Journal of Medical Systems (2020) 44:98
https://doi.org/10.1007/s10916-019-1507-y

SYSTEMS-LEVEL QUALITY IMPROVEMENT

# Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations

**Soumitra Sudip Bhuyan**[1] · **Umar Y Kabir**[2] · **Jessica M. Escareno**[2] · **Kenya Ector**[2] · **Sandeep Palakodeti**[3] · **David Wyant**[4] · **Sajeesh Kumar**[5] · **Marian Levy**[2] · **Satish Kedia**[2] · **Dipankar Dasgupta**[6] · **Aram Dobalian**[2]

Received: 31 July 2018 / Accepted: 14 November 2019

**Abstract**

The recent rise in cybersecurity breaches in healthcare organizations has put patients' privacy at a higher risk of being exposed. Despite this threat and the additional danger posed by such incidents to patients' safety, as well as operational and financial threats to healthcare organizations, very few studies have systematically examined the cybersecurity threats in healthcare. To lay a firm foundation for healthcare organizations and policymakers in better understanding the complexity of the issue of cybersecurity, this study explores the major type of cybersecurity threats for healthcare organizations and explains the roles of the four major players (cyber attackers, cyber defenders, developers, and end-users) in cybersecurity. Finally, the paper discusses a set of recommendations for the policymakers and healthcare organizations to strengthen cybersecurity in their organization.

**Keywords** Cybersecurity · Cyber security · Data breach · Patient data · Security · Privacy · Blockchain · Cyberattack

## Introduction

Advances in technology have had numerous societal benefits, including in the healthcare sector. The rise in the use of Electronic Health Records (EHR) is expected to reduce healthcare costs by improving the quality and delivery of timely healthcare services [1]. Recognizing these benefits, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to increase the number of healthcare organizations adopting Health Information Technology (HIT) [1]. While HIT has substantial benefits, integrating healthcare with technology has increased the likelihood of breaches of patient records [2].

Information that is lost, stolen, displaced, hacked, or communicated to unofficial recipients is defined as a breach of information; and this disruption in data information is considered a cyber-attack [3, 4]. About 94% of healthcare organizations have experienced at least one of these types of cyberattacks [5]. An estimated 150 million patient health records have been breached between 2009 and 2014 [6]· The majority of the breaches during this period were the result of breach, loss, or theft of portable computing devices [6].

A study conducted by McCue found that insiders rather than outsiders conduct 70% of data fraud in organizations [7]. The richness of data housed by healthcare entities has been cited as a primary reason that healthcare is susceptible to high data breach and financial risks [8]. Healthcare organizations usually possess a high volume of sensitive data. Data containing names, date of birth, social security number, address, and credit card information are abundant in hospital and insurance records. Moreover, hackers prefer focusing on healthcare organizations because healthcare data is more valuable than data from other industries in the black market. An

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Soumitra Sudip Bhuyan
bhuyanss@ejb.rutgers.edu

[1] Rutgers Urban and Civic Informatics Lab, Edward J. Bloustein School of Planning and Public Policy, Rutgers University, New Brunswick, NJ 07920, USA

[2] School of Public Health, The University of Memphis, Memphis, TN 38152, USA

[3] CareMore Health, Memphis, TN 38104, USA

[4] Jack C. Massey Graduate School of Business, Belmont University, Nashville, TN 37212, USA

[5] Health Info & Info Management, University of Tennessee Health Sciences Center, Memphis, TN 38104, USA

[6] Department of Computer Science, The University of Memphis, Memphis, TN 38152, USA

Published online: 02 April 2020

EHR, for instance, is worth between 10 and 100 times more than credit card information in the black market [9].

Cyber breaches add to the financial burden for the healthcare industry, which already confronts high expenditures and low-profit margins in comparison to many other industries. Presently, the average cost of data loss is greater for a healthcare organization compared to organizations in other sectors [8]. The penalties and fines imposed by entities like the Health and Human Services' Office for Civil Rights further compound the financial burden suffered by healthcare organizations, although they incentivize companies to improve their cybersecurity. It is estimated that data breaches will lead to $309 billion in lost revenue by 2019 [6].

The problem of cybersecurity goes beyond patients' privacy and the financial burden on the industry; it also poses a threat to patient safety [8]. For example, the use of wireless medical devices may expose patients to threats from cybercriminals. A cybersecurity flaw in a cardiac device like the one recently detected by the U.S. Department of Homeland Security could be exploited by cybercriminals to harm a patient [10]. Safeguards such as, encryption, shredding documents, locking doors, and using passwords, should be implemented to limit exposures and avoid inadvertent disclosures to protect sensitive healthcare information and reduce cyberattacks [3].

Despite growing threat of cyberattacks in healthcare, the research on this topic is nascent and there are major gaps in its literature [11]. To encourage awareness and further research on this topic, this paper discusses emerging threats posed by cyberattacks in healthcare as well as critical players involved in the cybersecurity. This paper also delves into existing cybersecurity policies at both the federal and state government levels and offers recommendations for policymakers to optimize healthcare cybersecurity. Finally, it identifies directions for further research on healthcare cybersecurity.

