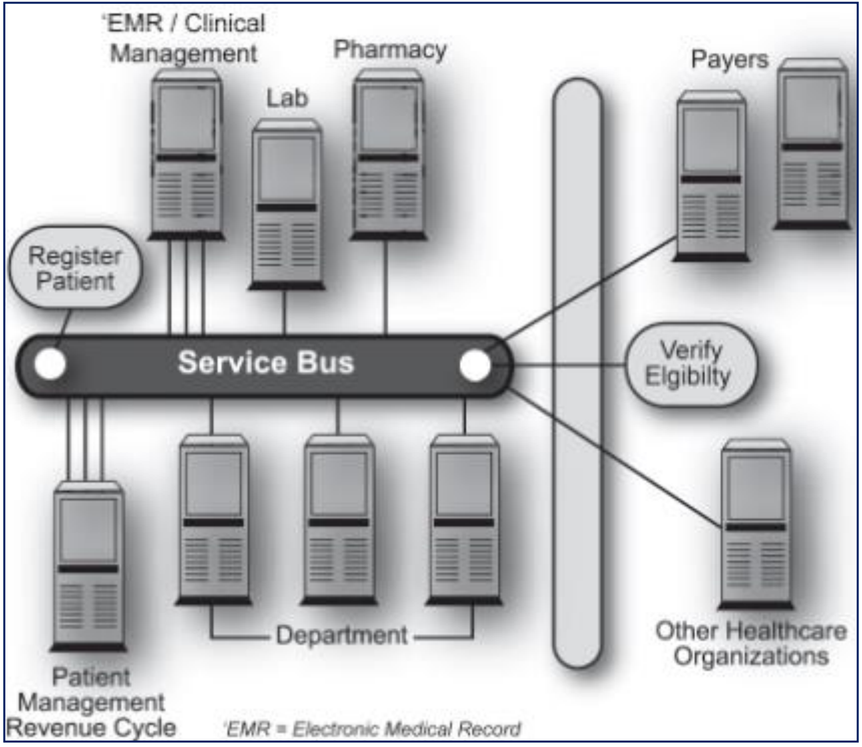
'EMR / Clinical Management
Pharmacy
Lab
Payers
Register Patient
Service Bus
Verify Elgibilty
Department
Other Healthcare Organizations
Patient Management Revenue Cycle
'EMR = Electronic Medical Record

Figure 3: The proposed SOA-based EHR and its integration in healthcare operations

3.Current Trends in Endpoint Security Attacks

As recently as 2017, several cyber-attacks have been reported in the healthcare industry, putting endpoint information security at stake. One of the broad categories reported has been ransomware, a top security trend observed to affect about 78 percent of healthcare service providers [20]. Specific and major events that have been documented include *NotPetya* and *WannaCry*. Major breaches have also been reported in the healthcare industry. Given the continuing struggle by the industry to keep abreast with information security and IT − relative to other industries, criminals have exploited this gap [20]. Particularly, the first half of 2017 witnessed at least 791 reports of breaches in which criminals accessed about 12 million records, with the healthcare industry unexceptional.

3.1 A Shift from Reliance on End-User Mistakes

Other scholarly investigations hold that currently, most of the hackers are unlikely to rely on the mistakes that end-users commit. In IT security, the end-users' mistakes have been observed to be the weakest links for a significant period [21]. As such, the end-users have historically emerged as the main targets of malware. The current literature contends that the majority of healthcare industry players have embraced malware campaigns with the aim of sensitizing the end-users regarding some of the tricks that criminals or cyber attackers employ to trick the end-users into visiting compromised websites or downloading malicious email attachments [21, 22]. The implication is that the majorities of the organizations in the healthcare industry are aware of the vulnerability and continue to employ security awareness training, as well as investing in email security [22]. Whereas these steps are promising, some studies caution that recent infection trends point to an evolution of attacks in such a way that the criminals are keen to avoid the issue of user interaction [24]. Specific examples of this trend in which the attackers are avoiding end-user interaction include the cases of Hancock Health and Allscripts. In these situations, the cyber attackers employed a direct method whereby they relied on vulnerable servers to access the firms. From these affirmations, it can be inferred that the future of endpoint information security in the healthcare industry will witness the attackers target unsecured ports and vulnerable servers. The implication for the industry's and organizations' IT professionals is that the need to prioritize the identification and to secure open ports cannot be overemphasized.

3.2 Reliance on Organizational Administration Tools against the Healthcare Industry Players

In the recent past, it has also been observed that cyber attacks in the healthcare industry have targeted legitimate system processes and tools. The motivation of these attacks has been to exploit networks and spread infections while evading detection [23, 24]. Given that the approach requires the use of the existing system programs without incorporating traditional malware, it has proved difficult for traditional antivirus solutions to detect the same. Similar to the trend discussed above, NotPetya forms a notable and high-profile case in which the administration tools of the organization were used against it. Initially, the users triggered the infection via the installation of updates. The updates involved a Ukrainian accounting software, spreading via Windows Management Instrumentation (WMI) and PSExec. Given that most of the system administrations employ these tools widely without experiencing security warnings, the lateral spread of the attack was rapid and operated at the detriment of the victim networks. The implication for IT professionals in the health industry is that any administration tools that are not in use are worth disabling. Even for those in use, the ability to survive such cyber attacks is seen to depend on the extent to which access is restricted.

3.3 Evolution of Automatically-Propagating Attacks

An additional trend in cyber attacks targeting the endpoint information systems of the healthcare industry concerns the resurgence of attacks that have leveraged worm components in such a way that the latter could be successful in the transformation of a single infection into crippling events that target the entire network [25]. An example of this trend is the case of the WannaCry ransomware outbreak. Targeting over 50 countries, the attack spread to about 400,000 computers and the healthcare industry was adversely affected. The resultant lesson from this scholarly observation is that in the healthcare industry, attacks are no longer perceived in terms of a certain employee targeting one machine. Instead, a single infected machine could emerge as a catalyst and transform into a large outbreak capable of taking down external and internal networks [24, 25]. A summary of these trends in the recent security attacks targeting the healthcare industry is highlighted in the figures below.

