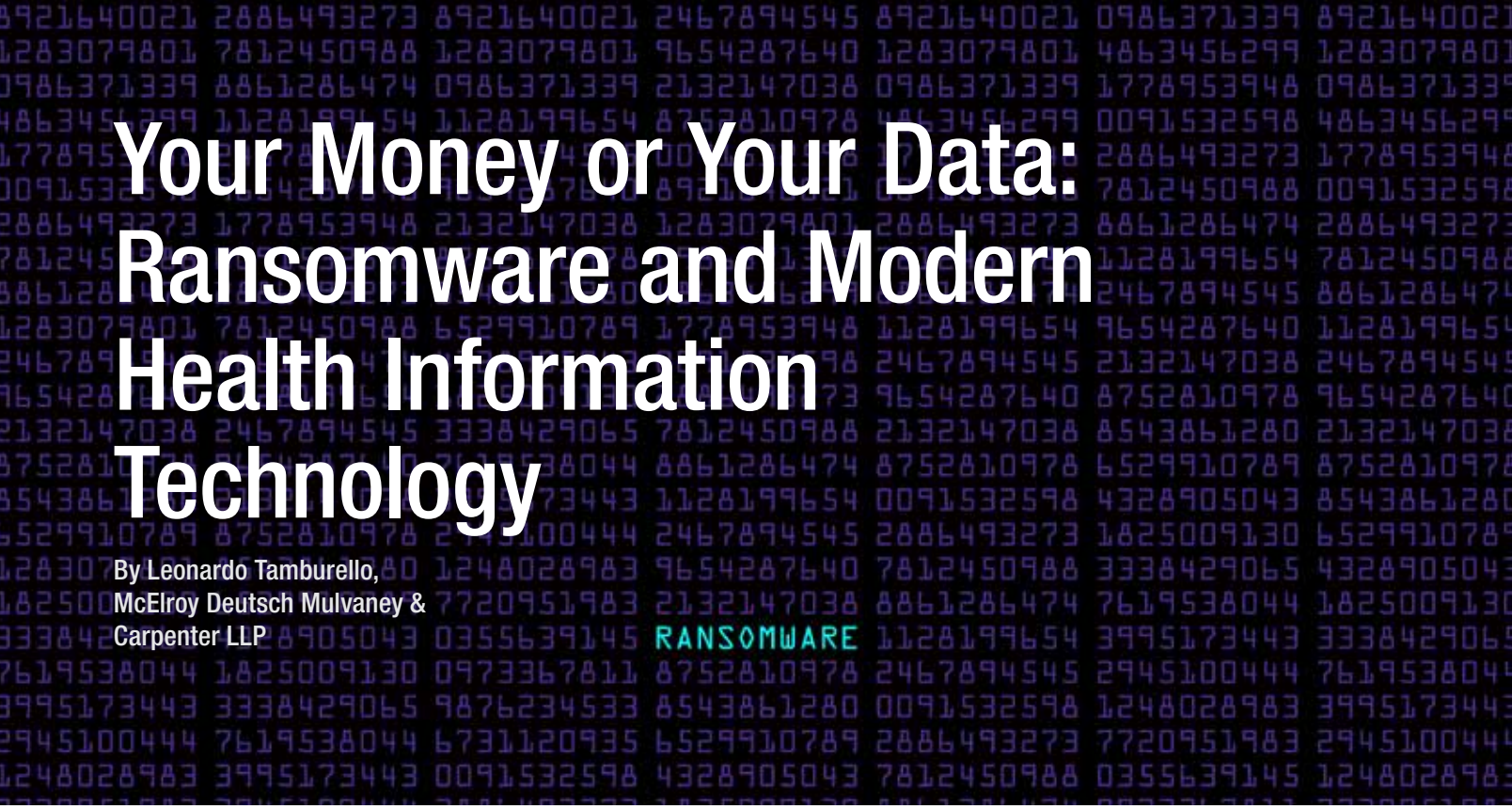
Your Money or Your Data: Ransomware and Modern Health Information Technology

By Leonardo Tamburello, McElroy Deutsch Mulvaney & Carpenter LLP



In his 2004 State of the Union Address, President George W. Bush provided a vision for health care in the United States whereby through "computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care."[1] Since then, the federal government has provided nearly $40 billion in incentive payments resulting in over 96% of all non-federal acute care hospitals possessing certified electronic health record (EHR) technology.[2] Similarly, approximately 83% of office-based physicians have implemented EHR systems to date.[3]

These information technology systems and the resulting hoard of data have created a new universe of vulnerabilities and potential risk. Breaches of protected health information (PHI) affected over 113 million individuals in 2015. During that timeframe, "hacking" accounted for nearly 99% of all individuals affected but only about 20% of all reported breaches.[4] In other words, while hacking incidents accounted for approximately one of every five breach incidents, these events accounted for nearly all of the individuals whose PHI was compromised in 2015. Hacking has emerged as the unmistakable single greatest threat to the security of PHI.