## Types of Cyberattacks

There have been some attempts to classify cybersecurity threats [12]. Each of these studies has utilized a different set of criteria to classify cybersecurity based on the purpose, severity, scope, and legality of cyberattacks [4]. We discuss the major types of cyberattacks and the motivations behind them.

### Denial-of-Services (DoS)

The aim of a DoS attack is to flood a network with traffic in order to disrupt service and prevent users from accessing network resources [13]. This type of attack is capable of significantly slowing or shutting down the entire network of a healthcare organization. The attack on Boston Children's Hospital in 2014 is an example of how "hacktivists" deployed a distributed DoS attack to disrupt the network of several organizations [14]. In addition to the financial losses related to restoring systems after a DoS attack, it is particularly dangerous as it can prevent healthcare providers from accessing or transmitting vital information during the attack.

### Privilege Escalation

Privilege escalation attacks are driven by the goal of achieving a higher level of access to a network or program; they are usually executed by exploiting vulnerabilities in a program or network [15]. Hackers could choose to use the elevated access to do a number of things to the system, such as changing a patient's chat information, thereby, compromising the patient's safety. There are two major types of privilege escalation attacks: vertical and horizontal [16]. "Multi-layered attacks" can also utilize malware to escalate privileges on a system and inflict even more damage.

### Man in the Middle (MITM) or Eavesdropping

An eavesdropping attack is considered a type of reconnaissance attack [4]. It occurs when an intruder intercepts communications between two parties [17]. The attacker eavesdrops on the contents communicated by secretly acting as an intermediary in the information exchange. The integrity of the data communicated can easily then be compromised since the intruder is capable of altering the data before relaying it to the other party or parties, unbeknownst to them. In healthcare, an eavesdropper could gain access to confidential information and possibly even blackmail patients.

Man-in-the-Browsers (MITB) attacks build on MITM attacks by facilitating the attack remotely. The most sophisticated MITB attacks utilize Trojan malware that is capable of evading antivirus programs [18].

### Cryptographic Attack

A cryptographic attack is carried out with the intention of revealing information that has been concealed; in other words, it seeks to decrypt encrypted information [19]. Cryptography is the process of encrypting and decrypting information into codes, so only the sender and intended receiver can understand it [20]. The binary coding obscured to others because the algorithms used in encrypting the information are only accessible to its creator [21].

### Structured Query Language Injections Exploit

Several websites use the programming language Structured Query Language (SQL) to manage their databases. Vulnerabilities in SQL may be exploited by hackers to execute malicious "payloads" (harmful SQL statements) that make the data servers divulge information. During such an SQL injection attack, hackers can alter the information in the database, affecting the integrity, confidentiality, and availability of information stored on that database [22]. In 2015, vulnerability in version 3.3 of Epiphany Cardio Server, a central web-application that manages data for hospitals, was discovered that could allow for an SQL injection to exploit it [23].

## Malicious Software

Malware or malicious software refers to a group of programs that are designed to harm or compromise a computer system without the permission of the user [24]. These programs carry out various functions that include altering, damaging, spying, or deleting user information. Malware is spread either physically using an external drive or through internet downloads such as "phishing" emails. Some common malware are worms, bots, viruses, adware, Trojans, spyware, adware, backdoors, ransomware, and rootkits.

### Virus

A virus, the most common malware, self-propagates without the permission of the user and infects other computers [25]. Viruses are usually malicious; they perform actions like deleting or corrupting data [26]. Although viruses are self-propagating, they require user activation to exact their effect but replicate automatically [25]. The need for user activation is due to the fact that the majority of viruses are executable files attached to host file.

In 2017, a virus shut down the computer system at Erie County Medical Center in upstate New York and delayed performance as laptops had to be distributed to staff so they could access backed up patient information [27].

### Trojans

Like the mythological Trojan horse, this piece of malicious software is designed to appear as useful, legitimate software [25]. Another important feature of a Trojan is that, unlike viruses and worms, this type of malware is not self-replicating and does not need a host file [25, 28]. Trojans can give hackers a "backdoor" to allow access to an infected system [25]. The Alaska Department of Health and Social Services was recently hit by a Trojan attack, and two computers were found to have malicious software that masqueraded as legitimate applications [29]. It is possible that the Trojan horse had already created a backdoor through which patients' records were exposed.

### Spyware

Spyware is "a software that is installed on a computer without the user's knowledge and transmits information about the user's computer activities over the Internet" [30]. Spyware works covertly on a system and allows the attacker to monitor the target's usage and gather personal information [31, 32]. A spyware can come in the form of a Trojan horse utilized to carry MITM attacks. Spyware can also slow down computers, typically by overworking the system [31].

