ESSAI

Volume 17 Article 10

Spring 2019

Insecure

Michelle Apreza
College of DuPage

Insecure

by Michelle Apreza

(English 1102)

The term "hacked" is a very broad term, when referring to a system that was infiltrated for a purpose. IT professionals use the phrase "data breach" when referring to an event where stolen information was taken by those to whom it is not supposed to be available. The topic of cybersecurity is essential in the 21st century considering how much insecure technology is around. When a device is insecure, it means that there are code sections that prevent a program from working more fluently and/or efficiently. Hackers target these vulnerabilities.[1] Cybersecurity seeks to control availability. The World Wide Web is not the same as the Internet; it is actually a global telecommunications system that connects small networks. Everything that runs on a program is connected to it.[2] If any information is given to the wrong person, this can lead to identity theft, terrorism, invasion of privacy, even death.

No company or person is immune from data breaches, but when it comes to susceptibility, the healthcare industry is at the top of the list.[3] Some industries are stronger than others when it comes to data security; this is because they spend more time and money on controlling information availability. However, the health sector is just the absolute worst when it comes to cybersecurity. Why do healthcare data breaches happen so frequently, and what can be done?

The fact that the healthcare industry is the most vulnerable to data breaches at first does not make any sense, because the information such organizations or facilities contain is critical. Kristen Heald, who holds a Juris Doctor Degree (J.D.) from the University of Maryland Francis King Carey School of Law, informs the reader in her most significant piece of legal writing from 2017, "Why the Insurance Industry Cannot Protect Against Health Care Data Breaches," that most organizations have the Commercial General Liability (CGL) policy, which protects businesses from "liability . . . claims of . . . advertising and personal injury liability," property damage, and physical injury (p. 283). It is the least expensive and recently, the Court found an exception in the CGL policy; in *Zurich American Insurance v. Sony Corp. of America* (2014), the Court found out that "CGL policy requires the policyholder to actually commit the act," and since the hackers were not associated with Sony, Sony "did not qualify for coverage" (p. 285). Because the CGL policy provides no coverage against other parties, medical institutes would have to pay for protection against cyber threats.[4] To make matters more complex, cybersecurity insurance companies claimed that they would offer "reduced premiums . . . if they [healthcare] take steps to decrease the extent of . . . liability," because data breaches are unpredictable, as are the financial losses following them, therefore, making it difficult for companies to settle on a fair price[5] (p. 286). It was estimated that a medical facility would need as much as "$1 billion in cyber insurance to protect its assets," but would be "unable to secure more than $300 million" (p. 287). Associations are forced to choose between insurance and investment in cybersecurity; both are very expensive. It seems that most would rather pay for an inefficient insurance policy. That lack of cybersecurity funding makes it easy for hackers to infiltrate healthcare systems.

Another weakness of this industry is the framework. The frequency of data breaches has exposed how low in quality are the safeguards in the medical field. In clinics and hospitals, their reason for failing is that they concentrate on providing services other than security of patient information.[6] Glyn Cashwell is another J.D. from the University of Maryland Francis King Carey School of Law, along with a master's in Electrical and Computer Engineering from the Johns

Hopkins University, as well as a Certificate in Cyber and Crisis Management. In his 2018 article, "Cyber-Vulnerabilities & Public Health Emergency Response," he discovered that another vulnerability in medical facilities is workers' own devices that "connect to their network containing PHI [Protected Health Information] to provide patient care" (p. 32). More and more personally-owned devices keep on being added to these settings, creating more opportunities for cybercriminals. Unfortunately, IT departments cannot regulate information on these devices due to privacy laws. Additionally, they can easily be hacked because malware, or bugs/viruses, may already be embedded in their systems.

