The John Marshall Journal of Information Technology & Privacy Law

Volume 32 | Issue 3 Article 1

Spring 2016

Health Information and Data Security Safeguards, 32 J. Marshall J. Info. Tech. & Privacy L. 133 (2016)

Jane Kim

David Zakson

Follow this and additional works at: https://repository.law.uic.edu/jitpl

 Part of the Computer Law Commons, Consumer Protection Law Commons, Criminal Law Commons, Health Law and Policy Commons, Internet Law Commons, Law and Society Commons, Medical Jurisprudence Commons, Privacy Law Commons, Science and Technology Law Commons, and the Torts Commons

Recommended Citation

Jane Kim & David Zakson, Health Information and Data Security Safeguards, 32 J. Marshall J. Info. Tech. & Privacy L. 133 (2016)

https://repository.law.uic.edu/jitpl/vol32/iss3/1

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

ARTICLES

HEALTH INFORMATION AND DATA SECURITY SAFEGUARDS

JANE KIM & DAVID ZAKSON*

ABSTRACT

The healthcare industry possesses information coveted by cyber criminals. Unfortunately, healthcare providers are also among the most vulnerable and unprepared to deal with cyber attacks. The Introduction sets the background of this paper with cyber security statistics of the healthcare sector. Part A of this paper will discuss how new Russian law impacts global data security. Part B takes a broad look at data security safeguards. Part C focuses on U.S. attempts at safeguarding data through NIST and its Presidential Policy Directive. In Part D, the paper explores in greater detail causes that precipitate security breaches and specific security defenses that may be implemented. Lastly, Part E examines compliance programs that are essential in detecting, preventing or, at least, minimizing security threats and hacks, further obviating individual responsibility of corporate officers for breaches.

---

* Jane Kim is a law partner at KYZ Law P.C. focusing on healthcare, regulatory and compliance matters, also including litigation. Ms. Kim has handled matters at all levels of federal and state court systems. She has received her undergraduate degree at The School of the Art Institute of Chicago, J.D. degree at John Marshal Law School of Chicago and an LL.M. in Health Law with a Certificate in Healthcare Compliance at Loyola University Chicago School of Law. My gratitude goes to the Journal's Editorial Board, with particular thanks to Mirko Akrap and Ryan Tunney, as well as to my husband, lawyer and author, Young Kim, for providing valuable suggestions to my written work, always with a smile.

David Zakson is a Chief Security Architect of Tenneco and formerly the Security Architect of Motorola Solutions. He is solely responsible for the opinions expressed in this article, which in no way represent his employer's positions, views, or strategies.

INTRODUCTION

Today, cyber criminals recognize that a treasure trove of confidential and protected information is found not within financial institutions but within the healthcare industry. In addition to financial information, medical institutions hold information on valuable IP, health records, and sensitive research.[1] Health records sell for up to 20 times more than credit card information on the black market.[2] A "full identity 'Kitz'," a complete medical record, coupled with health and financial information, can demand up to $1,300 per person.[3] Cyber criminals salivate over such financial healthcare data rewards.

It is disconcerting that although "healthcare organizations manage a treasure trove of financially lucrative personal information [, they] [...] do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect patient data."[4] The FBI has warned the healthcare industry that the "IT systems and medical devices [of healthcare providers] were at risk for increased attacks from hackers due to lax cyber security standards and practices."[5]

And the statistics speak for themselves:

> A recent study by the Ponemon Institute found that 91 percent of healthcare organizations have suffered at least one data breach in the past two years, 39 percent have experienced two to five data breaches, and 40 percent have suffered more than five. Still, the study found, half of all healthcare organizations have little or no confidence that they have the ability to detect all patient data loss or theft, and more than half don't believe their incident response process has adequate

---

1. Christine R. Couvillon, *It's (Not) Academic: Cybersecurity Is a Must for Universities and Academic Medical Centers*, THE NATIONAL LAW REVIEW, (November 23, 2015), http://www.natlawreview.com/article/it-s-not-academic-cybersecurity-must-universities-and-academic-medical-centers#sthash.s9holOIJ.dpuf.

2. Caroline Humer and Jim Finkle, *Your medical record is worth more to hackers than your credit card,* REUTERS (September 24, 2014), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924#c2IUK2WcQ5xypa3D.97.

3. Jeanine Skowronski, *What your information is worth on the black market,* BANKRATE, (July 27, 2015) http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx#ixzz3tklgL6E6.

4. Jeff Goldman, *91 Percent of Healthcare Organizations Suffered Data Breaches in the Past Two Years,* (May 12, 2015), http://www.esecurityplanet.com/network-security/91-percent-of-healthcare-organizations-suffered-data-breaches-in-the-past-two-years.html (hereinafter *91 Percent*).