### Ransomware

Lately, stories of ransomware attacks have become a daily headline in the news [33]. A central feature of this type of malware attack is the demand for ransom in exchange for decryption of information [33]. Ransomware, however, can use one of the several other types of malware to hack an organization. Occasionally, in addition to encrypting the victim's information, the hackers threaten to sell or expose the information to the public if the ransom is not paid. The 2017 attack on Britain's National Health Service (NHS) was facilitated using ransomware named WannaCry (also known as WannaCrypt). This attack hindered patient care throughout the health system [34].

## Phishing

The use of social engineering to trick individuals or organizations into either divulging information or perform an activity harmful to their computer is referred to as phishing [35]. Phishing is more of a technique or a vector than a type of attack. It is one of the most common ways to delivery malware [36]. Assailants usually make use of emails that redirect the receiver to a website, which either collects their information or prompts the download of malicious software. Spear-phishing is a type of more targeted phishing that is directed at certain individuals or organizations [37]. New York's largest provider, Kaleida Health, was breached twice in 2017 using the spear phishing technique and more than 3000 patient records were compromised [38].

### Worms

Unlike viruses, worms do not rely on a host file to run, self-replicate, or propagate [25]. Dissemination of worms usually depends on vulnerabilities in the target system or through social engineering [25]. The WannaCry that affected Britain's NHS is a worm by design [34].

## Major Players in Cybersecurity

The major players in cybersecurity include a host of individuals and organizations that range from software developers to end-users [19]. These players include hackers, cybersecurity professionals, software developers, government regulators, and end users. Each of these individuals plays either a critical role in safeguarding or jeopardizing cybersecurity. A deep understanding of their roles in achieving cybersecurity and a recognition of their limitations will aid healthcare organizations in better planning to prevent cyber breaches.

### Cyber-Attackers

Cyber-attackers constitute the main threat to cybersecurity. Cyber attackers are the main reason that cybersecurity exists. Understanding the motivation of the various type of cyber-attackers can serve as a foundation for building strong cybersecurity protocols.

A hacker is an individual that seeks to gain remote access to data with or without authorization [39]. However, when the attempt is made without a malicious or criminal intent and under the appropriate authorization, it is referred to as ethical hacking [40]. Therefore, the intent and authorization status determines the type of attacker. Attackers use one or a combination of cyberattack methods to achieve their goals.

Fischer (2016) broadly classified cyber attackers into hacktivists, terrorists, spies, and criminals [41]. This classification is similar to Goderdzishvili's classification of cyber-attack based on legality in 2010 [42]. Under these two authors' classification, cybercriminals are individuals that use a computer to commit crimes like theft or extortion, and their motivation is usually monetary. Hacktivists, however, are fueled by nonmonetary motivations; they engage in cyber attacks to promote their political agenda. The two studies defined cyberterrorists as individuals that are involved in the deliberate disruption of computer networks. Cyber terrorists could belong to either subnational or clandestine groups. Hackers involved in espionage are cyberspies who eavesdrop on sensitive classified or proprietary materials belonging to either government, private companies, or individuals.

### End Users

End users also play a crucial role in ensuring cyber security. End users can be either malicious or non-malicious players, and both present a specific kind of threat. End users have proven to be a "weak link in protecting organizations against some cyber-attack strategies [43].

A study of over 900 breaches in 2010 revealed that insiders who are either current or former employees were responsible for orchestrating 48% of all data breaches in the study, and only 10% of the incidents were unintentional [44]. Malicious insiders are deemed extremely dangerous since they are familiar with strengths and weakness of the system [45]. However, non-malicious end users also serve as a gateway for cyber attacks. For example, spam emails that carry a cyber threat spread only because somewhere along the system, a spammer is using someone's machine as a host [46]. In a survey in 2013 by the SANS Institute, 50% of all the responders consider non-malicious users the top threat to cybersecurity [47].

Even if healthcare organizations implement the best security protocols, failing to prepare their workforce, i.e. end users, leaves them susceptible to cyber-attacks. To be fully capable of preventing cyber-attacks, the organization must prepare their workforce. Employee education should focus on understanding privacy and security related to protecting patient information [48]. Employee monitoring and human security testing should also be a priority [49].

It should be noted that security policies put in place to protect networks against cyber breaches may be a source of nuisance for end-users. Accordingly, achieving a successful cybersecurity culture in an organization requires obtaining the buy-in of end-users and understanding their needs [19].

### Cyber Defenders

The cyber defender is an umbrella term that we adopt for a vast array of individuals that are actively working to ensure cybersecurity. These include IT professionals (cybersecurity experts) and government agencies. Information technology professionals that work to ensure cybersecurity go by different titles; among the commonly used titles for them are security engineers or architects, security analysts, IT directors, and systems administrator [50]. Their primary role is in planning and executing security measures to ensure that their organization is protected from cyber threats [51]. The healthcare field is currently facing a shortage of cybersecurity experts. This shortage is attributed to low pay and lackluster recruiting efforts [52].