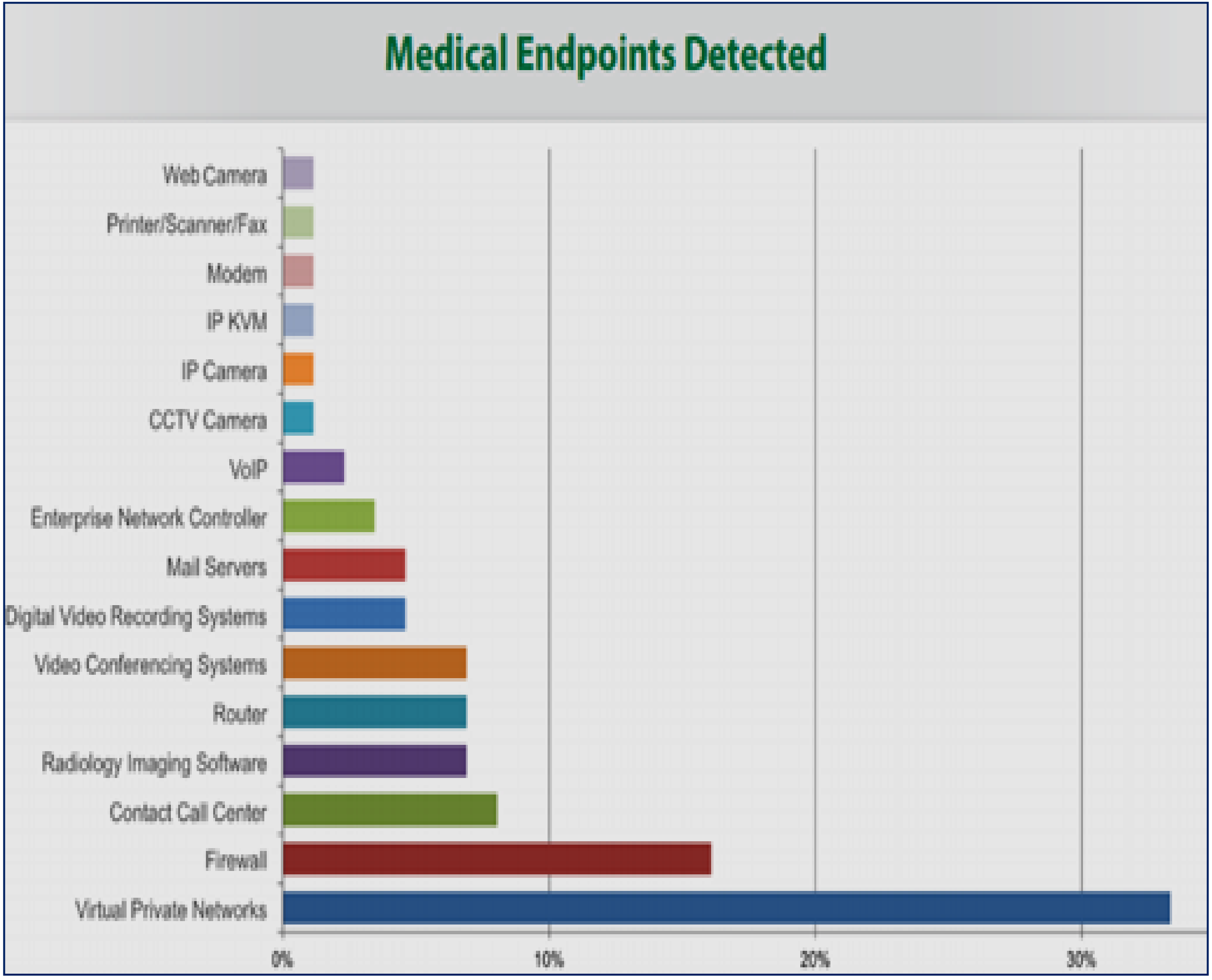

Figure 4: Security attacks in various medical endpoints

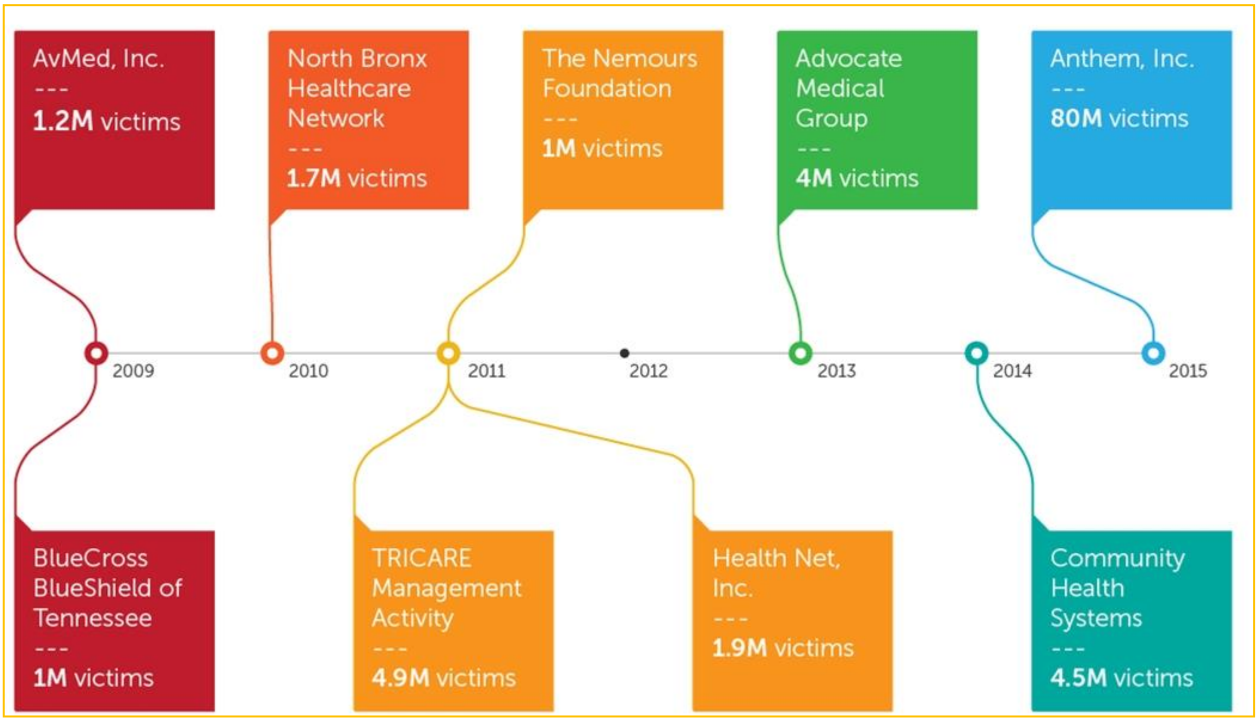

Figure 5: Recent healthcare breaches

4.Endpoint Information Security for Authorized Disclosures in the Healthcare Industry

Cross the organizational boundaries of the healthcare industry, sharing data is required due to the need to support the multiple stakeholders' interests. Despite the crucial role of the data sharing process, the decision to release patient data implies that some of the identifying information associated with the patients is likely to be exposed. Also, sensitive information could be released and, in turn, cause socio-economic repercussions while violating the patients' privacy [26]. However, some data is masked for sensitive and identifying information and the need for its release is informed by a reason such as epidemiological research [24-26]. Technological advancements have also paved the way for health record consolidation from various sources and transforming the information into one research database. The role of such databases has been to support researchers concerned with health services, clinical methods, and public health [27]. The risk surrounding the possible release of sensitive and identifying information associated with patients has led to some investigations proposing data-masking frameworks and methodologies seeking to control or minimize disclosure risks linked to the patients' data [27, 28]. Some of these methodologies include the removal or de-identification of data identifiers, data encryptions, data swapping, data perturbation, and micro-aggregation [28].