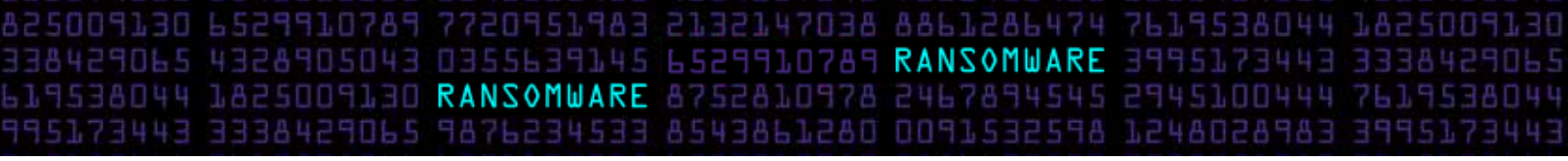
The threat to EHRs and other forms of health information technology posed by malevolent software ("malware") in general and a sub-species known as "ransomware" is only now being realized. The first iterations of "ransomware" merely restricted access to certain files until payment was tendered. More recently, ransomware has evolved to the point where it actively encrypts underlying data, making recovery impossible without a unique decryption key. (These programs are technically "*crypto*-ransomware" based on the additional step of encrypting the target files rather than only restricting user access. However, the term "ransomware" is used in this article to refer to both traditional ransomware and crypto-ransomware sub-variants.) That key, available for a price, is stored on a "command and control" server somewhere on the internet. These servers are computers that hackers have compromised and commandeered to run their schemes. Further ratcheting up the pressure, the decryption keys are designed to self-destruct after a fixed amount of time, adding urgency to the unfortunate ransomware victim's despair when they learn that their system has fallen victim to one of these programs.[5]

The proliferation of ransomware reflects the relatively recent widespread availability of sophisticated encryption algorithms and the rise of Bitcoin (BTC) as a form of anonymous and untraceable virtual currency.

Ransomware: New Wine, Old Bottles

The basic criminal strategy of ransomware is not new. Long before the invention of EHRs, King Richard I was captured near Vienna when returning to England from the Crusades and held until a "King's Ransom" of nearly $150,000 marks, almost twice England's GDP at the time (or approximately $3.3 billion in present value), was paid for his release.[6] As recently as 2010, armed gunmen operating in the waters off the Horn of Africa captured freighters and their crews until millions of dollars were paid.[7] The first known case of digital ransom-taking occurred in 1989 when a malicious program circulated via infected floppy discs and rendered a system unusable until the user paid a "license fee" of $189.[8]

Although the majority of contemporary single-system ransomware infections demand between $200 and $500 to unlock data, targets such as health care providers and their business associates that store more valuable information are



at risk of hackers commanding higher demands.[9] In addition, recent versions of ransomware not only target individual machines or workstations, but also actively search for network drives, including backups and core servers that store shared databases and files across an enterprise.[10]

The proliferation of ransomware reflects the relatively recent widespread availability of sophisticated encryption algorithms and the rise of Bitcoin (BTC) as a form of anonymous and untraceable virtual currency. In 2014, one form of ransomware known as CryptoLocker hauled in an estimated $27 million worldwide.[11] Between April 2014 and June 2015, which is before the most recent rash of infections affecting hospitals hit the news, ransomware victims reported more than $18 million in losses, according to the Federal Bureau of Investigation (FBI).[12] Between June 4 and June 21, 2016, CryptXXX ransomware raked in over $45,000.[13] In the first three months of 2016, all forms of ransomware accounted for approximately $209 million in revenues, putting ransomware on pace to become a $1 *billion* industry for the year.[14]

As demonstrated by these numbers, ransomware has become the preferred low-risk/high return value proposition for enterprising internet criminals. There is little fear of law enforcement reprisal, and ransomware software packages are available for sale by operators for a modest fee.[15] A 2015 Trustwave Global Security Report estimated a 1,425% return on investment for a single ransomware campaign.[16] According to data from the first half of 2016, attempted ransomware intrusions have increased by ten-fold to over 30,000 attempts per day on some systems.[17]

The threat to EHRs and other forms of health information technology posed by malevolent software ("malware") in general and a subspecies known as "ransomware" is only now being realized.