Several government departments are charged with defending cybersecurity, for example, the Department of Homeland Security and Department of Justice are responsible for apprehending and charging cybercriminals, respectively [41]. Other government agencies like the National Institute of Standards and Technology (NIST) contribute to the development of frameworks for ensuring cybersecurity [53]. Congress has recently taken an active role in developing laws aimed at mitigating cybercrimes. Between the 113th and 114th Congress sessions, at least six cybersecurity bills were enacted [41].

### Developers

Developers are essential to ensuring cybersecurity as it is their mistakes that cyber attackers exploit to breach systems.

Malware can easily be introduced into a network when there are mistakes in programming by developers [54, 55]. An estimated 90% of security incidents happen through exploiting a vulnerability in a software program [56]. For example, the Wannacry ransomware attack of 2017 that affected over 99 countries exploited a vulnerability in Microsoft Server Message Block (SMB) in Windows [57]. Vulnerabilities like this one are ubiquitous and growing in number. The National Vulnerability Database of NIST currently lists more than 100,000 Common Vulnerabilities and Exposures (CVS) in its database [58].

While several organizations choose to invest money in protecting their networks, many breaches actually occur at the application layer [59]. The apparent disconnect between developers and defenders also strains defenders and ultimately weakens cybersecurity [60]. In a survey of developers by SANS in 2015, it was discovered that less than 20% of security testing is conducted by the development team or quality assurance personnel in an organization [60]. To strengthen the backbone of cybersecurity, security-risk-aware programming principles must be applied in developing software [61]. In addition, the information silo that exists between developers and defenders has to be broken [60].

## Recommendations

Cybersecurity issues threaten access, quality, and cost in health care. Technology offers hopeful alternatives for each of these goals, but in order to realize the benefits of these technologies, cybersecurity issues must be resolved.

### Policymakers

1. In dealing with cybersecurity, policymakers face a constantly evolving target. For example, when the meaningful use incentive program was first enacted, handheld mobile devices were a relatively minor part of eHealth, compared to more recent times. Furthermore, the regulatory process takes time and can be difficult to change. Consequently, policymakers will likely continuously be in a catch up mode as they try to develop cybersecurity policies. For example, although HIPAA laws have been updated (for example to deal with the issue of business associates), as technology changes, it can be expected that HIPAA will need to evolve further [62].
2. Policymakers should note that major government programs, such as Medicare, Medicaid, and the Veterans Health Administration (VHA) might have specific program goals that are threatened by cybersecurity issues. For example, these programs might want to encourage alternative delivery approaches through the use of technology (for example, telemedicine). Over the past few years, VHA has begun to make significant investments in telehealth. Consequently, policymakers must deal with cybersecurity both from the perspective of the threat to our society in general, and also from the perspective of the threat to particular government programs.
3. Cybersecurity issues in healthcare are linked to the larger set of cybersecurity issues in society. As innovations occur, policymakers may need to alter the regulatory environment to allow technological innovations to be applied to healthcare. For example, some observers believe that blockchain technology offers the possibility of highly secure, decentralized, and longitudinal health records [63]. This technology would likely require regulatory changes. For example, HIPAA's 1996 security, privacy, and transaction sets are not aligned with blockchain technology [64].

### Healthcare Organizations

1. For healthcare organizations, cybersecurity involves trade-offs. For example, an organization may consider enhancing privacy by requiring that a patient grant approval before a specialist may access the patient's information. However, that could delay the completion of the referral. It is worth noting that claims processing staff and insurance company staff have access to much of the patients' information [65]. In addition cybersecurity measures may use significant resources. Financial costs are not the only concern in this regard. There is also the opportunity cost of key IT staff. In considering cybersecurity initiatives, it has been suggested that governance should take the approach that they are managing a "portfolio" of IT projects, and that the use of staff on one project will make that staff unavailable for other projects. There is an extensive literature on project portfolio management in this regard [66].
2. One concern for deciding HIT risk trade-offs is the idea of "hiding in the bell curve". An organization does not want to badly trail their peers in meeting a regulation; however, there is likely little to gain by going through the expense of greatly outpacing their peers. If instead an organization is in the middle of the peer group, it is unlikely to be the focus of regulators or strongly disadvantaged competitively [67].
3. Healthcare organizations, like all other organizations, need to take a comprehensive approach to cybersecurity rather than an ad hoc approach of dealing with threats on a case-by-case basis as they are discovered. The ad hoc process faces a difficult challenge in adequately identifying and addressing all emerging security gaps. Security should be viewed in the context of processes, and not specific technological fixes. Concerning security

problems, Schneier stated, “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” [68].

