Chapter

Ransomware and Academic International Medicine

Andrew C. Miller, Abbas M. Khan and Sophia Ziad

Abstract

Healthcare is among the leading industries targeted by cyber-criminals. Ransomware exploits vulnerabilities to hijack target information technology (IT) infrastructures for monetary gain. Due to the nature and value of information, access to medical information enables cyber-criminals to commit identity theft, medical fraud, and extortion, and 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. Research suggests that an individual's medical information is 20–50 times more valuable to cyber-criminals than personal financial information. As such, cyber-attacks targeting medical information are increasing 22% per year. This chapter explores the history of ransomware attacks in healthcare, ransomware types, ransom payment, healthcare vulnerabilities, implications for international health security, and means of institutional protection.

Keywords: information technology, cyber-attack, ransomware, healthcare

1. Introduction

Healthcare is among the leading industries targeted by cyber-criminals [1]. Malware, or malicious software, refers to programs designed to infiltrate computers without the users' consent, and includes threats such as viruses and ransomware. Ransomware, a version of malware, exploits vulnerabilities to hijack target information technology (IT) infrastructures for monetary gain. Health information is an attractive target for cyber-criminals, as research suggests that an individual's medical information is 20–50 times more valuable than personal financial information [1]. Access to medical information enables cyber-criminals to commit identity theft, medical fraud, and extortion, and illegally obtain controlled substances. The utility, versatility, and centralized storage of medical information, relatively weak IT security systems, and expanding use of healthcare IT (HIT) infrastructure all contribute to an increase in cyber-attacks on healthcare entities [1]. In fact, cyber-attacks targeting medical information are increasing ≥22% annually [1]. Depending on completeness, recency, and accuracy, a single patient's file may fetch hundreds to thousands of dollars on the Dark Web [2, 3]. In Australia, it has been reported that the medical card number of every citizen is for sale on the Dark Web [3]. Moreover, attack-associated costs are reported to cost $1–3.7 million USD to clean up, with an average downtime cost per attack being $141,000 USD [1, 4–6]. A study by IBM and the Ponemon Institute reported that cyber breaches in the United States (U.S.) cost up to $6.2 billion per year and that almost 90% of hospitals have reported a data breach [7].

2. Search strategy

A literature search was performed of: China National Knowledge Infrastructure (CHKD-CNKI), Cochrane CENTRAL, CINAHL, Directory of Open Access Journals (DOAJ), Embase, Korean Journal Database (KCI), Latin American and Caribbean Health Sciences Literature (LILACS), IEEE-Xplorer, information/Chinese Scientific Journals database (CSJD-VIP), Google Scholar, Magiran, PsycInfo, PubMed, Scopus, Scientific Electronic Library Online (SciELO), Scientific Information Database (SID), TÜBİTAK ULAKBİM, Research Gate, Russian Science Citation Index (RSCI), and Web of Science (WoS). Relevant bibliographies were also searched. The search terms included the U.S. National Library of Medicine MeSH terms *hospitals* and *computer security*, as well as the terms *ransomware*, *cyber security*, *web security*, and *healthcare*.

3. What is ransomware?

Ransomware utilizes malicious software to infiltrate computer systems or connected devices to encrypt a user's files in order to carry out an extortion attack [8, 9]. Most commonly, ransomware infects a system when its user opens a compromised e-mail or visits a compromised website (i.e., drive-by downloads) [8]. Once downloaded, servers (i.e., web and e-mail), databases, end-user computers and removable media may become involved, including personal cloud storage services [2, 9]. The intended purpose of encryption is privacy, where someone with access to the encrypted data ("ciphertext") is unable to discern its contents in a readable form ("plaintext") [9]. There are two types of encryption, or cryptography: symmetric key and public key. In symmetric key cryptography, the sender and receiver use the same secret key to encrypt and decrypt the data. Public key cryptography uses a pair of keys: a public key (shared between both parties) and a private key (sender and receiver have their own unique private key) [9].

Ransomware uses a hybrid encryption system that combines the two cryptographies to create an asymmetrical cryptosystem in which data are encrypted using a randomly generated symmetric key, which is subsequently encrypted using a public key where one party has the corresponding private key [9]. The cyber-criminal uses the private key to decrypt the symmetric key in order to decrypt the data back into "plaintext" and sends the key back to the victim, who can then use it to regain access to their system [9].