Traditional InfoSec Goals Thwarted by Ransomware

The traditional "triad" of information security aims to defend and maintain the *confidentiality, integrity,* and *availability* of information systems and the data they house.[18] The Health Insurance Portability and Accountability Act (HIPAA) Security Rule mirrors this principle, requiring covered entities and business associates to "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits."[19]

Unlike other data breaches that involve a compromise of data's confidentiality (i.e., the data is physically or virtually somewhere it is not supposed to be), most current forms of ransomware compromise the *availability* of not only the underlying data, but also the information systems themselves by locking users out of them altogether. For health care enterprises, these are mission-critical components of their daily operations and include EHRs, pharmacy systems, scheduling databases, and similar networks that are used to create, store, retrieve, and share data. In this respect, the threat posed by ransomware is different both in kind and scope from other types of breaches. Whereas the information lost in a compromised database had the greatest potential to affect the individuals to whom it is related, ransomware brings the institutional systems that create, store, and move the data to a grinding halt. Hospitals whose EHRs have fallen victim to ransomware have been forced to resort to pre-EHR "pen and paper" as they struggled to continue operations.[20]

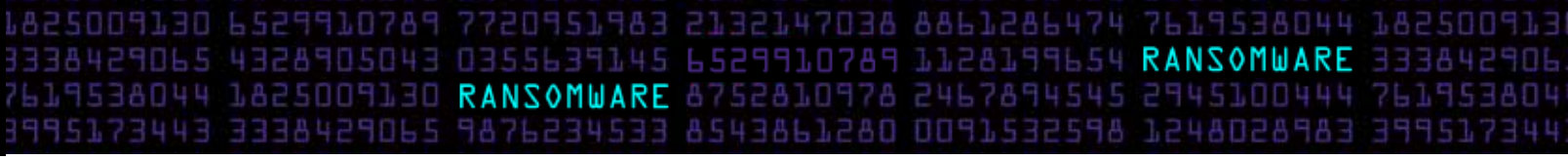
Common Attack Vectors: Phishing, "Malvertising" and Zero-Day Attacks

Oftentimes, the first sign of ransomware infection is a screen like this one:

Ransomware most frequently gains entry into networks through users who unwittingly open malicious email attachments. So-called "phishing" emails use social engineering to trick recipients into providing access credentials (which are then captured by the hackers) or opening an attachment (most often a Microsoft Word document) that will unleash a hidden ransomware program.[21] The more personalized the lure, the more successful such attacks are likely to be.[22]

The cost of personalization in terms of the time required to gather background information and then incorporating it into highly targeted "spear-phishing" emails that appear to originate from known or trusted source has, so far, limited this type of threat.[23] However, with the proliferation of company websites and social media, individuals are exposing much more of their once-private information through Facebook, Twitter, LinkedIn, and the like. At least one fraudster known as "TA530" may have found a way to scale spear-phishing by including the target's name, title, phone number, and company name in the email body, subject, and attachments.[24] Hackers also phish using so-called "soft targeted" emails aimed at individuals with a particular job title or in a specific industry. For example, a physician may receive an email with "lab results" attached, or a practice manager may receive a "resume" via email in response to a recent job posting online.[25] It is estimated that in the first four months of 2016, up to 93% of phishing emails were ransomware lures.[26]

The compromise of legitimate advertisement networks also has caused ransomware infections to visitors who simply viewed websites with infected ads, without the need for any further clicking.[27] This is accomplished by the surreptitious



insertion of ransomware into the advertising banners served by these networks, which then are shown to users worldwide on legitimate and popular websites. A recent advertising network infection served malicious ransomware-installing video ads to visitors of the BBC, *The New York Times*, the NFL, MSN, and AOL, among others.[28]

Ransomware infections also occur by the exploitation of known and unknown flaws in popular software such as Microsoft Windows, Adobe Flash, and others. Of particular concern are unknown or "zero-day" exploits that are "software or hardware vulnerabilities that have been discovered by an attacker where there is no prior knowledge of the flaw in the general information security community, and thus no vendor fix or software patch available for it."[29] By their very definition, there is no way to prepare or defend against these attacks, hence the term "zero-day," meaning there are "zero days" to fix the vulnerability before it is used maliciously. As such flaws are discovered, they usually are patched within a short time by software and hardware vendors, assuming the products are still supported. This makes the installation of regular updates and patches, along with removing hardware and software that is no longer supported by security updates, an extremely high priority. In June 2016, a hacker was selling a plaintext database of 9.3 million records from an unnamed "U.S. health insurer" for 750 BTC (approximately $500,000) that they claimed to have obtained via a zero-day exploit within Microsoft's Remote Desktop.[30] At least one government network also was taken offline after a ransomware attack via an unpatched zero-day exploit.[31]