Despite the promising nature of these techniques, other studies contend that it is not possible to use them to delink all the patient identities contained in the health data [29]. Therefore, additional scholarly examinations have led to the evolution of *k*-anonymity algorithm as a means of protection enhancement [27, 28], as well as SQL searching mechanisms that target the patients' encrypted data [29, 30]. During data disclosure, the latter techniques have proved important in enabling the concerned healthcare organizations and stakeholders to maintain patient confidentiality. Another technique that has been proposed to aid in barring intruders from matching and accessing patient information that is publicly available is *k*-unlinkability. Particularly, this algorithm focuses on information such as trails revealing the patient's location visits. The following figures illustrate the functionality of the proposed algorithms that have gained increasing adoption towards barring unauthorized access to the patients' authorized disclosures.

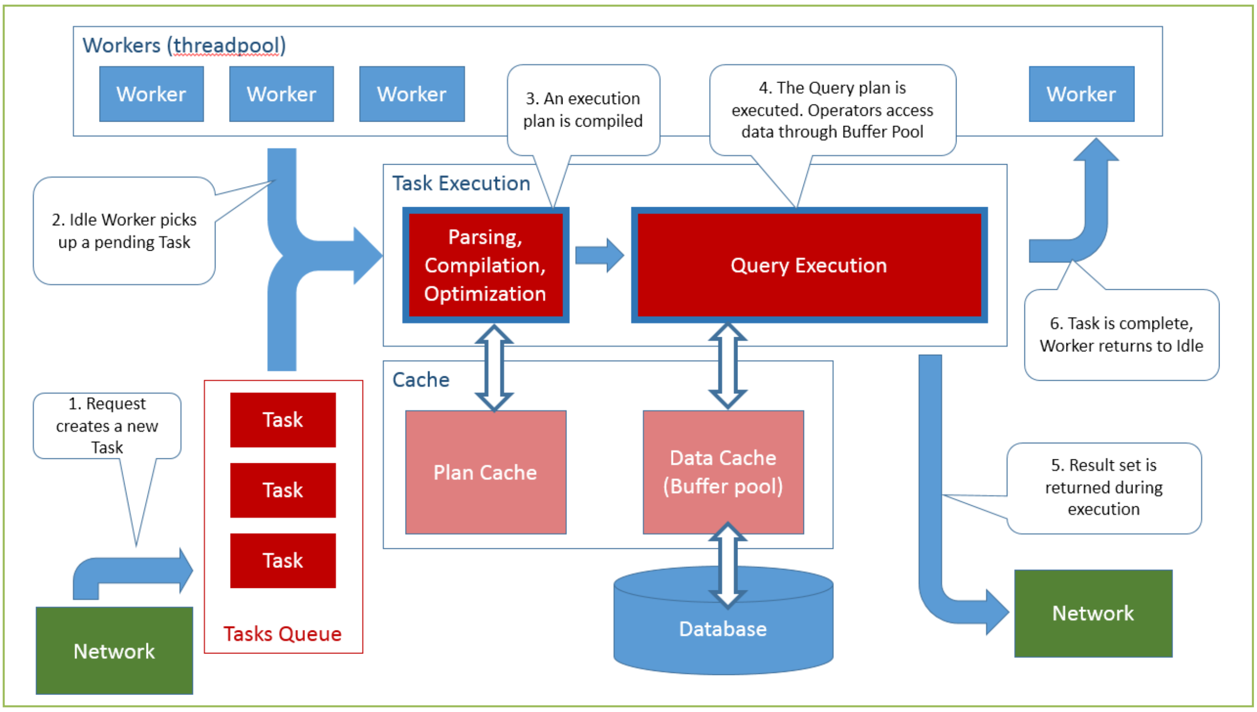
Workers (threadpool)
Worker
Worker
Worker
Worker
3. An execution plan is compiled
4. The Query plan is executed. Operators access data through Buffer Pool
2. Idle Worker picks up a pending Task
Task Execution
Parsing, Compilation, Optimization
Query Execution
6. Task is complete, Worker returns to Idle
Cache
Plan Cache
Data Cache (Buffer pool)
1. Request creates a new Task
Task
Task
Task
Tasks Queue
5. Result set is returned during execution
Network
Database
Network