Attempts to regulate the frequency of attacks are evident in Acts passed by Congress and the Office of the President to regulate cybersecurity, which does not actually correspond to effectiveness.[7] It is essential to note that all medical providers, insurance companies, and clearinghouses, have different cybersecurity requirements. The common ground is the most important and effective act: the Health Insurance Portability and Accountability Act (HIPAA) specifies what data should be private, and dictates the "administrative, physical, and technical safeguards" that should be fulfilled (Cashwell, 2018, p. 37). Obviously, the security rule is the issue. The requirements for that section are flexible, to allow entities to determine if certain steps are "'reasonable and appropriate'" (p. 38). If not, it also provides alternatives. Cashwell highlights that the flexibility is actually a drawback, because "[o]ut of the eighteen . . . safeguards, only six are required" (p. 38). Most importantly, he discovered that security advocates are placing more emphasis on the fact that "covered entities" are so focused on "ensuring they are HIPAA-compliant" that they have a deficiency of resources and funds that "implement other security controls," which could lead to safeguards more "effective against medical identity theft" (p. 39). Cashwell concludes that, although HIPPA is helpful and the most influential in past legal order, it is not sufficient when "cyber risks" are considered (p. 39).

Another Act influenced by HIPAA that is somewhat effective is the Cybersecurity Act of 2015. This allows the Department of Homeland Security to gain access to information from a private sector, not including PHI. All healthcare and non-healthcare administrations are required "'to use technical means to scrub [PHI] . . . before it is transferred" (Cashwell, 2018, p. 42). The only risk with this, is that businesses may not separate PHI from other information, giving the government a chance to track individuals. Concerning healthcare, data of any kind, besides PHI, is to be shared across the industry, benefitting small providers. In addition, it mandates the Department of Health and Human Services (HHS) to create cybersecurity guidelines for healthcare providers and insurers, as well as their business associates. The Act also defines cybersecurity positions and obligations of each HHS department. This task force identifies "common cyber-threats in the health care sector" as well as "incorporate best practices from other industries" (p. 43). The two flaws with this Act are that first, it does not recommend specific hardware or software to follow their guidelines, and second, it contains vocabulary only technical workers would understand.

Also influenced by HIPAA is Executive Order 13010 and 13636, which resulted in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. According to Cashwell (2018), it is a "good first step in identifying . . . standards for defensive cybersecurity measures" (p. 45). Another outcome was the DHS Cybersecurity Evaluation Tool, which helps "an organization develop a security plan and identify vulnerabilities" for free (p. 45). Cashwell also located the flaw with it; it does not suggest "specific technical security solutions" (p. 46).

The last (somewhat-effective) Act is the Presidential Policy Directive (PPD) 8 and 21, which requires the existence of a list of cybersecurity threats to critical infrastructure. From this, the Strategic National Risk Assessment (SNRA) was born, and its duty is to determine which threats pose massive risks as well as provide "preparation, response, mitigation, and recovery recommendations" for said threats (Cashwell, 2018, p. 46). The list only gives tips on before and

after a data breach. Considering the frequency of data breaches in the medical field, the list is not very effective. Also, from a hacker's perspective it is logical never to pick the same target twice. Cashwell reviews plenty of other Acts, and in every one of them, he analyzed and revealed that they do not contribute much - or at - all to cybersecurity in healthcare.

Cybersecurity in the healthcare insurance sector can be highly improved. The first action in any healthcare setting is to increase funding. This can be done in multiple forms, but the most efficient is for officials to convince Congress to support cybersecurity in the healthcare industry. Jay P. Kesan, a professor from the University of Illinois in association with the Critical Infrastructure Resilience Institute (CIRI) and DHS S&T Center of Excellence, and Carol M. Hayes, a research associate, also from U of I and associate of the CIRI, joined forces to discover methods that could improve cybersecurity in any industry. In their 2017 article, "Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment," Kesan and Hayes claim that "establishing standards . . . before a crisis can mitigate the worst" of a data breach, therefore, it is one reason why "NIST's Cybersecurity Framework is important" (p. 217). Glyn Cashwell (2018) also supported this idea. Kesan and Hayes know that "cybersecurity policy requires cooperation between the government and . . . private sector" (p. 217). With insurance, companies and people act more carelessly, increasing risk. There is nothing anyone can do about that; it is human nature, but insurance is still needed. Kesan and Hayes analyzed 146 legal cases such as *RSVT Holdings, LLC v. Main Street America Assurance Co*. (2011), *Travelers Indemnity Co. v. Portal Healthcare Solutions, LLC* (2016), and *Apache Corp. v. Great American Insurance Co*. (2016). Kesan and Hayes concluded that the necessity for "insurance products directed at specifically covering cyber risk and harms" is a great deal (p. 268). Instead of focusing on preventing data breaches, cybersecurity insurances should focus on the recovery after an event. It is not feasible trying to predict what will happen and when. Kesan and Hayes also recommend that, in order for the insurance industry to create balance with companies, they could "impose the kind of Best Available Control Technology standards" (p. 268).