5. Gabriel Perna, *After the Community Health Systems Incident, FBI Issues Another Hacking Warning to Healthcare*, HEALTHCARE INFORMATICS (August 25, 2014), http://www.healthcare-informatics.com/news-item/after-community-health-systems-incident-fbi-issues-another-hacking-warning-healthcare.

funding and resources.[6]

According to one study, "data breaches could be costing the healthcare industry as much as $6 billion per year."[7] The likelihood of breaches reverberates throughout the healthcare industry which affects how patients receive care; over 10% of patients tend to withhold relevant medical information from their doctors for fear of it being re-disclosed to unauthorized persons.[8]

The healthcare industry can strengthen its data security through two avenues simultaneously: (a) a risk-based approach through NIST and Formal Security Frameworks, which set priorities based on the probability of exploitation and impact on business; and (b) a compliance-based approach to train, monitor, audit, remedy, and importantly, ensure that the responsible corporate officers are engaged and are not held individually responsible (turning a blind-eye is no longer an acceptable excuse[9]) for breaches.

Therefore, Compliance Officers and other responsible corporate officers need to be at least familiar with how data works and what it takes to protect it in order to make proper decisions in such regard. A responsible corporate officer cannot merely rely on cyber or data breach insurance to protect their entities' wallets (not data) from data hacks on a rainy day.[10]

A. RUSSIAN LAW'S IMPACT ON GLOBAL DATA

By the end of 2016, half of the sensitive data of Global 1000 companies will be in the Cloud,[11] but this does not literally mean there is an actual, data storing cloud somewhere. The Cloud is a term of art, and data in the Cloud is located somewhere at a physical location, similar to

---

6. Jeff Goldman, *Data Breach at UCLA Health Exposes 4.5 Million People's Personal Information,* (July 21, 2015), http://www.esecurityplanet.com/network-security/data-breach-at-ucla-health-exposes-4.5-million-peoples-personal-information.html (hereinafter *Data Breach at UCLA*).

7. *91 Percent*, *supra* note 4.

8. Sara Peters, *90% Of Industries, Not Just Healthcare, Have Disclosed PHI In Breaches* (December 2015), http://www.darkreading.com/analytics/90--of-industries-not-just-healthcare-have-disclosed-phi-in-breaches/d/d-id/1323535.

9. *See generally* DEPARTMENT OF JUSTICE, MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, SALLY QUILLIAN YATES (Sept. 9, 2015).

10. Lena J. Weiner, *Cybersecurity Insurance Basics for Healthcare Organizations,* HEALTHLEADERS MEDIA (June 8, 2015), http://healthleadersmedia.com/content.cfm?content_id=317181&page=1&topic=TEC; Christine Marciano, *How much does Cyber/Data Breach Insurance Cost?*, DATA BREACH INSURANCE (Feb. 1, 2016), http://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/.

11. Goran Čandrlić, *How Cloud Computing Works?,* GLOBALDOTS (February 26, 2013), http://www.globaldots.com/how-cloud-works/.

a hard drive in a computer, and likely not located in the United States. How much control and access large corporations have to data located on the servers that corporations maintain is an ongoing debate.

There is also a distinction between information and data. "Data itself has no meaning, but becomes information when it is interpreted."[12] In other words, data is what computers use, and information is what humans use; information gives meaning and context to data.[13] Experts estimate that by 2017, "1.4 zettabytes of data will be flowing over global networks, meaning that the majority of data will be in motion and remain in motion as it traverses clouds."[14]

Exacerbating cyber security matters, data traverses over, and is stored in, foreign jurisdictions exposing it to a higher degree of theft. Some countries have begun to address the issue of protecting the data of its citizens through laws specifying that servers must be physically located within the borders of their country. In such regard, decision makers should understand how doing business in a globalized market affects data security, zeroing in on safeguarding data within their own organizations.

Russia has taken the position that information of their citizens is best protected if it resides on servers that are physically located in Russia.[15] Consequently, the Russian government has taken steps to protect its citizens' information, promulgating Federal Law 242-FZ, which went into effect September 1, 2015.[16] Anyone who collects data on Russian citizens, including foreign corporations, must have servers located in Russia.[17] As a result, all data, data in motion, and data at rest will reside in Russia, including data of foreign companies that may contain some confidential and proprietary information unrelated to Russian citizens.

Healthcare entities should not ignore the new Russian data law when they contemplate doing business in Russia or, for instance, when they collaborate with medical researchers from Russia. Not only must corporate decision-makers implement an effective policy and compliance

---

12. DICTIONARY.COM, http://dictionary.reference.com/help/faq/language/d58.html.

13. Martin Doyle, *What is the Difference Between Data and Information?*, DQ GLOBAL(August 6, 2014) http://www.business2community.com/strategy/difference-data-information-0967136#skV7H4ZFqU9UWOTm.99.