Figure 6: Functionality of the proposed SQL searching mechanism

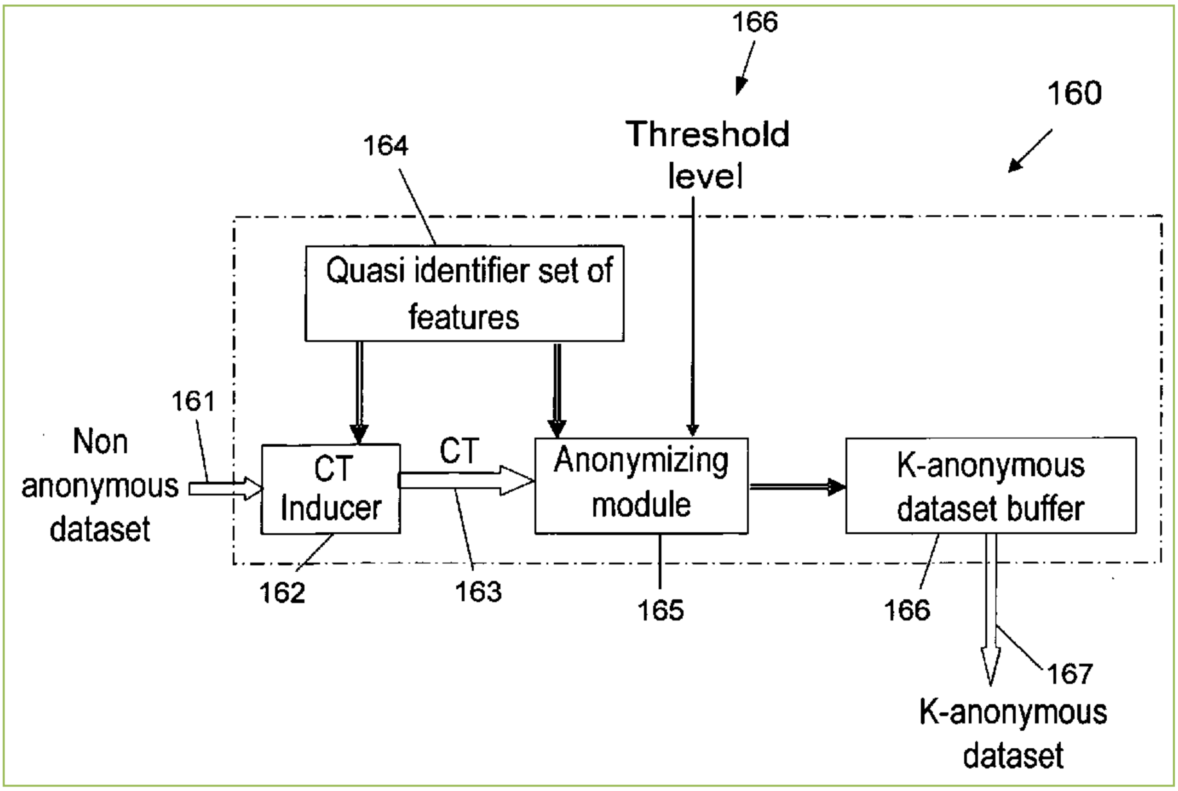

Figure 7: Illustration of the proposed *k*-anonymity algorithm for protecting authorized disclosures

5.Common Hospital Vulnerabilities and Why the Healthcare Industry Is Targeted

Since 2010, criminal attacks targeting the healthcare industry have increased by 125 percent [31]. Security attacks such as those that were witnessed in 2015 (in which over 100 million healthcare records leaked) have led to the exposure of medical records of the affected patients. Apart from major insurers, healthcare providers have been targeted. For instance, Blue Cross Blue Shield forms an example of a health insurer that has been targeted while Anthem forms an example of a healthcare provider that has been targeted by cyber attackers [31, 32]. In the past five years, additional scholarly observations indicate that the increase in security attacks targeting players in the healthcare industry has been more than twice [33]. This alarming trend attracts a further analysis of why the healthcare industry emerges as one of the most attractive targets of security attacks.

In most of the recent studies aimed at examining trends in cyber attacks and motivations behind the alarming rates documented above, findings suggest that the cybercriminals' quest to gain revenue combines with lax cybersecurity to account for such trends [29, 33, 34, 36]. One of the common vulnerabilities in the healthcare industry has been documented to entail the open physical space, with hospitals expected to maintain this space [34, 35]. The situation is compounded by the affirmation that throughout these hospitals, wireless networks continue to be scattered to connect medical systems and their corporate systems [35]. As such, the healthcare industry emerges as a target-rich environment due to the scattered wireless networks [33-35].

Research projects have also been conducted to investigate the manner in which cyber attackers exploit medical devices. One of such studies was conducted by TrapX Security. The target setting was in San Mateo, CA. The six-month experimental approach involved virtual replicas of medical devices, with the study conducted in a controlled environment. Findings suggested that a breakthrough would be realized if cybercriminals embraced *spear phishing*. It was also observed that hackers, upon using *spear phasing*, would smuggle malware from computers housed in the nurses' stations through the network systems of the healthcare organizations into devices such as radiological machines and blood gas analyzers [36]. Also, the study noted that outmoded operating systems controlled most of the target devices, including Windows XP and Windows 2000. Therefore, the devices failed to provide warnings or indicate the attacks to the healthcare providers; neither could they defend themselves from malware such as *spear phishing*. The defenseless and compromised medical devices were also used as platforms for penetrating further into the hospitals' networks to access the data source. The figure below illustrates the experimental set-up and results as reported by TrapX.