4. One example of a comprehensive approach to cybersecurity is the CERT Resilience Management Model [69]. In the context of this model. “resilience” is the ability of an organization to withstand an impact, continue operations, and return to the original condition. The model includes a detailed evaluation of process areas throughout an organization. This comprehensive approach includes establishing a governance structure over each process, and ensuring that planning, training, financing, and other factors are adequate to achieve required resilience in each process area.
5. Another approach is risk management. This approach involves a risk assessment that begins with identifying potential risks. Once each risk is identified, the specific asset and vulnerability are determined. Next a risk assessment is developed based on the likelihood of an adverse event, the impact if that event occurs, and any safeguards currently in place to reduce the effect of the occurrence. The next step is mitigation planning, where a specific step is identified, a person is made responsible, and a due date is assigned. The activity is then monitored and a revised assessment of the risk is made following the mitigation. Traditionally the different approaches to risk management have been classified under the headings of mitigating risk, avoiding risk, transferring risk (i.e. through insurance) and bearing risk [70, 71]. To avoid preconceived biases and cover-ups, risk assessments can be conducted through external parties.
6. The choice of risk management techniques has been influenced by the emerging field of cyber insurance. Policies may be purchased that cover expenses associated with data breaches, including “notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft” [72]. Vaughan & Vaughan provide “rules” to help guide the decision about how to respond to specific risks during the risk management process, including a “tool” that helps identify which risks should be insured against [73]. However, the healthcare organizations should have a clear understanding of what is covered under cyber insurance and under which circumstances.
7. Another option for a comprehensive approach is to integrate cybersecurity into the strategic planning and budgeting process. Over time, there has been a change in the role of IT in the planning process. At first, the IT manager was viewed as an “applications provider” and was not part of the strategic planning process. However, it has since been recognized that spending on IT was often inconsistent with the organization’s strategic goals, and consequently efforts were made to “strategic align” the goals of the organization and the IT budget. This was followed by recognition that the IT manager could be viewed as a “strategic contributor” (instead of reacting to a completed plan), and be part of the planning team that is conducting the “strategic assessment”. One goal was IT fusion, which exists when there is a high degree of alignment between IT and the rest of the organization. Building on this concept, Bensaou and Earl discussed the idea of “strategic instinct” [74]. They point to the example of Japan where IT investments tend to be made not because of specific goals, but because the investment is essential to the long-range objectives of an organization.
8. In another comprehensive approach Baker attempts to generate a “trust framework” by creating layers of protection [75]. The first layer of protection is risk management; and the second layer is information assurance policy that covers policies for security, privacy, and safety. The third layer consists of physical safeguards such as, workstations and devices. The fourth layer is operational safeguards such as, training, designating a security officer, and continuity of operations planning. Layer five is architectural standards, dealing with interoperability, availability, and reliability. Layer six is a technology safeguard regarding data encryption, access control, audit controls, and protection against malicious software. Layer seven is usability features such as single sign-on. These layers are expected to work together to create trustworthiness for data security and privacy.
9. Training rank and file employees is important. There is an adage in cybersecurity that goes “You are only as safe as your ‘weakest’ person”. One key concern is countering efforts at social engineering. Depending on the circumstances, other safeguards may be put in place. For example, one type of social engineering involves leaving a USB drive in an employee parking lot in the hopes that an employee will take it inside and try to determine what is on it. Such threats are countered by not having USB drive ports on computers. Another increasingly important area for training is the appropriate and cautionary use of handheld devices.
10. A hospital-specific approach is suggested by the American Hospital Association (AHA), which proposes six actions to manage cybersecurity risk [76]. Three of the six involve planning. These are developing a response plan: establishing procedures, cybersecurity teams, and testing the response plans. The AHA suggests that the plan be “mindful” of NIST’s Cybersecurity Framework [77]. The other three actions

focus on specific issues: investigate all medical devices following FDA guidelines, participate in information sharing organizations that identify new risks facing hospitals, and make sure insurance covers cybersecurity risks [78].

11. Another potential strategy could be monitoring the user's behaviors and leveraging the identity and access management protocols.

## Summary

Healthcare organizations face a variety of crucial challenges that they have little control over; examples include the general economy, reimbursement policy by major payers, and the regulatory environment. Within the challenges over which they do have some control, the response cybersecurity threats is likely to strongly influence their long-term success. Fortunately, management actions can have significant impact on a meaningful cybersecurity planning and implementation. This review can assist healthcare managers in prioritizing actions that would be appropriate in strengthening the cybersecurity of their organization.

### Compliance with Ethical Standards

FedEx Institute of Technology University of Memphis funded this study.
For this type of study, formal consent is not required.

**Human and Animal Studies** This article does not contain any studies with human participants or animals performed by any of the authors.