14. Frank Ohlhorst, *Encryption is front-line defense for data at rest,* TECHREPUBLIC (July 3, 2014, 1:00 AM), http://www.techrepublic.com/article/encryption-is-front-line-defense-for-data-at-rest/.

15. *New Russian law prohibits citizens' personal data being held on foreign servers,* CROWN WORLDWIDE GROUP (August 7, 2015), https://www.crownworldwide.com/en-us/article/new-russian-law-prohibits-citizens--personal-data-being-held-on-foreign-servers.

16. *Id.*

17. *Id.*

plan specifically addressing doing business in a high-risk country with the Foreign Corrupt Practices Act (FCPA), but they must also be cognizant of the technological ramifications for doing business with Russia as such business decisions are being made. Responsible corporate officers cannot be ignorant of the intersection of technology and the law while promoting and growing their business.

B. BACKGROUND, DATA SECURITY SAFEGUARDS

"The use of 'Big Data' in health care promises to fundamentally change the way we provide, measure, and pay for health care."[18] We are entering the age of mobile health and "wearables" that communicate with health records and disrupt the health care business model as we know it. The conundrum is to balance the rising use of cutting edge internet-based applications with their inherent risks and vulnerabilities to hacks.

Some lessons learned for safeguarding information may be traced back thousands of years ago. For instance, in warfare, a well-orchestrated offense almost always forces capitulation of defensive mechanisms or safeguards. The list of great physical safeguards caving back targeted attacks is endless and may find its roots from the Bible with the Gates of Jericho that fell to the Hebrews, Masada falling to the Romans, the Great Wall of China falling to the Mongols, the Maginot Line falling to the Germans, and the Mannerheim Line falling to the Soviets.[19] 1,300 ft cliffs (pre-airplanes), 13ft high casemate walls, tremendous thickness of five-foot concrete walls were ultimately not sufficient to withstand purposeful, targeted attacks.

Fast-forward to the 21st century, we have the likes of Kevin Mitnick who can pass a set of stringent, layered security controls similar to those defined by NIST SP 800-53[20] to obtain G.W. Bush's Texas driver's license information, hack into your cell phone and extract your social security number and home address in 30 seconds, and monitor the FBI

---

18. Kristen Rosati, *Top Ten Health Law Issues,* Big Data in Health Care*,* AHLA CONNECTIONS (February 2015), *available at* www.polsinelli.com/~/media/.../Rosati_AHLA_December2013.

19. An isolated example of a defensive wall having withstood the attacks is the Königstein Fortress in Germany. It is 1,800 meters long with walls up to 42 meters high and steep sandstone faces, still stands today mainly unscathed. *Germany - Elbtal From Festung Koenigstein,* FINEARTAMERICA, fineartamerica.com/featured/germany--elbtal-from-festung-koenigstein-christine-till.html (accessed on Feb. 17, 2016).

20. *See* SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, JOINT TASK FORCE TRANSFORMATION INITIATIVE, NIST SPECIAL PUB. NO. 800-53 (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (NIST 800-53 document is an umbrella document defining "Security and Privacy Controls for Federal Organizations).

who was monitoring him at the time.[21] This is not the stuff of sci-fi movies anymore; this is reality.

Defensive mechanisms in security applications are nothing more than Masada-like fortifications; eventually they, too, will fall to a well-orchestrated, highly intelligent, targeted cyber attack. Unsurprisingly, 80% of security executives in North America do not believe conventional network security solutions are sufficient to protect their companies' computing environments.[22]

According to the Department of Health and Human Services, more than 120 million people have been compromised in more than 1,110 separate breaches since 2009 – a third of the U.S. population. […] 'These data breaches are symptomatic of a failure of healthcare organizations to invest in preventative measures, such as threat isolation[.]'[23]

A closer look reveals that the primary source for the breaches is theft of unencrypted laptop computers.[24] Therefore, the majority of breaches are preventable at very low cost. There has been a shift in breaches in the healthcare industry, however, "'[w]hile employee negligence and lost/stolen devices continue to be primary causes of data breaches, *criminal attacks* are now the number one cause' […] One third of respondents don't even have an incident response process in place."[25]

C. PRESIDENTIAL POLICY DIRECTIVE AND NIST

Presidential Policy Directive/PPD-21 (Presidential Directive) attempts to address security vulnerabilities in sectors affecting the public and "establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure" sectors.[26]

The Presidential Directive establishes 16 critical infrastructure sec-

---

21. Jonathan Littman, *The Invisible Digital Man,* PLAYBOY, 64 (June 2007), *available at* https://dl.dropboxusercontent.com/u/4689551/kevin-mitnick.pdf.

22. James Bourne, *Four in five execs think conventional security is not enough for cloud environments,* CLOUDTECH (July 1, 2015; 11:11 AM), http://www.cloudcomputing-news.net/news/2015/jul/01/four-five-execs-think-conventional-security-not-enough-cloud-environments/.