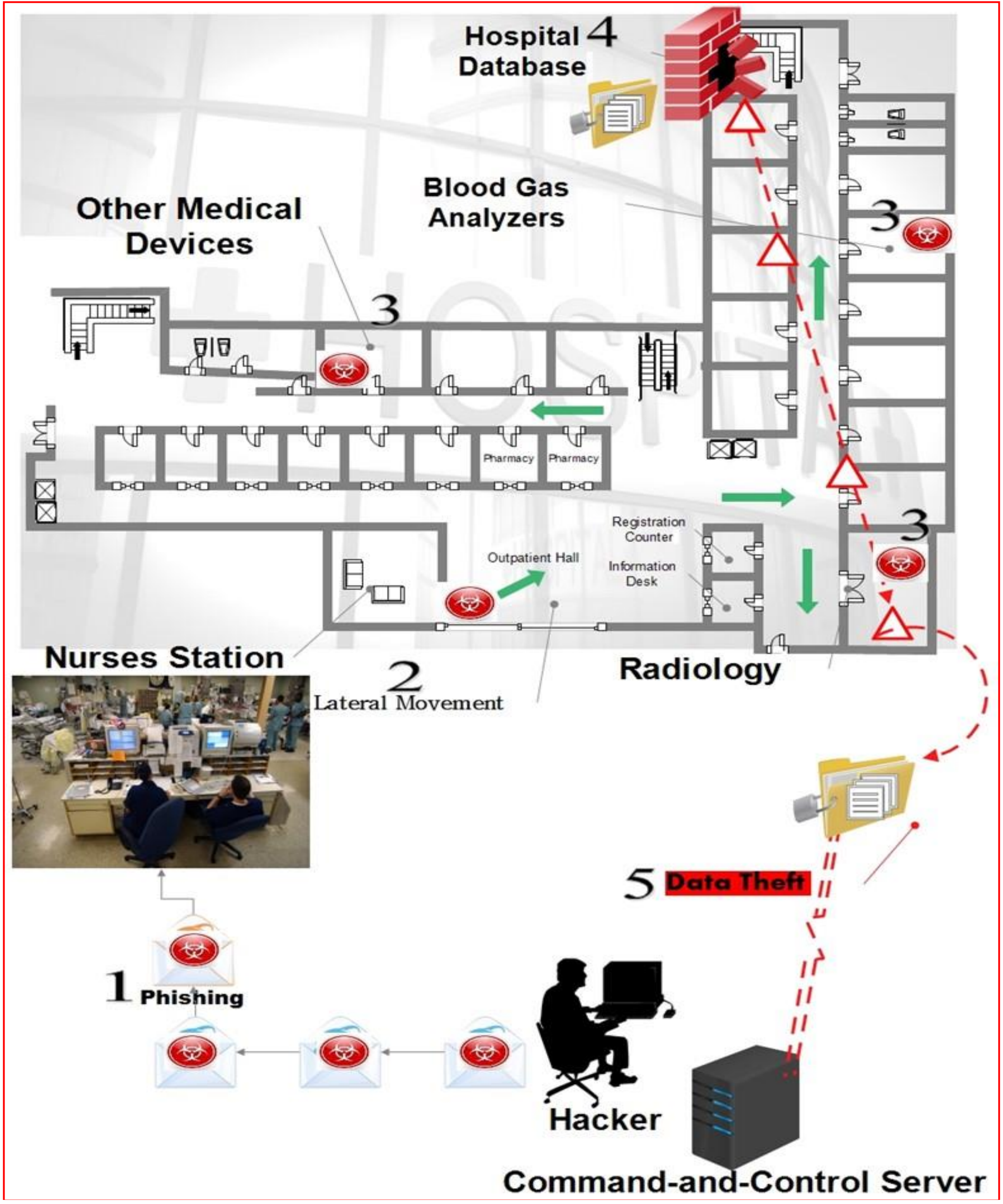

Figure 8: An experimental illustration of security attack as demonstrated by TrapX Company

Other researchers have experimented with the vulnerability of healthcare provider networks by launc6hing probe attacks. For such investigations, the external web servers have been the target environments [35, 36]. With the servers' vulnerabilities exploited, experimental results suggest that the cybercriminals could control machines and gain access to the internal controls, ensuring further that scans reveal vulnerable patient monitors. Similar observations by related scholarly investigations suggest that when the attackers access the hospitals' internal networks, they could force monitors to disable alarms, display wrong vital signals, and emit false alarms; adversities that are associated with serious patient harm [37, 38]. These results are demonstrated in the figure below.