Once encrypted, information becomes indecipherable and inaccessible. The user receives a pop-up notification demanding payment of a ransom (usually in untraceable digital currency such as bitcoin) in exchange for the decryption key [10]. Ransomware often does not destroy data, but rather, locks-up the data until a ransom is paid [11]. Even if the ransomware infection is removed, the data may remain encrypted [11]. But it is important to note, the mere infection of a machine with ransomware is not enough. The ransomware must communicate with a server to get an encryption key and report its results [11]. This requires a server hosted by a company that will ignore the illegal activity and guarantee the attackers anonymity (called Bulletproof Hosting) [11]. These companies are often located in China or Russia [11]. Attackers also use a proxy or virtual private network (VPN) services to further disguise their own internet protocol (IP) addresses [11]. Attack numbers have grown in part because malware authors have adopted an easy-to-use modular design of ransomware distribution [12]. This Ransomware-as-a-Service (RaaS) approach has become increasingly available, assisting technically naive attackers through simplistic distribution with phishing and exploitation kits, while employing a trustworthy business model [12]. RaaS is most easily accessed on the Dark Web [13], where prospective cyber-criminals are provided access to an affiliate console allowing them to walk-through the process of receiving their ransomware exploit kit, configure settings, target selection, and selecting ransom rates [13]. Metrics on malware instillations and success rates are also available [13].

3.1 Ransomware types

Ransomware can be divided into three basic types: crypto-, locker-, and wipe-ransomware (**Table 1**). Although crypto- and locker-ransomware represent the two main categories, current variants often incorporate traits from both [8]. Crypto-ransomware (most common) encrypts both files and data [11]. Thus, infected files remain inaccessible if transferred to another device [11]. Critical system files are typically spared, enabling the device to continue functioning, as it may be needed to pay the ransom [11]. Additionally, crypto-ransomware prefers bitcoin due to the increased privacy of cryptocurrency. However, owing to worries over law enforcement, bitcoin anonymizers and laundering services have emerged.

Conversely, locker-ransomware (a less effective extortion tool) locks the device by creating a digital "locker" around the computer system to block access [8, 11]. However, unlike crypto-ransomware, the data stored on the device are typically untouched and can often be recovered by moving it to another functioning computer for access [11]. Moreover, users may be able to remove the locker-ransomware remotely and avoid paying the ransom [8]. However, if remote malware removal is unsuccessful, ransom payments are typically made through payment voucher systems or cryptocurrency [8]. For example, online betting services may accept the

Ransomware Type	Examples	Characteristics	Data recoverable by moving files to another device?
Crypto-	Cryptolocker Cryptowall CTB-Locker KeRanger[a] Locky Petya Santana TeslaCrypt TorrentLocker WannaCry	Encrypts files and data. Typically, does not target critical system files, thereby allowing the device to function as it may be needed to pay the ransom	No
Locker-	Reveton	Creates a digital locker around the computer system to block user's access. The data on the device are typically untouched	Possibly
Wipe-	PetrWrap	Encrypts files and data. Does not unlock files or device after ransom payment	No

[a] *Believed to be the first piece of ransomware to successfully infect Mac computers (running OS X).*

Table 1.
Ransomware types and characteristics.

voucher codes as payment, subsequently transferring the money to prepaid debit cards [11]. Money mules are then used to withdraw the cash.

Wipe-ransomware first appeared in 2017 with the PetrWrap attack that encrypted the target's master file table (MFT) forcing the operating system (OS) to reboot [14]. Unlike crypto- and locker-ransomware, the files encrypted by wipe-ransomware do not unlock it after payment, effectively resulting in data loss [14].

3.2 Ransom payment

Before 2005, online payment methods were less readily available. Victims were instructed to pay ransoms by sending checks to offshore accounts, SMS text messages, prepaid cards, or even premium rate telephone numbers that earned money for the attacker [11, 15]. However, these methods were risky since they were traceable. In 2008, the largely anonymous cryptocurrency bitcoin came into use, facilitating expansion of ransomware attacks [11]. The use of third-party holdings companies such as PayPal has provided additional payment avenues [15].