23. *Data Breach at UCLA*, *supra* note 6.

24. *Breaches Affecting 500 or More Individuals*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

25. *91 Percent*, *supra* note 4 (Emphasis added).

26. Press Release, The White House, Office of the Press Secretary, Presidential Policy Directive -- Critical Infrastructure Security and Resilience (Feb. 12, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

tors including the Healthcare and Public Health Sector (HPH Sector).[27] The HPH Sector states that "[b]ecause the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure."[28]

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce, which provides security standards and configurations to the 16 sectors under the Presidential Directive.[29] Compliance-based NIST through the National Infrastructure Protection Plan (NIPP)[30] provides guidelines for maximum-security settings in accordance with NIST benchmarks for any equipment storing and transmitting confidential data (e.g., cellular phones, computers, servers), commencing with risk analysis and management and ending with the intricate details of encryption algorithms.[31]

The NIST issued An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.[32] Centers for Medicare and Medicaid (CMS) mentions the NIST documents as potentially helpful guidance but not mandatory for compliance with the HIPAA Security Rule.[33]

Unless an entity is fully compliant with NIST, however, the U.S. government has a right to refuse to do business with, or provide federal funds to, the entity. The Presidential Directive and compliance with its NIST guidelines may directly influence how the government spends Medicare/Medicaid funds. The U.S. government has considerable leverage with healthcare providers through its Medicare/Medicaid funds.

---

27. U.S. Dept. of Homeland Security, Critical Infrastructure Sectors, http://www.dhs.gov/critical-infrastructure-sectors.

28. U.S. Dept. of Homeland Security, Healthcare and Public Health Sector, www.dhs.gov/healthcare-and-public-health-sector.

29. *See National Institute of Standards and Technology*, http://nist.gov (stating that the NIST, "write[s] model laws, distribute[s] uniform standards, and provide[s] training for inspectors, which result[s] in a more orderly and fair marketplace."

30. NIPP framework process identifies the following: "(1) Identify Assets, Systems, Networks, and Functions; (2) Assess Risks; (3) Prioritize Infrastructure; (4) Develop and Implement Protective Programs and Resilience Strategies; (5) Measure Effectiveness; (6) Continue Research and Development; (7) Continue Partnership Model; (8) Identify Information-Sharing Products." *Healthcare and Public Health Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Department of Health and Human Services, 43-44 (2010), *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf (numeration added).

31. *NIST Special Publications*, NIST (Jan. 28, 2016), http://csrc.nist.gov/publications/PubsSPs.html#800-53.

32. Matthew Scholl, et. al., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST (Oct. 2008) http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf

33. HIPAA Security Rule, 68 Fed. Reg. 34, 8346-8355 (February 20, 2003).

Consider that in 2014, the U.S. government allocated 23% of the $3.5 trillion federal budget to Medicare and Medicaid programs, with $597 billion allocated to Medicare[34] and $475 billion allocated to Medicaid.[35]

Although NIST guidelines are mere guidelines and are not mandatory for much of the healthcare sector, they should certainly not be overlooked. The HPH Sector-Specific Plan touts the doubling of the number of security site audits at medical countermeasure facilities.[36] Should the government place higher emphasis on the healthcare industry meeting NIST specifications, it could certainly utilize the Presidential Directive as a threat and another vehicle to exclude entities/individuals from federal health program participation for non-compliance.

Curiously, there are no laws or regulations mandating specific safeguards for e-data within the healthcare industry. The Presidential Directive and the HITECH Act's provisions are not mandatory and are mere "guidance" as well.

D. DEFENSE IN DEPTH AND BUILDING SECURITY FORTIFICATIONS

The U.S. government acknowledges that, "[a] breakdown in the healthcare infrastructure would result in a significant impact on the economy, a loss of human life, and a breakdown in other critical sectors."[37] To manage this risk, Federal Sentencing Guidelines require that: "the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [...] to reduce the risk of criminal conduct identified through this process."[38] However, it is up to each organization to design its own robust and effective programs to assess risks.

Cyber risks are ubiquitous and to mitigate those risks requires the deployment of multiple layers of information protection, commonly known as "defense-in-depth," placed throughout the information technology (IT) system. One of those layers with high impact on the quality of Information Protection is encryption. Encryption "means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[39] "A covered entity may be in compliance with the Security

---

34. *The Facts on Medicare Spending and Financing*, THE HENRY J. KAISER FAMILY FOUNDATION (July 24, 2015), http://kff.org/medicare/fact-sheet/medicare-spending-and-financing-fact-sheet/.

35. Total Medicaid Spending, THE HENRY J. KAISER FAMILY FOUNDATION (2016) http://kff.org/medicaid/state-indicator/total-medicaid-spending/.

36. *Healthcare and Public Health*, *supra* note 30 at i.