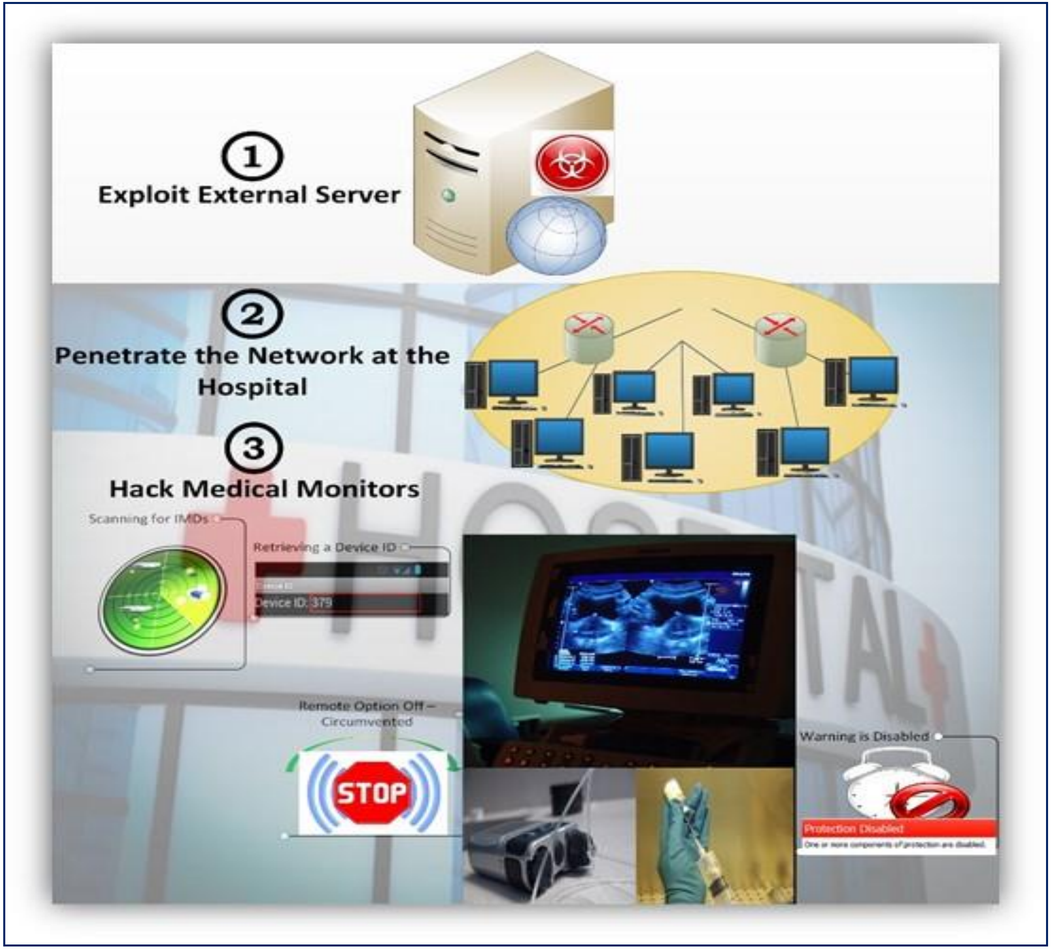

Figure 9: External web servers targeted by launching probe attacks

Based on the experimental results above, real-world security attacks have been witnessed in the recent past operations of the healthcare industry. For example, such an attack was witnessed at the Californian Hollywood Presbyterian Medical Center experienced a data breach in February 2016 while MedStar Health Inc. also succumbed to cyber attack about a month later. In the same month, a security attack was reported at San Diego's Alvaro Hospital Medical Center. Based on these worrying trends surrounding endpoint information security in the healthcare industry, several studies have focused on the best practices that might reverse the trend and assure future survival and safety or privacy of the patients' data.

6.A Review of the Proposed Best Practices to Counter Security Attacks in the Healthcare Industry

To protect healthcare data, most of the previous studies advocate for comprehensive cybersecurity approaches. However, some studies caution that the best practices ought to be flexible to the extent of ensuring that they keep abreast with the ever-changing threat landscape. The figure below summarizes the best practices that the majority of the previous studies have recommended.

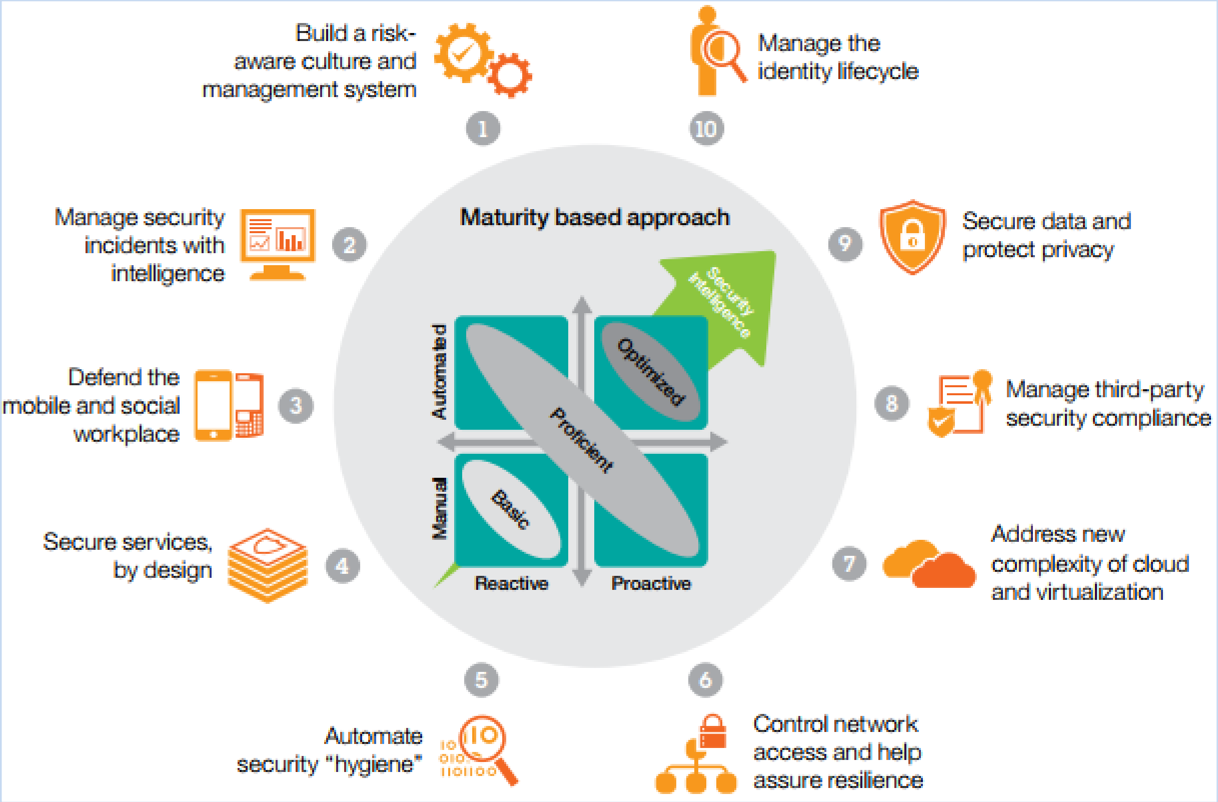
Build a risk-aware culture and management system
1
Manage the identity lifecycle
10
Manage security incidents with intelligence
2
Maturity based approach
Security Intelligence
9
Secure data and protect privacy
Defend the mobile and social workplace
3
Automated
Optimized
Proficient
8
Manage third-party security compliance
Manual
Basic
Secure services, by design
4
Reactive
Proactive
7
Address new complexity of cloud and virtualization
5
6
Automate security "hygiene"
Control network access and help assure resilience