Since one's ability to pay may vary greatly by geography and local economy, ransomware uses dynamic geographical pricing. Once a computer or system is infected, the ransomware establishes contact with its command-and-control (C&C) server, reports the infected device's IP address, and the C&C server returns a price for the country associated with that IP address based on a pre-populated database [11]. Additionally, criminals more frequently target businesses than individual users owing to greater potential for ransom extraction. It has been reported that about $10,000 USD may be the optimal business ransom as it is both low enough to pay, and low enough to generate reluctance on the part of law enforcement to investigate [11].

The decision whether to pay the ransom is critical. The U.S. Federal Bureau of Investigation (FBI) does not recommend paying ransoms, as only 50% of victims ultimately regain access to uncorrupted usable data. Further, ransom payment incentivizes attackers to continue exploiting healthcare targets [16]. Even so, an estimated 40% of organizations choose to pay the ransom in hopes of recovering data accessibility and mitigating further losses [17]. This may be more likely to occur if the hospital has a questionable backup and no business continuity [13].

Choosing not to pay, however, comes with the added costs of extended down-time and recovery, which may approach 23 times the ransom cost [6, 18]. Smaller organizations have been forced to close after not paying the ransom [19]. The FBI estimated that in 2016 alone, ransomware-associated monetary losses exceeded $1 billion USD, with an average downtime cost per attack of $141,000 [4–6]. Ultimately, the decision of whether to pay the ransom is an individual one and depends on the unique circumstances and stakes of every incident.

4. Ransomware and healthcare

The targeting of healthcare by ransomware dates to 1989, when the Harvard-trained evolutionary biologist Dr. Joseph L. Popp used malware to prey on scientists and organizations interested in early acquired immunodeficiency syndrome (AIDS) research [1, 11]. Dr. Joseph Popp, a World Health Organization (WHO) consultant and AIDS researcher himself, mailed 20,000 floppy disks containing ransomware to a group of attendees at the WHO's International AIDS conference [1, 11]. When inserted into the target's computer, the virus (known as *AIDS Program*, *AIDS Trojan*, or *PC Cyborg*) infected the computer with a virus that lay dormant until the 90th time the system was re-booted, at which point a note would appear on the screen asking for licensing fees to be paid while it encrypted and locked computer files [8, 12]. A $189 USD ransom to be mailed to a physical mailing address was demanded to "renew the software," or users must forgo further use of their computer [1, 8]. Although authorities apprehended Dr. Popp, his creation resulted in many derivatives that serve as a framework for modern cyber-criminals [1].

Over 15 years passed before the next instance of ransomware (GPCoder), which was delivered via e-mail [15]. Among the first major medical centers attacked was Hollywood Presbyterian Medical Center (2016), a 400-bed hospital in Los Angeles, California [1, 10, 11]. Rather than pay the initial $3.7 million USD ransom, the hospital reverted to paper records until they were able to negotiate the decryption key ransom payment down to 40 bitcoins (about $17,000 USD) [1, 10, 11]. 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. Subsequent U.S. attacks have included academic, government, and private healthcare systems including: Alaska Department of Health Office of Children's Services (Anchorage, Alaska); Appalachian Regional Hospitals (Lexington, Kentucky); Berkshire Health Systems (Pittsfield, Massachusetts); Emory Healthcare (Atlanta, Georgia); Hancock Regional Hospital (Greenfield, Indiana); Heritage Valley Health System (Pennsylvania); Medstar (Baltimore, Maryland); Kansas Heart Hospital (Wichita, Kansas); Keck Medicine of the University of Southern California (Los Angeles, California); Los Angeles Health Department (Los Angeles, California); Methodist Hospital (Henderson, Kentucky); National Capital Poison Center (Washington, D.C.); Princeton Community Hospital (Princeton, West Virginia); J.W. Ruby Memorial Hospital of West Virginia University (Morgantwown, West Virgina); University of Buffalo and State University of New York (Buffalo, New York); and Verity Medical Foundation (San Jose, California) [9, 10, 12, 20, 21]. Additionally, health insurance companies have also been targeted [7]. The Anthem Blue Cross insurance company (USA) had over 78 million medical records stolen in 2015 [7].