37. *Id.*

38. U.S. SENTENCING COMMISSION, 2011 FEDERAL SENTENCING GUIDELINES MANUAL, ch.8, http://www.ussc.gov/guidelines-manual/2011/2011-chapter8.

39. 45 C.F.R. § 164.304.

Rule even if it reasonably decides *not* to encrypt electronic protected health information (PHI) and instead uses a comparable method to safeguard the information."[40] To date, there is no comparable method to encrypt PHI data in motion except for the tokenization method,[41] which is currently being explored within the healthcare industry. Ultimately, it may prove insufficient to address the multiple layers of protection required for PHI data.[42] Consequently, at the present time, encryption of data should be implemented to prevent possible breaches as part of defense in depth strategy.

a. Defense In Depth

In a *Defense In Depth* approach, encryption mechanisms apply as follows: the hard drive (HD) encryption, file encryption, transparent database encryption, field level database encryption, transport protocol encryption, encrypt data in RAM (Random Access Memory), encrypt some aspects of data at rest, encrypt data in motion and encrypt data in use. Each layer is designed to protect information from a particular type of attack. For instance, disk encryption is designed to protect information on a laptop/mobile device from physical theft of that device, and RAM encryption is designed to protect from "memory dumps" and accesses to memory from other applications. However, even such encryption may not guarantee adequate protection anymore, in that a seven-dollar "can of compressed air used upside down will cryogenically freeze memory and keep the data intact for several minutes to an hour. This means the ultrasensitive encryption keys used to protect data can be exposed in the clear."[43]

U.S. regulations do not mandate encryption, although security experts agree that, "encryption is front-line defense for data at rest"[44] and data in motion. However, "data in use" must be brought back to "clear text" and cannot be encrypted. Moreover, if given sufficient resources almost any encryption can be defeated. On the other hand, most data hacks can be prevented through proper encryption and a well-maintained Risk Management program. In other words, if a strong de-

---

40. *Federal Register, Vol. 74, No. 162*, 42741, National Archives and Records Administration (Aug. 24, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf (Emphasis added).

41. *Tokenization (data security),* WIKIPEDIA (last modified January 15, 2016), https://en.wikipedia.org/wiki/Tokenization_(data_security).

42. *See generally Tokenization, What's Next After PCI?,* RSA, *available at* http://www.slideshare.net/emcacademics/tokenization-whats-next-after-pci (last accessed on Feb. 17, 2016).

43. George Ou, *Cryogenically frozen RAM bypasses all disk encryption methods,* ZD NET (Feb. 21, 2008), http://www.zdnet.com/article/cryogenically-frozen-ram-bypasses-all-disk-encryption-methods/.

44. Ohlhorst, *supra* note 14.

fensive mechanism is implemented, it may delay the attacker's success and may channel the hacker toward an easier target.

The approach to building security fortifications should consist of two inquiries. Answers to these inquiries will help determine the financial scope of the security project and gauge the extent of protection necessary based on risk of loss analysis.

Inquiry 1: *What* are you trying to protect? In other words, have information classification levels been assigned? Has a Business Impact Analysis been conducted to understand actual value of the data? How many data sources have to be monitored, maintained and protected?

Inquiry 2- *From whom* are you trying to protect this information? Of note here, some statistical knowledge is useful- most hacks (70%) may be happening from within the organization and may be malicious or non-malicious compromises.[45] Malicious hacks may be caused by disgruntled employees, unscrupulous competition or commercial spies.[46] A "non-malicious" insider may be a person making an honest mistake based on lack of awareness, eager to perform work quickly or perhaps falling victim to social engineering.[47]

b. Common hacks

Many successful attacks from the outside come in by way of e-mails or money extortions called "business e-mail compromise" where the hackers pose as top officers of companies and request employees to hand over confidential financial information.[48] Somehow these requests work so well that the FBI has reported that hackers "have funneled $1.2 billion out of companies' accounts" in the last two years.[49] Hollywood Presbyterian Medical Center from California is the first victim within the health industry to report a "business e-mail compromise" hack paying to hackers $17,000 in ransom.[50]

---

45. *TrendMicro- Simply Security* (September 2012) http://blog.trendmicro.com/most-data-security-threats-are-internal-forrester-says/(noting that most data security threats are internal).

46. Roger A. Grimes, Your guide to the seven types of malicious hackers, INFOWORLD (Feb 8, 2011) http://www.infoworld.com/article/2623407/hacking/your-guide-to-the-seven-types-of-malicious-hackers.html.

47. "Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter." *Social engineering*, SEARCH SECURITY, *available at* gauss.ececs.uc.edu/Courses/c6056/pdf/social-engineering-main.pdf.

48. David Goldman, *Hackers stole $1.2 billion from 7,000 businesses in 2 years*, CNN MONEY (Aug. 18, 2015), money.cnn.com/2015/08/28/technology/hackers-fbi/index.html?iid=ob_article_hotListpool&iid=obinsite.