Figure 10: Summary of the proposed best practices to counter security attacks in the healthcare industry

As shown in the figure above, one of the proposed solutions to security attacks in healthcare has been the establishment of risk-aware culture. For proponents of this strategy, most of the results indicate that all members of the organization can infect healthcare enterprises; including failure to install security patches on the mobile devices [29, 30, 32]. To establish a security-rich healthcare organization, these studies advocate for the involvement of all stakeholders and ensure that goals and risks are set; with the managed expected to play a leading role before ensuring that the intolerance against security attacks spreads top-down [31]. Other studies have proposed the realization of rapid threat responses and intelligent security operations [32, 33]. For these reports, an example that has been demonstrated in experimental set-ups in which related security incidents are experienced in a physician's office or remote clinic and others in hospital settings. Without security intelligence, most of the studies avow that these security incidents may be related but go unnoticed [33]. Hence, the need to establish a unified and automated system that would enable healthcare organizations to respond rapidly and monitor their operations has been documented [31-34].

Regarding the decision to defend the workplace in terms of mobile and social site security-rich collaboration, most of the results obtained by previous studies suggest that the majority of cybercriminals targeting healthcare firms have continually capitalized on organizational weaknesses. Some of the sites and devices that have been found to be possible targets of malicious attacks include Smartphones, laptops, and work stations [33, 34]. As such, the studies acknowledge the need to classify data streams across the healthcare firms, with sole routing and risk profiles linked to the respective user circles [33]. As mentioned earlier, devices used in healthcare organizations have been targeted by some of the recent security attacks. In response to this negative trend, some studies advocate for the need to design security-rich products [27, 28] while assuring hygienic IT management [24]. Whereas some organizations in the healthcare industry have stuck to old software programs [21], the management of updates on such programs has proved difficult [23]. As such, the scholarly investigations point to the need for the administrators to switch to current programs capable of installing patches and updates as they evolve.

Based on recent cases of security attacks among insurers and hospitals, in-depth analyses revel that firms that establish resilient and security-rich networks are better placed to survive; especially by utilizing monitored access points for purposes of channeling registered data [36, 37]. When resilient and security-rich networks are established in the healthcare industry, proponents predict that the administrators might be better placed to detect and isolate malware [29]. In the wake of complex virtualization and cloud computing, healthcare organizations with procedures and tools capable of monitoring potential threats and isolating themselves from others have been predicted to survive the future of the cyberspace [36-38]. Also, the current literature indicates that the management of the security compliance of third parties might enable organizations in the healthcare industry to counter possible security attacks [18]. Particularly, it has been established that the management of the state of security compliance among third parties stretches beyond organizational walls to ensure that best practices that touch on suppliers and contractors are established [18-22].

Regarding the assurance of data privacy and security, proponents avow that firms in the healthcare industry house non-public financial information of clients, some documents detailing mergers and acquisitions, technical and scientific data, and protected health information [37, 38]. To assure endpoint information security, the studies suggest that special treatment needs to be directed to the critical data; with regular inventory conducted. Lastly, the criticality of managing digital identity lifecycles has been documented. An example of this management has been illustrated for the case of a contractor who gets promotion and, later, is hired by a competitor in the healthcare industry [26]. In such a case, the initial system is expected to grant limited access and, eventually, cut the contractor's access completely [27, 28]. In so doing, the studies assert that the process assures successful management of the identity lifecycle. Some studies also caution that if the identity lifecycle is mismanaged, the vulnerability of healthcare organizations to intrusions might increase [35-38].

7.Conclusion

In summary, the healthcare industry's ability to remain ahead of security attackers calls for combinations of measures. Examples of these measures include quick reactions to potential or detected intrusions, the development of analytics that promise to spot intruders on time, and the use of robust system defenses. This paper has reviewed the current literature regarding the subject of endpoint information security, with critical insights gained from the case of the healthcare industry. In the findings, most of the previous scholarly studies contend that the healthcare industry forms one of the industries that security attackers have targeted. It is also evident that as the scale of the security attackers becomes sophisticated, the destructiveness and scale of intrusions targeting the healthcare industry is growing. Examples of recent events that have witnessed endpoint information security compromised in the healthcare industry include the Californian Hollywood Presbyterian Medical Center that experienced a data breach in February 2016 and MedStar Health Inc. (in the same month), as well as San Diego's Alvaro Hospital Medical Center that succumbed to a data breach in the following month. Based on these worrying trends, scholarly studies have proposed algorithms and strategies that might assure endpoint information security, especially in the healthcare sector. The proposed algorithms include the use of SOA-based EHRs, the implementation of the RBAC model, the use of *k*-anonymity, *k*-unlinkability, and the SQL searching mechanisms that target the patients' encrypted data. Some of the strategies that might reduce the incidence and prevalence of security attacks, as documented by most of the previous scholarly investigations, include the management of identity lifecycles, the establishment of risk-aware cultures, the management of third-party security compliance, and securing healthcare firms' devices in terms of design. In the wake of complex virtualization and cloud computing, it can be inferred that the future survival of organizations in the healthcare industry will depend on the extent to which they keep abreast with the evolving nature of endpoint information security.

References

[1] AHC Media LLC. Hackers target hospitals with "ransomware". *Ed Legal Lett*. 2016; 27(4): 1-4.

[2] Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS, Cyber threats to health information systems: A systematic review. *Technol Health Care* 2016; 24(1), 1-9.