Researchers in the improvement of cybersecurity often start from scratch and try to come up with a completely new system, but the key is to look at existing systems. Cybercriminals target systems that are difficult to improve, so nothing can be done directly by healthcare.[8] A professional programmer prepares the program not "if" a data breach occurs, but "when" it occurs. Hiroshi Yamamoto and Hiroshi Ishii, from the Tokai University School of Information and Telecommunication Engineering, teamed up with Yusuke Hiraide from Hitatchi, Ltd., Tokyo, Japan, to determine a "quantitative measure for the amount of information that is leaked during a [web] search" (Yamamoto et al., 2017, p. 2495). In their experiment, they searched on the web for "apples" and "oranges," and it resulted in the anticipated search result. The number of results brings the attacker closer to the search result. Yamamoto et al. (2017) decided to use Private Information Retrieval, which is a "secure search scheme using plain text" to find the number of results, without leaking information about the searched phrase (p. 2496).

Using the Shannon Entropy equation to "quantify the ambiguity" of the search phrase, Yamamoto et al. concluded that the leaked information is equal to 100log37-log$n$ - meaning that, "[i]f one half of all . . . possible" phrases are searched, "the leaked information to the search engine in 1 bit" (Yamamoto et al., 2017, p. 2500). Because data breaches are inevitable and perfect privacy is not possible, the goal was (and is) to always protect a certain amount of privacy. Healthcare encryptions are weak enough that it might not even make a difference to leave PHI in plain text, although HIPPA requires PHI to be encrypted. Replacing a search string with encrypted PHI, means that, if 16 bits or 2 bytes are stolen, then 2 characters are stolen. 8 bits equals 1 byte, which is equal to 1 letter or small number. Considering how small a byte is and how much time hackers have, with the "lag of . . . response [ranging] from 14 to 57 s" (p. 2504), the healthcare industry loses a lot of information in a few seconds. Yamamoto et al.'s experiment supports the fact that instead of focusing on the defense of quality of information, cybersecurity must focus on the quantity because it can be

controlled. In addition, Kesan and Hayes analyzed a study similar to that conducted by Yamamoto et al.'s and concluded, with the same results.

Now it can be concluded that technical cybersecurity is important, and only the quantity of data cybercriminals obtain can be regulated to a certain degree because data breaches will always happen. There are a multitude of ways to regulate availability and username and password are the most common. Nicole Hennig is a user experience professional with skills in every software aspect in emerging technologies, and in her 2018 article "Chapter 2: Security," she provides information on the best way to secure any information, which is limited. Hennig warns that it is extremely easy for "internet traffic to be viewed by hackers" using public wi-fi in order to find usernames and passwords that would benefit the "'man-in-the-middle'" (p. 12). Facilities where anyone can walk in probably have a public wi-fi server, so it's best not to have those servers connected to the system containing PHI. She also points out that a virtual private network (VPN) secures a server for the user and can be downloaded by any portable device (p. 12), which can actually fix the issue concerning personal devices in hospitals and clinics. To control how much data is stolen, "[s]afetly [backed] up" servers, which contain data, "on a regular basis" and having multiple servers with enhanced encryption spreads out data and reduces availability to hackers.

Speaking of availability, certain officials can access that data by adding two-factor authentication. A common method is security questions after establishing username and password. Henning (2018) suggests a numeric code be sent by text message or email to the individual trying to access data, because it is a "one-time use code" and a "new code is needed each time" (p. 14). By this method, only certain individuals with access to a physical device or certain email can access PHI, unless the attacker has that information too. An interesting point also the author points out is that using mobile payments like Google Pay, Apple Pay, and Samsung Pay, is more secure than the physical credit or debit card (p. 15). Even though it may take a while and may be painful, the only way to pay for services could be by mobile. Biometrics is another method, but there is also a risk of a threat obtaining bio information physically. "[M]onitoring . . . accounts on a regular basis" (p. 18) can decrease the financial burden following a data breach. Because the healthcare industry focuses more on providing services, they should focus on checking on their security every once in a while, because they do not realize when a data breach has occurred until months later.