49. *Id.*

50. Laura Wegner, LA Hospital Pays Hackers Nearly $17,000 To Restore Computer Network (February 17, 2016) http://www.npr.org/sections/thetwo-

The following is an example of the most common hack:

> A fictitious Acme Company had all its data encrypted in the database; Acme Company asks Mary Joe Peoples to run a statistical analysis report. Mary accesses the data, does whatever it is she ought to do in the Excel program and saves the data onto her laptop. Her laptop is not encrypted and from that point forward the data is free game for anyone who needs by using one of many standard hacks.

There are cost-effective cyber security programs available; most hacks and breaches may be prevented with limited funds, including the Acme Company hack example above, which could have been easily prevented if Mary's computer was either encrypted or Mary understood through effective compliance training that she should never save anything to a personal, unencrypted device.

c. Advanced persistent threat

Another example is the UCLA's recent two hacks that occurred within a 10-month period. The most recent hack was in July 2015 and may have occurred because a laptop did not appear to be encrypted but merely contained a password.[51] It is almost a trivial task to compromise a password. An adversary is capable of up to one trillion guesses per second to crack a password.[52] Alternatively, having physical access to the device, passwords can simply be erased or, in some instances, replaced with a password known to the attacker.

Additionally, UCLA may have become a victim of an advanced persistent threat (APT). A hacker may infiltrate via a fishing e-mail or a web server vulnerability, gain a bridgehead and lay low, slowly infiltrating throughout the corporate network. Once the hacker establishes a presence, creates a backdoor, and covers his or her tracks, s/he carefully awaits an opportunity to arise. It may take months, it may even take years, but since the payout may be measured in millions of dollars, it may be well worth the wait. Since UCLA reported the first hack in October 2014 and the second data breach occurred about ten months thereafter, we can at least speculate that UCLA fell victim to an APT.

---

way/2016/02/17/467149625/la-hospital-pays-hackers-nearly-17-000-to-restore-computer-network.

51. Rajiv Leventhal, *UCLA Health System Gets Hacked Again*, HCI (September 2, 2015), http://www.healthcare-informatics.com/news-item/ucla-health-system-hacked-again. The first security breach with a malicious hack at UCLA resulted in 4,500 patient records exposed. *Data Breach at UCLA*, *supra* note 6.

52. CITIZENFOUR (HBO Documentary Films 2014).

To seek inoculation against an APT is akin to seeking a vaccine against cancer; while theoretically possible, it is currently impractical. This "helplessness" is addressed in the Federal Sentencing Guidelines for corporations, which states: "[t]he failure to prevent or detect the instant offense does not necessarily mean that the [compliance] program is not generally effective in preventing and detecting criminal conduct."[53]

d. Hacks through an electronic data interchange

Another possibility for the UCLA breach is by means of a CVS photo breach.[54] CVS is likely connected to UCLA electronic data interchange (EDI). It is entirely feasible that the hackers could have leveraged CVS's EDI to gain a foothold in UCLA's domain. Typical EDI communication is *not* encrypted, in that ANSI standards (ANSI is one of the NIST standards) provide that data is required to be in "clear text" form although it should travel over encrypted "pipe." So if a bad guy manages to inject himself on either end of this "pipe" he may get lucky and start collecting EDI information that can further his attack on other components of the UCLA infrastructure.

e. Prevention by deception

One clever approach to safeguarding data is by deception, adapting Sun Tzu's philosophy on warfare, that, "[a]ll warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[55]

For instance, a prime target for most intruders is sensitive data (e.g., PHI, PI). But envision introducing a very similar database with very similar datasets but instead, and here is the deception, the data is completely fake: fictitious names, social security numbers, sham diagnoses and treatments. This data is a decoy. An example of *possible* decoy PHI data can be found at pastebin.com. This PHI data may or may not be a decoy. The only way to know is to contact the information holder.

Importantly, the "real" data storage is hardened with security con-

---

53. 2011 FEDERAL SENTENCING, *supra* note 38.

54. Anjali Rao Koppala, *CVS Health's photo service, UCLA Health get hacked,* REUTERS (July 17, 2015), http://www.reuters.com/article/2015/07/17/us-ucla-health-cyberattack-idUSKCN0PR1ZW20150717#HGGCVi05MkWtjuad.97.