**Conflict of Interest** The authors have no conflict of interest to declare.

### Glossary

| | |
|---|---|
| Cryptographic attack | An attack carried out with the intention of revealing information that has been concealed. |
| Cyber-attack | The act of intentionally disrupting data information. |
| Data breach | This is when information is lost, stolen, displaced, hacked, or communicated to unofficial recipients. |
| Denial-of-Services (DoS) | An attack that aims to flood a network with traffic in order to disrupt service and prevent users from accessing network resources. |
| Malicious Software or Malware | A group of programs that are designed to harm or compromise a computer system without the permission of the user. |
| Man in the Middle (MITM) or Eavesdropping | A reconnaissance attack in which an intruder intercepts communication between two parties. The attacker eavesdrops on the contents communicated by secretly acting as an intermediary in the information exchange. |
| Phishing | The use of social engineering to trick individuals or organizations into either divulging information or perform an activity harmful to their computer. |
| Privilege escalation | Attacks driven by the goal of achieving a higher level of access to a network or program; they are usually executed by exploiting vulnerabilities in a program or network. |
| Spyware | A software that is installed on a computer without the user's knowledge and transmits information about the user's computer activities over the Internet. |
| SQL Injections Exploit | Attack that exploit vulnerabilities in SQL to execute malicious "payloads" (harmful SQL statements) that make the data servers divulge information. |
| Trojans | A type of malware designed to appear as useful, legitimate software. |
| Virus | A common malware that self-propagates without the permission of the user and infects other computers. |
| Worms | A type of malware that does not rely on a host file to run, self-replicate, or propagate. |

## References

1. HealthIT (2018). Benefits of Electronic Health Records (EHRs). Retrieved from https://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs
2. American Hospital Association (n.d.). Cybersecurity; Cybersecurity vulnerabilities and intrusions pose risks for every hospital, and its reputation. Retrieved from https://www.aha.org/advocacy/leveraging-technology/cybersecurity
3. Department of Health and Human Services (2013). Summary of the HIPAA privacy rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.
4. Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. International journal of Network Security, 15(5), 390–396.
5. Filkins, B. (2014). Health Care Cyberthreat report: Widespread compromises detected, compliance nightmare on horizon. *SANS* Norse. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735
6. Berger, D. W. (2016). Breach Report 2015: Protected health information (PHI). Redspin. Retrieved from https://www.redspin.com/resources/download/breach-report-2015-protected-health-information-phi/