This problem, however, is far from constrained to U.S. entities; it is global. On May 12, 2017, a ransomware (WannaCry) that utilized a stolen National Security Agency (NSA) tool that highlighted a vulnerability of the Windows OS (MS17-010) infected more than 300,000 computers in at least 150 countries [12]. Sixty trusts within the United Kingdom's National Health Service (NHS) experienced system-wide lockouts forcing at least 16 hospital closures, ambulance diversions, inability to access patient records, patient care delays (canceled appointments and elective surgeries), and function loss in connected devices such as MRI scanners and blood storage refrigerators [3, 21–23]. Five hospitals, including Barts Health (Royal London Hospital), one of the main trauma centers in London, had to close their emergency departments [7]. Similarly, the Singapore Health System experienced a breach of over 1 million patient records, including those of the Prime Minister [7].

4.1 Why is healthcare vulnerable?

The rise in healthcare attacks in the U.S. may be linked to the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 [24]. This identified healthcare organizations as potential cash cows for cyber-criminals. Prior to 2008, only 9.4% of hospitals had adopted a basic electronic health records (EHR) system [8]. By 2014, 75.5% of hospitals had adopted basic EHRs [8], and now approximately 95% use them [12]. Additionally, HIT including glucose meters, infusion pumps, and implanted medical devices are also connected to, and dependent on, the hospital's network [12]. Moreover, healthcare systems are twice as likely to have Flash (Adobe Inc., San Jose, USA) installed and three times as likely to have Java (Sun Microsystems, Santa Clara, USA) installed, two plugins that can be exploited by hackers [8]. Healthcare organizations have been focused on healthcare, not cyber security, thus several issues have increased their vulnerability over time. While aiming to improve care efficiency, increasingly connected technology allowing for multiple ways to connect to easily accessible medical devices increases the likelihood of a breach [3]. Also, the interface between HIT systems and mobile general-purpose consumer devices (e.g., smart phones) increases the challenge to protect PHI. Moreover, no U.S. federal or state law requires encryption for PHI. Though encryption is encouraged, and often incentivized, nothing requires covered entities to utilize even the minimum standard of encryption [8]. Lastly, cyber-security funding is lacking, contributing to time lags between breech occurrence and detection [3].

Importantly, not all ransomware- and malware-generated traffic patterns are distinguishable from the normal traffic patterns generated by medical devices and systems with networking capabilities [21]. In this sense, both a malware encrypting a shared folder and an application compressing the same files have similar traffic patterns. Moreover, normal changes in the clinical environment may be misinterpreted as attacks if detection mechanisms adapt improperly [21]. Furthermore, malware developers are increasingly using encrypted traffic to avoid payload inspection [21]. Thus, achieving an acceptable balance between detection and false alarm rates remains challenging. A high false alarm rate may frustrate administrators and users, whereas a low detection rate may herald inefficacy.

Despite the growth of new technologies, many healthcare organizations persist in using legacy systems. For example, the use of Window XP (not supported since 2014) by some facilities allowed WannaCry to avoid detection [3]. Additionally, the proprietary nature of medical device software may prevent HIT teams from accessing internal device software, resulting in reliance on manufacturers to design and maintain effective device security [3]. Facilities in low- and middle-income countries (LMIC) may be at added risk owing to their use of open-source EMRs whose security may not be rigorously maintained.

Lastly, outsourcing may play a role in healthcare organization vulnerability. Health insurance niche software and service vendors are offering outsourcing as a remedy for organizational cost controls [9]. However, offshore outsourcing companies are mostly self-regulated [9]. There is currently no standard as to how a healthcare provider may ensure that offshore business associates are adequately protecting the electronic PHI of their patients.

4.2 Implications of international health security

With the dominance of ransomware as a leading cyber-security threat, it is important to consider its impact on International Health Security (IHS) [25]. Many countries lack the legal infrastructure to prosecute such crimes. Globally, cyber-attacks may result in substantial loss of resources, money, and life [26]. Although many security threats have emerged from LMIRs, many of these regions lag behind higher income regions in implementation of automated technologies and EMRs in the medical sector. That said, the IHS community is actively endeavoring to increase the availability and use of these technologies in LMIRs [27]. Thus, with falling costs and rising availability and implementation, HIT security will have an increasingly important role in IHS in upcoming years.