55. Eric Jackson, *Sun Tzu's 31 Best Pieces Of Leadership Advice,* FORBES (MAY 23, 2014), http://www.forbes.com/sites/ericjackson/2014/05/23/sun-tzus-33-best-pieces-of-leadership-advice/.

figurations while the decoy is effortless to acquire. The easier target will lure many intruders to compromise sham datasets. They will be enticed to believe that the final goal is near, easy to achieve, low hanging fruit, in alignment with one of Sun Tzu's postulates.[56] But instead, they hit a "honeypot,"[57] a decoy of no value, specifically setup to trap the intruders. The honeypot is also configured to record all intruders' actions to further study their behavior and, subsequently, adjust protection mechanisms of the "real" data based on what was learned from the honeypot.[58] The bad guys, of course, are progressively catching up to the existence of honeypots. As a result, the required honeypot/honey net technology's sophistication must be increased.

f. Kiosks, limiting the attack vectors

Another approach to safeguarding data is to severely restrict the functionality of electronic devices by implementing "kiosks" where users can only do a specific set of tasks. This approach minimizes attack vectors. Each device has multiple attack vectors, avenues through which an attacker can get to the data. The biggest attack vectors (78%) on a computer are an Adobe Flash Plugin, browser and Java;[59] another attack vector is e-mail. NIST gravitates toward total control approach to deployment and configuration of components.

g. Measuring effectiveness of a Security Program

Any Information System will contain unavoidable vulnerabilities. The amount and range of vulnerabilities, however, does not determine the effectiveness of a security program. Rather, it is measured by the risk remaining after compensating controls are deployed. In other words, to measure the effectiveness of a cyber security system, or to calculate risk exposure, you need to benchmark the current security posture (vulnerabilities) and account for risk or falling victim to exploitation of vulnerabilities ("Risks = Threats x Vulnerabilities x Impact / Counter Measures").[60] The lower your risk the more effective your pro-

---

56. MARTIN J. GANNON & RAJNADINI PILLAI, UNDERSTANDING GLOBAL CULTURES: METAPHORICAL JOURNEYS THROUGH 28 NATIONS, CLUSTERS OF NATIONS, AND CONTINENTS, 385 (Sage Publications, Inc., 5th ed. 2013).

57. Eric Peter and Todd Schiller, A Practical Guide to Honeypots, Sec.1.2 Honeypots (April, 15 2008), http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/#sec1.1.

58. *Id.*

59. Andra Zaharia, Is Java the Biggest Vulnerability on Your PC? A data-driven answer (July 2015) https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/; and, Stefan Frei, Thomas Dübendorfer, Gunter Ollmann, Martin May, Understanding the Web Browser Threat (July 1, 2008) http://www.technicalinfo.net/papers/UnderstandingTheWebBrowserThreat.html.

60. ecole, *Insider Threat Risk Formula: Survivability, Risk, and Threat* (October,

gram is.

Smaller and mid-size entities ("those with revenue between $50 million and $2 billion") spend, on average, $13,000 per employee on IT.[61] The key to an effective cyber security program with restricted funds is to do away with highly specialized roles of employees and retain the services of "jacks of all trades." The EU and Russia have embraced this approach. Naturally, the *formality* of the compliance program and security safeguards have to commensurate the size and financial strength of the corporation,[62] although *risks* must be addressed irrespective of a corporation's size.

E. COMPLIANCE

A compliance and ethics program is intended to "prevent and detect criminal conduct."[63] The requirements for an effective compliance and ethics program find its roots in Section 805(a)(2)(5) of the Sarbanes-Oxley Act of 2002 (SOX).[64] In 2002, in response to a series of accounting scandals involving U.S. companies, Congress enacted SOX, which strengthened the accounting requirements for public companies.[65] SOX Section 302 requires that a company's senior management take responsibility for, and certify the integrity of, their company's financial reports on a quarterly basis.[66]

SOX compliance principles have been adopted throughout other high-risk industries including health-related industries. Federal Sentencing Guidelines provide the footprint for effective compliance programs, and state that a "compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct."[67]

Compliance programs carry a two-fold purpose. First, compliance programs ensure easier adherence to complex regulations and, in some healthcare sectors, such compliance is mandated by the Patient Protection and Accountable Care Act (PPACA).[68] However, the second purpose

---

2012), https://cyber-defense.sans.org/blog/2012/10/23/insider-threat-risk-formula-survivability-risk-and-threat.

61. Megan Santosus, *How Company Size Relates to IT Spending,* (first published in 20015), http://searchcio.techtarget.com/magazineContent/How-Company-Size-Relates-to-IT-Spending.

62. 2011 FEDERAL SENTENCING, *supra* note 38.

63. *Id.*

64. *Sarbanes-Oxley Act Of 2002 - SOX*, INVESTOPEDIA, www.investopedia.com/terms/s/sarbanesoxleyact.asp (last accessed on Feb. 19, 2016).

65. *Id.*

66. *Id.*

67. 2011 FEDERAL SENTENCING, *supra* note 38.

68. Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010).

of compliance programs may be less obvious and is certainly not mandated but is very helpful whenever the government knocks on the door: it is to protect not only the corporations but the *individuals* inside the corporations, the individuals in positions to influence decisions within health-related organizations.