Another (and more complicated) manner to reduce the amount of data stolen is by improving encryption; however, it is only something an IT professional or computer scientist can deal with. Ever since the technology boom in the 2000s, people have increasingly become interested in computer science and cryptography. Therefore, making it more difficult to protect data because many decryption algorithms could be uncovered using techniques taught in computer science curriculum. That information is now made public because it is not as effective anymore. Research in the area is essential for the encryption of PHI to improve.

Although the healthcare industry is extremely behind in cybersecurity, it is never too late to return to the modern world. The lack of cybersecurity insurance and legal standards are the only issues that make the healthcare industry more prone to data breaches. If advocates could shift their focus on improving cyberinsurance and raising cybersecurity standards, the frequency of data breaches could be lessened in only a few years. Even if certain people do not have insurance of any kind, cybersecurity is an important topic in the 21st century because technology is *everywhere*; therefore, the enhancement of cybersecurity is everyone's business, considering how much data in on the internet and the various webs.

Notes

1. What hackers actually do is look at sections of code, find an insecurity (section of code that prevents the program from completely working fluently without the risks), copy, and paste it throughout the rest of the code. These repeated strings are called "bugs."
2. There are three sections to the internet. The "surface web" contains Google, Bing, Wikipedia, and other websites that could give all of the information on it, to anyone. The "deep web," contains legal documents, scientific reports, medical records, social media, autonomous programs (for cars, medical equipment, factory machines, etc.) and so on. The dark web contains hitmen for hire, drug and human trafficking, child pornography, illegal information, private communications, human products, and so on. I do not encourage anyone in any way to go looking into this part of the Internet.
3. For more information on industries most susceptible to data breaches, please see https://www.cimcor.com/blog/five-industries-in-greatest-danger-of-a-data-breach
4. For the purposes of this paper, I will not go into the debate about flaws of Article III Standing, which deals with the "injury-of-fact." The individual suing an organization or person must prove that s/he was injured, which easily makes it hard for those whose personal information was electronically stolen or manipulated.
5. This can be visually summarized in Figure 1 of Kesan and Hayes (2017). Strengthening cybersecurity with cyberinsurance markets and better risk assessment. *Minnesota Law Review*, *102*(1), 191–276. Retrieved from https://cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=126903120&site=ehost-live&scope=site.
6. The source of this detail is not readily available.
7. Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Cybersecurity Act of 2015, Health Information Technology: Certification Criteria for Health Information Technology (provides accreditation standards for Electronic Health Records), and Cybersecurity Enhancement Act of 2014.
8. The two vulnerabilities that are extremely difficult to secure are the power grid and telecommunications infrastructure (TI). The TI transports sensitive information, which can directly provide the infiltrator information directly. Also, it depends on electricity, hence the power grid can be targeted. See Cashwell, G. (2018). Cyber-vulnerabilities & public health emergency response. *Journal of Health Care Law & Policy*, *21*(1), 29–57. Retrieved from https://cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=133142545&site=ehost-live&scope=site.

References

Cashwell, G. (2018). "Cyber-vulnerabilities & public health emergency response." *Journal of Health Care Law & Policy*, *21*(1), 29–57. Retrieved from https://cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=133142545&site=ehost-live&scope=site

Heald, K. (2017). "Why the insurance industry cannot protect against health care data breaches." *Journal of Health Care Law & Policy*, *19*(2), 275–298. Retrieved from https://cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=126275158&site=ehost-live&scope=site

Hennig, N. (2018). Chapter 2: Security. *Library Technology Reports*, *54*(3), 8–21. Retrieved from https://cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=128707557&site=ehost-live&scope=site

Kesan, J. P., & Hayes, C. M. (2017). "Strengthening cybersecurity with cyberinsurance markets and better risk assessment." *Minnesota Law Review*, *102*(1), 191–276. Retrieved from https://cod.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=126903120&site=ehost-live&scope=site

Yamamoto, H., Ishii, H., & Hiraide, Y. (2017). "A quantitative measure of the information leaked from queries to search engines and a scheme to reduce it." *Journal of Supercomputing*, *73*(6), 2494–2505. https://doi.org/10.1007/s11227-016-1942-1