Traditional charting and management methodologies are steadily being replaced with digital ones. Technologies including digital algorithms and artificial intelligence are increasingly being used to monitor and coordinate threat responses [28, 29]. The IHS community has come to increasingly rely upon digital global surveillance networks such as the ProMED-mail (PMM) Network and the World Health

Dimension	Role	Recommendation
Leadership		• Establish a Board-Level Information Technology (IT) Committee • Hire a Chief Information Security Officer (CIO) • IT security should be under the control of executives with extensive IT experience (e.g., CIO)
Physical safeguards	Prevention and preparation	• Buildings and equipment access to protect against unauthorized access and theft
Hardware and software	Prevention and preparation	• Encrypt sensitive practice data • Perform regular back-ups. Store 1 copy off-line • Consider tools such as ShieldFS© or Redemption to create real-time safe-guarded copies of attacked files • Maintain a “gold image” of system configurations; this allows one to reset systems to the pre-attack state • Test backup’s restore function regularly (e.g., quarterly or yearly) • Patch management for operating system, application software, browsers, plug-ins, firmware, and anti-virus software • Make sure the firewall is properly configured • Segment the network by categorizing IT assets (e.g., desktops, servers, routers), data, and personnel into groups, and restricting access to these groups using entry and exit traffic filtering
	Incident Response	• Disconnect the infected computers from the network • Turn off wireless network functionality of the infected machine • If widespread, shut down all network operations to prevent further spread
Clinical content	Intrusion detection	• “Whitelist” or allow only specified programs to run, while blocking all others, to prevent malicious executables from running • Web and e-mail filtering: Block messages with attachments *.exe, *.zip, *.rar, *.7z, *.js, *.wsf, *.docm, *.xlsm, *.pptm, *.rtf, *.msi, *.bat, *.com, *.cmd, *.hta, *.scr, *.pif, *.reg, *.vbs, *.cpl, and *.jar from suspicious sources
User interface	Education	• Legitimate messages should have a telephone number someone can call (i.e., out of band check), and a personal e-mail address that has a legitimate username that people can check in their local directory; e-mail and website links should display complete internet address (URL) to build trust
	Prevention and preparation	• Use a virtual private network (VPN) to create a secure connection, even on a public unsecured network • Establishing strict processes of removable media to prevent ransomware brought into the closed network
	Intrusion detection	• At the first sign of an alarm message, turn off the computer and report the incident to the IT support team immediately

Dimension	Role	Recommendation
People	Education	• Do not follow unsolicited Web links in e-mails • Train users on ransomware prevention strategies, how to identify malicious e-mails, and to avoid clicking on potentially weaponized attachments
	Identity and access management	• Restrict users' administrative privileges on local desktops and laptops. For users who require administrative access, configure two accounts, one with administrative privileges that is used only when necessary, and one with more restrictive privileges that they use for routine activities, including reading e-mail and browsing the Internet • Restrict the ability of users to "write" (i.e., create and delete files), on shared drives of departmental or group shares • Establish policies and processes for protection of HIT systems in smart working environment using cloud computing and teleworking
Workflow and communication	Intrusion detection	• Scan all software downloaded from the internet prior to executing
	Risk assessment	• Conduct simulated attacks to raise user's awareness • Conduct mock system recovery exercises • Conduct regular risk assessments and auditing
	Identity and access	• Dual-factor authentication • More stringent version of the Unique User Identification Standard to prevent generic usernames and passwords
	Incident response	• System-wide password reset following a successful attack
Internal policies, procedures and environment		• Based on risk and business impact assessments, identify applications and data based on importance to the business (e.g., Tier 0—essential for business operations; Tier 1—1 hour downtime acceptable; Tier 2—1 day downtime acceptable; Tier 3—1 week downtime acceptable)Develop a plan to manage a ransomware situation accordingly • Utilize the principle of "Least Privilege" to limit users' access to only those systems and services required by their job
External rules and regulations	Preparation	• Develop a Health Insurance Portability and Accountability Act (HIPPA)-compliant information security regimen
	Incident response	• Contact your organization's insurance provider, a computer forensics expert, and the FBI in the event of a successful attack
Measurement and monitoring		• Monitor network activity to identify suspicious activity • Monitor the external environment for security incidents and address gaps and deficiencies as they are identified • Review any extended downtime (e.g., ransomware) to identify potential root causes, and discuss future prevention or mitigating procedures

HIT = health information technology.

Table 2.
An approach to preventing or mitigating ransomware attacks.