7. McCue, A. (2008). Beware the insider security threat, CIO jury. Retrieved from http://www.silicon.com/management/cio-insights/2008/04/17/bewaretheinsider-security-threat-39188671/
8. Perakslis, E. D. (2014). Cybersecurity in health care. N Engl J Med, 371(5), 395–397. Retrieved from https://pdfs.semanticscholar.org/286f/f60b6740da758bb47340d83ca409c72fc906.pdf
9. Akpan, A. (2016). Has health care hacking become an epidemic? The Public Broadcasting Service. Retrieved from https://www.pbs.org/newshour/science/has-health-care-hacking-become-an-epidemic
10. Chicago Tribune (2017). Homeland Security warns that certain heart devices can be hacked. Retrieved from http://www.chicagotribune.com/lifestyles/health/ct-cybersecurity-flaw-in-heart-devices-20170111-story.html
11. Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: bibliometric analysis of the literature. Journal of medical Internet research, 21(2), e12644.
12. Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489–496.
13. Unite States Computer Emergency Readiness Team (2009). Security Tips (ST04–015): Understanding Denial-of-Service Attacks. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015
14. Nigrin, D. J. (2014). When “Hacktivists” Target Your Hospital. New England Journal of Medicine 371(5), 393–395. Retrieved from https://doi.org/10.1056/NEJMp1407326
15. Long, M.C. (2016). Attack and Defend: Linux privilege escalation techniques in 2016. The SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/testing/attack-defend-linux-privilege-escalation-techniques-2016-37562
16. Piscitello, D. (2016). What is Privilege Escalation? Retrieved from https://www.icann.org/news/blog/what-is-privilege-escalation
17. Lab, K. (n.d.). Man in the Middle Attack -Kaspersky Daily. Retrieved from https://www.kaspersky.com/blog/man-in-the-middle-attack/1613/
18. Cain, C. (2014). Analyzing Man-in-the-Browser (MITB) Attacks. *SANS Institute*. https://www.sans.org/reading-room/whitepapers/forensics/analyzing-man-in-the-browser-mitb-attacks-35687
19. Langer, G. (2017). Cybersecurity Issues in Healthcare Information Technology. J Digit Imaging 30(1):117–125. doi: https://doi.org/10.1007/s10278-016-9913-x
20. Encyclopedia Britannica (n.d.). Cryptography. Encyclopedia Britannica online. Retrieved from https://www.britannica.com/topic/cryptography
21. Cho, A. (2014). Quantum spy games. Science, 343, 482–283. DOI: https://doi.org/10.1126/science.343.6170.482
22. Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices (Auckland, N.Z.), 8, 305–316 https://doi.org/10.2147/MDER.S50048
23. Unite States Computer Emergency Readiness Team (2015). Vulnerability Note VU#630239: Epiphany cardio server is vulnerable to SQL and LDAP injection. Retrieved from https://www.kb.cert.org/vuls/id/630239
24. Federal Trade Commission (2015). Consumer Information; Malware. Retrieved from https://www.consumer.ftc.gov/articles/0011-malware
25. Cisco Systems, Inc. (n.d.). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved from https://www.cisco.com/c/en/us/about/security-center/virus-differences.html
26. Virus. (n.d.). In Merriam-Webster’s dictionary. Retrieved from https://www.merriam-webster.com/dictionary/virus
27. HealthITSecurity (2017). NY Computer Virus Raises Healthcare Data Security Concerns. Retrieved from https://healthitsecurity.com/news/erie-county-medical-center-continues-four-day-battle-with-virus
28. Symantec (2016). What is the difference between viruses, worms, and Trojans? Retrieved from https://support.symantec.com/en_US/article.TECH98539.html
29. Davis, J. (2017). Alaska DHSS facing potential breach after two Trojan malware attacks. Retrieved from http://www.healthcareitnews.com/news/alaska-dhss-facing-potential-breach-after-two-trojan-malware-attacks
30. Spyware. (n.d.). In Merriam-Webster’s dictionary. Retrieved from https://www.merriam-webster.com/dictionary/spyware
31. Unite States Computer Emergency Readiness Team (2009). Security Tip (ST04–016): Recognizing and avoiding spyware. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-016
32. National Institute of Standards and Technology (NIST) (2013). Glossary of key information security terms. doi: https://doi.org/10.6028/NIST.IR.729r2. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
33. Sharma, R. & Purohit, M. (2018). Emerging Cyber Threats and the Challenges Associated with them. International Research Journal of Engineering and Technology (IRJET) 05, 02. Retrieved from https://www.irjet.net/archives/V5/i2/IRJET-V5I2127.pdf
34. Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A time to act. Journal of Medical Systems, 41(7), 104. Retrieved from https://doi.org/10.1007/s10916-017-0752-1
35. US-CERT (n.d.). Incident Reporting System. Retrieved from https://www.us-cert.gov/report-phishing
36. Hummel, R. (2017). Securing Against the Most Common Vectors of Cyber Attacks. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995
37. The Federal Bureau of Investigation (2009). Spear Phishing. Retrieved from https://www.fbi.gov/news/stories/2009/april/spearphishing_040109
38. Davis, J. (2017). Hackers breach New York’s largest provider with phishing attacks. Retrieved from http://www.healthcareitnews.com/news/hackers-breach-new-yorks-largest-provider-phishing-attacks)
39. Hacker. (2016). In Butterfield, A., & Ngondi, G.(Eds.), A Dictionary of Computer Science. : Oxford University Press. Retrieved from http://www.oxfordreference.com/view/10.1093/acref/9780199688975.001.0001/acref-9780199688975-e-2283.
40. Ethical hacker (2010). In Stevenson, A., & Lindberg, C.(Eds.), New Oxford American Dictionary. : Oxford University Press. Retrieved http://www.oxfordreference.com/view/10.1093/acref/9780195392883.001.0001/m_en_us1444244.
41. Fischer, E. A. (2016). Cybersecurity Issues and Challenges: In Brief. Congressional Research Service. Retrieved from https://pdfs.semanticscholar.org/65e3/4c9bb7330fcfec378394b5d308b6a323947d.pdf
42. Goderdzishvili, N. (2010). Legal Assessment of Cyber Attacks on Georgia, Data Exchange Agency Ministry of Justice of Georgia. Retrieved from https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf
43. Winkler, I. & Hayden, L. (2005). Social engineering through human intelligence. The Information Systems Security Association Journal 6–8
44. Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., … Tippett, P (2010). 2010 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf
45. American National Standards Institute (2012). The financial impact of breached protected health information: A Business Case for