Individual responsibility continues to be the government's focus. The latest Yates Memo states that corporate cases should not be resolved without resolving individual cases, and the ability to charge individuals should be done without regard to that individual's ability to pay.[69] In other words, the Yates Memo makes clear that U.S. attorneys should not enter into settlements and corporate integrity agreements that would result in the dismissal of charges or immunity to individuals.[70]

But is it feasible to have a grip on what each employee is doing so as to detect and possibly prevent malicious and non-malicious hacks? Or, are the government's expectations of corporate officers in large organizations unrealistic and out of touch with reality?

The government's expectation that corporate officers know what every individual is doing within an entity may be realized through a robust and dynamic compliance and monitoring system. It may aid executives in preserving their employment, careers and reputations. Likewise, proper compliance programs will serve to protect entities from exorbitant fines and exclusions that may flow from violations or breaches, in that it should result in a lower culpability score. A Culpability Score determines the entity's fine, measures the involvement of corporate officers in, or tolerance of, criminal activity within the organization.[71]

Seven elements of an effective Compliance Plan are modeled on the federal sentencing guidelines, and include: (1) A clear commitment to compliance; (2) Appointment of a trustworthy compliance officer with a high level of responsibility; (3) Effective training and education programs; (4) Auditing and monitoring; (5) Communications; (6) Internal investigation and enforcement; and (7) Response to identified offenses and application of corrective action initiatives.[72]

The Office of Inspector General (OIG) expanded on each of the seven elements of an effective compliance plan by issuing "OIG guidance," which provides guidance to compliance officers. However, the word "guidance" coupled with the word "voluntary" is very misleading as to

---

69. DEPARTMENT OF JUSTICE, MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, SALLY QUILLIAN YATES, (Sept. 9, 2015).

70. *Id.*

71. 2011 FEDERAL SENTENCING, *supra* note 38.

72. *Federal Fraud Enforcement and Physician Compliance,* AMERICAN MEDICAL ASSOCIATION (2000).

whether such guidance has the force of law.[73] It appears that the OIG promulgated law under the rubric of "guidance," in that such compliance programs are "evidence" of complying with the law.[74] Compliance programs are "especially critical" in reimbursement and payment areas where fraud and abuse are more prevalent.[75] Financial information is one of the primary reasons why hackers target the healthcare industry. It is "incumbent" upon the health industry and corporate officers, especially, to ensure that adequate compliance programs are in place to facilitate legal conduct.[76] In crafting its guidance, the OIG sought input from various interested parties within the health sector; essentially, prior to this guidance being issued, it was open for comment as if during a rule making process.

In addition to "guidance" on compliance plans, certain federal laws mandate the institution of some policies and procedures within select types of organizations. For instance, the PPACA authorizes the HHS to require providers participating in Medicare and Medicaid programs to establish a compliance program.[77] Pursuant to HIPAA, covered entities and business associates are required to maintain certain administrative safeguards, such as the risk analysis, risk management, sanction policy and information system activity review.[78]

Although, it is required to implement administrative safeguards, having a compliance plan is largely not required under HIPAA. However, should a breach occur, a well-implemented compliance plan "provides evidence that any mistakes were inadvertent, and this evidence would be considered in determining whether a medical practice or other healthcare entity has made reasonable efforts to avoid and detect misbehavior."[79]

Finally, the Department of Justice emphasizes the distinction between whether a compliance plan is "real" or merely "paper."[80] In other words, a compliance program needs to become part of the organization's culture, embraced from the top down, and be effective.

---

73. *Id.*

74. *Id.*

75. *Federal Register, Vol. 63, No. 35*, (Feb. 23, 1998), *available at* www.hcca-info.org/.../P13-1.pdf.

76. *Id.*

77. Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010).

78. Jane Kim, *Japanese and American Privacy Laws, Comparative Analysis*, 32 J. Marshall J. Info. Tech. & Privacy L. 1 (2015)(citing HIPAA, §164.308).

79. *Federal Fraud Enforcement, supra* note 72.

80. Michael W. Peregrine, *DOJ's Important Message to Health System Leadership* (5/29/2015)(on file with author).

F. CONCLUSION

In the healthcare industry, the government mandates some kind of training on data security within certain organizations, leaving guidance on compliance programs and data security safeguards somewhat as an elective tool. Such government efforts to ensure that data (including PHI) is properly protected appear very fragmented and reactive, thus rendering such efforts ineffective. On the other hand, often overlooked within the healthcare industry, NIST provides very specific guidance on how to proactively ensure that data is protected. If such guidance is not followed, or large data hacks persist, it should not be a surprise if corporate officers are held personally responsible and, as punishment, the government seeks the exclusion of individuals and/or entities from participation in federally-funded programs (Medicare/Medicaid).

To ensure that technical safeguards are properly implemented and are working, training, monitoring and auditing this high-risk area as part of the effective compliance plan is the number one defense. Importantly, treating government guidance as law rather than mere guidance will further ensure that proper safeguards are implemented.