Organizations (WHO) Global Outbreak Alert & Response Network (GOARN); systems that help organizations improve coordination speed and response time to temper the impact of international infectious disease outbreaks [30–32]. These systems are often used by IHS networks and volunteers in the field and, if compromised, could become a portal of entry for cyber-attack [31]. The attacks on the United Kingdom's NHS demonstrate that even large state-sponsored institutions are not immune to cyber-attack [33].

Laboratory security is another important aspect for IHS, as the use and storage of sensitive pathogens make them attractive targets for attacks [33]. For this reason, the Global Health Security Agenda (GHSA) was created to help increase investment in global health security. GHSA is a 67-nation effort that hopes to increase the availability of laboratory systems for IHS use [34, 35].

5. Protecting your institution

As with most HIT issues, preventing a ransomware attack is a complex sociotechnical problem. Richard Schaeffer (2009), the U.S. National Security Agency (NSA) Information Assurance Director, testified to the U.S. Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security that 80% of all ransomware attacks could be prevented by adhering to security measures already in place [36]. In addition to a sophisticated encryption algorithm, ransomware attacks often rely on some form of "social engineering," or the psychological manipulation of people to gain their trust and lead them to divulge confidential information [15]. Solving these problems is a shared task between HIT users and those responsible for configuring, maintaining, and operating the HIT infrastructure. While preventing all ransomware attacks is not possible, there are several steps that healthcare organizations can take to reduce risk and mitigate harm (**Table 2**). Additionally, the U.S. Department Health and Human Services (HHS) offer guidelines on the best policies on how to properly secure electronic PHI. The need to maintain software updates and patches cannot be understated. For example, Microsoft Inc. had released a patch for the vulnerability exploited by WannaCry and NotPeyta 8 weeks before the attack [8]. If systems had remained up to date, the impact of both malwares would likely have been significantly diminished.

Another approach to recover from a ransomware attack without needing to pay a ransom is by copying a file when it is being modified, storing one copy in a protected area, and allowing any changes to be made to the other [14]. ShieldFS© (NECSTLab, Milan, Italy) approaches this by creating a protected (i.e., read-only) copy of files when a process requests to modify or delete it [14]. If ShieldFS© determines that a process is malicious, the offending process is suspended and the copies can be restored, replacing the modified (encrypted) versions [14]. Conversely, Redemption uses a similar approach, but its technique creates a copy of each of the files targeted by the ransomware and then uses the Windows Kernel Development framework to redirect (or "reflect") the write requests or filesystem operations (invoked by the ransomware to encrypt the target files) from the target files to the dummy copies in a transparent data buffer, hence leaving the original files intact [14].

Lastly, any ransomware attack should immediately be reported to the appropriate authorities [37]. In the U.S., federal law dictates that any breach undergo a thorough and properly documented analysis to determine if any unsecured PHI was compromised [38–40]. For anything other than a low probability of PHI compromise, one must inform the U.S. Department of HHS as soon as possible, and no later than 60-days post-breach (when over 500 person's PHI is affected) [10, 37, 41].

6. Conclusions

As HIT infrastructure struggles with new technology and security protocols, the industry is a prime target for medical information theft. Even worse, the healthcare industry is lagging behind other leading industries in securing vital data. Healthcare organizations must adapt to the ever-changing cyber-security trends and threats, such as ransomware, where critical infrastructure is exploited, and valuable patient data are extracted. It is imperative that time and funding are invested in maintaining and ensuring the protection of healthcare technology and the confidentially of patient information from unauthorized access.

Conflict of interest

The authors have no conflict of interests to disclose.

Author details

Andrew C. Miller[1,2]*, Abbas M. Khan[2] and Sophia Ziad[3]

1 Department of Emergency Medicine, East Carolina University Brody School of Medicine, Greenville, NC, USA

2 The MORZAK Collaborative, Columbia, MD, USA

3 Department of Mathematics and Statistics, University of Maryland Baltimore County, Baltimore, MD, USA

*Address all correspondence to: Taqwa1@gmail.com

References

[1] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017;**25**(1):1-10. DOI: 10.3233/THC-161263

[2] Chernyshev M, Zeadally S, Baig Z. Healthcare data breaches: Implications for digital forensic readiness. Journal of Medical Systems. 2018;**43**(1):7. DOI: 10.1007/s10916-018-1123-2

[3] Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018;**113**:48-52. DOI: 10.1016/j.maturitas.2018.04.008