Enhanced PHI Security. Retrieved from https://webstore.ansi.org/phi/

46. Camp, L. J. (2011). Reconceptualizing the role of security user. Daedalus, 140(4), 93–107. Retrieved from https://www.mitpressjournals.org/doi/abs/10.1162/DAED_a_00117
47. Filkins, B. (2014). New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652
48. Compliance Specialists Inc. [CSeye] (2015). 5 Mistakes in Training the Workforce on Healthcare Privacy and Security. Retrieved from http://www.cseye.biz/single-post/2015/06/08/Title-of-Something-That-Happened-Place-Holder?request_appointment=1
49. Evans, M.,Maglaras, L. A., He, Y. & Janickle, H. (n.d.). Human Behaviour as an aspect of Cyber Security Assurance. Retrieved from https://arxiv.org/ftp/arxiv/papers/1601/1601.03921.pdf
50. SANS Institute (2014). Cybersecurity Professional Trends: A SANS Survey. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615
51. U.S. Bureau of Labor Statistics (2018). Information Security Analysts : Occupational Outlook Handbook. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
52. Conn, J (2017). Low pay hinders healthcare's hunt for cyber cops. Modern Healthcare. Retrieved from http://www.modernhealthcare.com/article/20170121/MAGAZINE/301219984
53. National Institute of Standards and Technology [NIST] (2017). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Retrieved from https://www.nist.gov/cyberframework/draft-version-11
54. Zorabedian, J. (2014). How malware works: Anatomy of drive-by download web attack. Retrieved from https://news.sophos.com/en-us/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/
55. Rowe, D. C., Lunt, B. M. & Ekstrom, J. J. (2011). The Role of Cyber-Security in Information Technology Education. SIGITE'11, West Point, New York, USA. DoI:https://doi.org/10.1145/2047594.2047628
56. US Department OF Homeland Security (n.d.). Software Assurance. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosheet_SoftwareAssurance.pdf
57. New Jersey Cybersecurity and Communications Integration Cell (2017). WannaCry. Retrieved from https://www.cyber.nj.gov/threat-profiles/ransomware-variants/wannacry
58. National Institute of Standard (n.d.). NVD - NVD Dashboard. Retrieved from https://nvd.nist.gov/general/nvd-dashboard
59. Morgan, S. (2015). Is Poor Software Development the Biggest Cyber Threat? Retrieved from https://www.csoonline.com/article/2978858/application-security/is-poor-software-development-the-biggest-cyber-threat.html
60. Bird, J., Johnson, E., & Kim, F. (2015). 2015 State of Application Security: Closing the Gap. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942
61. Teto, J. K., Bearden, R. & Lo, D. C. (2017). The Impact of Defensive Programming on I/O Cybersecurity Attacks retrieved from http://delivery.acm.org/10.1145/3080000/3077571/p102-teto.pdf?ip=141.225.16.235&id=3077571&acc=NO%20RULES&key=EDE12515F121C113%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1521740112_a902a525895ff5c658edb3ccef9eb07e
62. Mancilla, D., Moczygemba J., Fenton S & Biedermann, S. (2014). Chapter 11 Security for Health Information in Biedermann, S., & Fenton, S. H. (Eds.), Introduction to Healthcare Informatics. AHiMA.
63. Miliard, M. (2018). How does blockchain actually work for healthcare? Healthcare IT News April 13, 2017 Retrieved from http://www.healthcareitnews.com/author/mike-miliard
64. Miliard, M. (2018). Blockchain faces tough roadblocks in healthcare. Healthcare IT News April 13, 2017. Retrieved from http://www.healthcareitnews.com/author/mike-miliard
65. Bhuyan, S. S., Bailey-DeLeeuw, S., Wyant, D. K., & Chang, C. F. (2016). Too Much or Too Little? How Much Control Should Patients Have Over EHR Data?. Journal of Medical Systems, 40(7), 174.
66. Schwalbe, K., & Furlong, D. (2013). Healthcare project management. Schwalbe Publishing.
67. Duncan, M., Rishel, W., Kleinberg, K., & Klein, J. (2001). A common sense approach to HIPAA. GartnerGroup. Retrieved from http://alecpalmer.tripod.com/HTMLobj-211/Gartner_Report.pdf
68. Schneier, B. (2018). Schneier on Security. Retrieved from https://www.schneier.com/books/secrets_and_lies/pref.html
69. Caralli, R. A., Allen, J. H., & White, D. W. (2010). CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience. Addison-Wesley Professional.
70. Pyke, G. (2013). Risk assessment and management. In McCormick, K. and Gugerty, G., (Ed.), Healthcare Information Technology. McGraw Hill pp 589–610.
71. Carroll, R., & Norris, G. (2011). Chapter 1 enterprise risk management in healthcare - the basics in Roberta Carroll (Editor) risk management handbook for health care organizations, volume 1. John Wiley & Sons.
72. International Risk Management Institute (2018). Cyber and privacy insurance. Retrieved from https://www.irmi.com/term/insurance-definitions/cyber-and-privacy
73. Vaughan, E. J.,& Vaughan, T.M. (1995). Essentials of insurance: A risk management perspective. Wiley. pp 34–37. Retrieved from https://www.wiley.com/en-us/Essentials+of+Insurance%3A+A+Risk+Management+Perspective%2C+3rd+Edition-p-9780470128961
74. Bensaou, M., & Earl, M. (1998). The right mind-set for managing information technology. Harvard Business Review, 76(5), 118–28
75. Baker, D. (2015). Chapter 10 "Trustworthy Systems for Safe and Private Healthcare" in Saba, Virginia, and Kathleen McCormick (Eds). Essentials of nursing informatics second ed. McGraw Hill Professional.
76. American Hospital Association (2018). Top six actions to manage hospital cybersecurity risks. Retrieved from https://www.aha.org/system/files/2017-12/aha-cyber-top6.pdf
77. National Institute of Standards and Technology (2018). Cybersecurity framework. Retrieved from https://www.nist.gov/cyberframework
78. Peretti K. & Burgess C. (2018). FDA issues final cybersecurity guidance October 10, 2014. Retrieved from https://www.alston.com/-/media/files/insights/publications/2014/10/icyber-alerti-fda-issues-final-cybersecurity-guida/files/view-alert-as-pdf/fileattachment/14818fdacybersecurity.pdf

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.