[3] AHC Media LLC. Ransomware attacks are on the rise, and hackers are getting better. *Ed Legal Lett.* 2016; 1(4): 1-4

[4] Wu F, Eagles S, Cybersecurity for medical device manufacturers: Ensuring safety and functionality. *Biomed Instrum Technol.* 2016; 50(1): 23-33

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

[6] 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; 36(1): 14-24

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

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

[9] Streger M, Ransomware: a ticking bomb for public safety. *News Network* 2016; 12

[10] American Association of Critical-Care Nurses. Ransomware poses major threat to hospitals. *AACN Bold Voices* 2016; 8(6): 14 [11] Van Alstin CM, Ransomware: It's as scary as it sounds. But with security best practices, you can fight back. *Health Manag Technol.* 2016; 37(4): 26-27

[12] Goedert J, Security: the ransomware nightmare. *Health Data Management* 2016; 24(3): 10

[13] Conn J, Ransomware scare: Will hospitals pay for protection? *Modern Healthcare* 2016; 46(15): 8

[14] Tuttle H, Ransomware Attacks Pose Growing Threat. *Risk Management* 2016; 63(4): 4

[15] Valach AP, What to Do After a Ransomware Attack. *Risk Management* 2016; 63(5): 12

[16] 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

[17] Page A, Kocabas O, Soyata T, Aktas M, Couderc JP, Cloud-based privacy-preserving remote ECG monitoring and surveillance. *Annals of Noninvasive Electrocardiology* 2015; 20(4): 328-37

[18] Rios B, Cybersecurity expert: medical devices have 'a long way to go'. *Biomed Instrum Technol.* 2015; 49(3): 197-200

[19] Welch SS, Five things providers need to know about cybersecurity. *Journal of the Medical Association of Georgia* 2015; 104(1): 40-42

[20] McDermott IE, Ransomeware: Tales from the cryptolocker. *Internet Express* 2015; 35-37

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

[22] Coronado AJ, Wong TL, Healthcare cybersecurity risk management: keys to an effective plan. *Biomed Instrum Technol.* 2014; 26-30 [23] 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 [24] Bangs G, New Ransomware and Cyber extortion Schemes Hold Businesses Hostage. *Risk Management.* 2014; 61(8): 30

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

[26] Luo X, Liao Q, Awareness education as the key to ransomware prevention. *Information Systems Security* 2007; 16(4): 195-202

[27] Roberts J, The necessity of information security in the vulnerable pharmaceutical
industry. *Journal of Information Security* 2014; *5*, 147-153

[28] Appari A, Johnson ME, Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management* 2010; *6*, 279-314

[29] Arora S, Yttri J, Nilsen W, Privacy and security in mobile health mHealth research. *Alcohol Research: Current Reviews* 2014; *36*(1), 143-150

[30] Claunch D, McMillan M, Determining the right level for your IT security investment. *Healthcare Financial Management* 2013; *67*(5), 100-103

[31] Cucoranu IC, Parwani AV, West AJ et al. Privacy and security of patient data in the pathology laboratory. *Journal of Pathology Informatics* 2013; *4*, 23-39

[32] Hedström K, Karlsson F, Kolkowska E, Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security* 2013; *21*, 266-287

[33] Perakslis ED, Cybersecurity in health care. *The New England Journal of Medicine* 2014; *371*, 395–397

[34] Roberts J, The necessity of information security in the vulnerable pharmaceutical industry. *Journal of Information Security* 2014; *5*, 147-153

[35] Wikina SB, What caused the breach? an examination of use of information technology and health data breaches. *Perspect. Health Inf. Mana.* 2014; 1-16

[36] Liu V, Musen MA, Chou T, Data breaches of protected health information in the United States. *J. Am. Med. Assoc.* 2015; 313(14): 1471-1473

[37] Lemke J, Storage and security of personal health information. *OOHNA J.* 2013; 32(1): 25-26

[38] Chen YY, Lu JC, Jan JK, A secure EHR system based on hybrid clouds. *J. Med. Syst.* 2012; 36(5): 3375-3384

Appendices

Appendix A: Summary Review of Selected Articles

Article	Objective	Findings
Wu et al. [4]	To investigate new wireless applications in endpoint information security in the healthcare sector	Device vulnerability continues to account for rising cyber attacks Hence, safety risk management needs to be redefined to counter the security attacks
Rowe [5]	To determine the role of Acts such as HITECH and ACA in addressing security attacks in the healthcare industry	The Acts provide room for greater network integration in the healthcare industry, promise future survival among organizations
Blanke & McGrady [6]	To examine trends in the evolution of cyber attacks in the healthcare industry	Risk monitoring and assessment form initial strategies that are likely to reduce the incidence and prevalence of security attacks in the healthcare sector
Hagland [7]	To find out some of the reasons why the healthcare industry is one of the most targeted sectors facing security attacks	The use of outdated software and the complexity in the physical space of hospital settings, as well as the increasing adoption of virtualization and cloud computer account for high rates of security attacks in the sector
Streger [9]	To find out the dominant security attacks facing healthcare organizations	Most of the attacks target devices Also, firm employees and retirees or those who have been laid off form a major threat to the IT infrastructure
Van Alstin [11]	To examine the current trends in security attacks among healthcare organizations and their specific departments	Increasing sophistication among cybercriminals has complicated the world of endpoint information security and, as healthcare organizations grappled with the threats, cybercrime is growing in the healthcare industry
Tuttle [14]	To establish some of the means through which healthcare organizations have addressed the challenge of security attack	Most of the organizations that face data breach resort to paying ransom In these cases, the majority of the firms fail to report the incidents to the rest of the public
Goedert [12]	To determine some of the contributory factors responsible for increasing trends in ransomware ransoms among healthcare organizations	Ransomware ransom is perceived to be inexpensive, attracting most of the targeted firms towards this path The absence of well-trained endpoint information security staff compounds the situation
Koppel et al. [16]	To investigate some of the emerging issues in endpoint information security among healthcare organizations	Most of the medical devices remain at-risk for security attacks Also, most of the cybercriminals have been responsive to changes in technology and healthcare organizations that fail to keep abreast with technological trends are more vulnerable
Page et al. [7]	To establish the role of endpoint information security in the practice of Telehealth	Methods such as end-to-end encryption are compatible with HIPAA requirements, especially in terms of access to Protected Health Information (PHI), as well as cloud storage that is HIPAA-compliant