[4] Spence N, Bhardwaj N, Paul DP, Coustasse A. Ransomware in healthcare facilities: A harbinger of the future? Perspectives in Health Information Management. 2018:**15**(Summer):1-22

[5] Cook S. 2017-2019 Ransomware statistics and facts. Comparitech [Internet]. 2019. Available from: https://www.comparitech.com/antivirus/ransomware-statistics/ [Accessed: 18 November 2017]

[6] Sussman B. Ransomware: Hackers Are Raising Their Prices. SecureWorld [Internet]. 2019. Available from: https://www.secureworldexpo.com/industry-news/ransomware-hackers-raising-prices [Accessed: 25 November 2019]

[7] Ghafur S, Kristensen S, Honeyford K, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digital Medicine. 2019;**2**:98. DOI: 10.1038/s41746-019-0161-6

[8] Slayton TB. Ransomware: The virus attacking the healthcare industry. The Journal of Legal Medicine. 2018;**38**:287-311. DOI: 10.1080/01947648.2018.1473186

[9] Krisby RM. Health care held ransom: Modifications to data breach security and the future of health care privacy protection. Health Matrix. 2018;**28**:365-401

[10] Pope J. Ransomware: Minimizing the risks. Innovations in Clinical Neuroscience. 2016;**13**(11-12):37-40

[11] Richardson R, North MM. Ransomware: Evolution, mitigation and prevention. International Journal of Management Reviews. 2017;**13**(1):10-21

[12] Branch LE, Eller WS, Bias TK, et al. Trends in malware attacks against United States healthcare organizations, 2016-2017. Global Biosecurity. 2019;**1**:15. DOI: 10.31646/gbio.7

[13] Kelpsas B, Nelson A. Ransomware in hospitals: What providers will inevitably face when attacked. The Journal of Medical Practice Management. 2016;**32**:67-70

[14] Hull G, John H, Arief B. Ransomware deployment methods and analysis: Views from a predictive model and human responses. Crime Science. 2019;**8**:1-22. DOI: 10.1186/s40163-019-0097-9

[15] Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from Ransomware attacks. Applied Clinical Informatics. 2016;**7**(2):624-632. DOI: 10.4338/ACI-2016-04-SOA-0064

[16] Federal Bureau of Investigation, U.S. Department of Justice. Cyber Crime [Internet]. 2019 Available from: https://www.fbi.gov/investigate/cyber/ [Accessed: 17 November 2019]

[17] Harley D. Ransomware: To Pay or Not to Pay? WeLiveSecurity [Internet]. 2016. Available from: https://www.welivesecurity.com/2016/08/22/

ransomware-pay-not-pay-2/ [Accessed: 01 May 2020]

[18] Pelley S. How cybercriminals hold data hostage … and why the best solution is often paying a ransom. CBS News 60 minutes [Internet]. 2019. Available from: https://www.cbsnews.com/news/ransomware-how-cybercriminals-hold-data-hostage-why-the-best-solution-is-often-paying-a-ransom-60-minutes-2019-08-25/ [Accessed: 18 November 2019]

[19] Sussman B. Doctors quitting due to ransomware attacks. SecureWorld [Internet]. 2019. Available from: https://www.secureworldexpo.com/industry-news/are-doctors-quitting-after-ransomware-attacks [Accessed: 17 November 2019]

[20] Zhao JY, Kessler EG, Yu J, Jalal K, Cooper CA, Brewer JJ, et al. Impact of trauma hospital Ransomware attack on surgical residency training. The Journal of Surgical Research. 2018;**232**:389-397. DOI: 10.1016/j.jss.2018.06.072

[21] Fernández Maimó L, Huertas Celdrán A, Perales Gómez ÁL, García Clemente FJ, Weimer J, Lee I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors. 2019;**19**(5):E1114. DOI: 10.3390/s19051114

[22] Collier R. NHS ransomware attack spreads worldwide. Canadian Medical Association Journal. 2017;**189**(22):E786-E787. DOI: 10.3390/s19051114

[23] Cohen IG, Hoffman S, Adashi EY. Your money or your Patient's life? Ransomware and electronic health records. Annals of Internal Medicine. 2017;**167**(8):587-588. DOI: 10.7326/M17-1312

[24] Charles D, Gabriel M, Searcy T. ONC Data Brief No 23. Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008-2014. The Office of the National Coorrdinator for Health Information Techonology, U.S. Department of Health and Human Services. 2015. Available from: https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf [Accessed: 02 February 2020]

[25] Park R. ISTR Insights Special Report: Ransomware and Business 2016. Symantec Connect [Internet]. 2016. Available from: https://www.symantec.com/connect/blogs/istr-insights-special-report-ransomware-and-business-2016 [Accessed: 01 May 2020]

[26] Bambery Z, Cassell CH, Bunnell RE, Roy K, Ahmed Z, Payne RL, et al. Impact of a hypothetical infectious disease outbreak on US exports and export-based jobs. Health Security. 2018;**16**(1):1-7. DOI: 10.1089/hs.2017.0052

[27] Thompson R, Perache AH. Optimism Meets Realism: The Politics of Technology Innovation in Global Health Security. Chatham House: The Royal Institute of International Affairs [Internet]. 2018. Available from: https://medium.com/chatham-house/optimism-meets-realism-the-politics-of-technology-innovation-in-global-health-security-54c82ad4aa89 [Accessed: 01 May 2020]

[28] Eckmanns T, Füller H, Roberts SL. Digital epidemiology and global health security; an interdisciplinary conversation. Life Sciences, Society and Policy. 2019;**15**(1):2. DOI: 10.1186/s40504-019-0091-8

[29] Simao MBG, Heymann DL, Sampath R, Kunii O, Koshiba M, Jones C, Hughes S. Harnessing New Technologies for Global Health Security. Chatham House: The Royal Institute of International Affairs [Internet]. 2018.

Available from: https://chathamhouse.soutron.net/Portal/Default/en-GB/RecordView/Index/181928 [Accessed: 01 May 2020]

[30] Institute of Medicine (US) Forum on Microbial Threats. Global Infectious Disease Surveillance and Detection: Assessing the Challenges. Washington D.C.: National Academies Press; 2007

[31] Mackenzie JS, Drury P, Arthur RR, Ryan MJ, Grein T, Slattery R, et al. The global outbreak alert and response network. Global Public Health. 2014;**9**(9):1023-1039. DOI: 10.1080/17441692.2014.951870

[32] Roberts SL, Elbe S. Catching the flu: Syndromic surveillance, algorithmic governmentality and global health security. Security Dialogue. 2017;**48**(1):46-62. DOI: 10.1177/0967010616666443

[33] Macintyre CR, Engells TE, Scotch M, Heslop DJ, Gumel AB, et al. Converging and emerging threats to health security. Environment Systems and Decisions. 2018;**38**:198-207. DOI: 10.1007/s10669-017-9667-0

[34] Osterholm MT. Global Health security—An unfinished journey. Emerging Infectious Diseases. 2017;**23**(13):S225-S227. DOI: 10.3201/eid2313.171528

[35] Global Health Security Agenda [Internet]. 2019. Available from: https://ghsagenda.org/ [Accessed: 01 May 2020]

[36] Zetter K. Senate panel: 80 percent of cyber attacks preventable. WIRED [Internet] 2009. Available from: https://www.wired.com/2009/11/cyber-attacks-preventable/ [Accessed: 02 February 2020]

[37] Office for Civil Rights. My entity just experienced a cyber-attack! What do we do now? U.S. Department of Health and Human Services [Internet]. 2017. Available at: https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf [Accessed: 01 May 2020]

[38] Healthcare for Ransom: A Look into the HIPAA Guidelines for Ransomware Incidents. Trend Micro™ [Internet]. 2016. Available at: https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/healthcare-for-ransom-a-look-into-the-hipaa-guidelines-for-ransomware-incidents [Accessed: 01 May 2020]

[39] Snell E. Breach notification center of presence health HIPAA settlement. Health IT Secur [Internet]. 2017. Available from: https://healthitsecurity.com/news/breach-notification-center-of-presence-health-hipaa-settlement [Accessed: 18 November 2019]

[40] United States Government Interagency Guidance Document, FACT SHEET: Ransomware and HIPAA. U.S. Department of Health and Human Services [Internet]. 2016. Available from: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf [Accessed: 01 May 2020]

[41] Office of Civil Rights. Submitting notice of a breach to the secretary. U.S. Department of Health and Human Services [Internet]. 2015. Available from: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html [Accessed: 18 November 2019]