In addition to zero-day exploits, failing to update systems and servers with the latest security patches also has led to ransomware infections.[32] Hospitals, health insurers, government agencies, and other large institutions are particularly susceptible to attacks that exploit software that is no longer patched or supported. Vulnerabilities in legacy systems including Windows XP-based machines for which official support ended in 2014 represent a potentially huge attack surface for all forms of malware, including ransomware.[33] Unfortunately, the health care industry's poor reputation for information security,[34] coupled with the value of the data that it possesses, makes the sector as a whole a ripe and tempting target for ransomware exploits. Unpatched network servers have been suspected but not confirmed as the culprits in several hospital ransomware attacks.[35]

Defense and Mitigation Strategies

Effective backups—meaning backups that allow for easy data restoration with little or no operational disruption once the infection itself is removed—are the best solution once ransomware is found on a system. Attesting to this, Methodist Hospital in Henderson, KY, stopped a ransomware attack and restored affected data from backups without paying a cent by activating its backup systems, which permitted uninterrupted operations while the main system was restored.[36] This scenario appears to be the exception rather than the rule, however. Several other hospitals reported ransomware infections in 2016, and it is believed many other infections have gone unreported.[37] The first reported ransomware infection affecting a hospital occurred at Hollywood Presbyterian Medical Center in Los Angeles in early February 2016. In that case, the hospital's computer network was shut down[38] and users were locked out of the EHR for more than a week.[39] Eventually, the facility paid forty BTC (approximately $17,000) to restore its systems.[40]

Recent ransomware iterations have targeted attached network drives, making Windows Volume Shadow Copy and Apple Time Machine backups potentially vulnerable to encryption by ransomware. Because encrypted backups are unusable, offline backups disconnected from network access after they are written are ideal for this purpose. Backup and data restoration policies and procedures are typically included in organizational disaster recovery plans, a required element of a HIPAA compliance plan,[41] and should be regularly tested to ensure data integrity and ease of restoration.[42] This planning should include testing of data and system backups that specifically quantifies the time required to restore compromised systems and data.

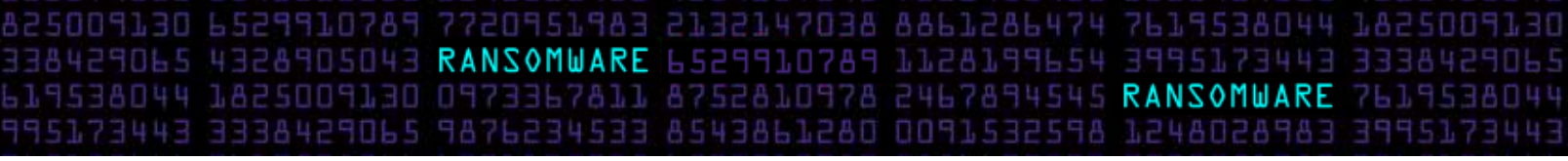
Effective backups—meaning backups that allow for easy data restoration with little or no operational disruption once the infection itself is removed—are the best solution once ransomware is found on a system.

If effective backups do not exist, the choice becomes starker: abandon the data that has been encrypted or pay the ransom. For many health care systems, giving up on their data is not an option. Paying the ransom, however, is not recommended by the FBI, as it rewards criminal behavior, and is believed to encourage more attacks.[43] This advice, however, can be difficult to follow for victims in the throes of a crisis. In such cases, paying the ransom in an individual case is oftentimes seen as "cheaper," particularly if effective backups are not available. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," according to one hospital's chief executive. "In the best interest of restoring normal operations, we did this," he concluded.[44]

The best defense to ransomware is to avoid becoming one of its victims. Although no defense is completely impenetrable, management and system administrators should focus resources in three important areas to fortify defenses against ransomware: user education, technical defenses, and disaster recovery planning. In addition, given the attention that ransomware has received, anticipating this threat should be part of an organization's ongoing Risk Assessment and Risk Management planning under HIPAA.[45]

All users must be educated about the dangers presented by sophisticated phishing attacks in general, and ransomware in particular. Employees must understand the critical role that each of them play in protecting the organization's data. Through new policies and training, organizations should strive for a high level of security awareness and culture change to minimize the possibilities that workforce members will unwittingly unleash a ransomware attack on their own systems.

In addition to educating users on the well-worn adage about not opening up emails or attachments from unknown or



The presence of ransomware on a covered entity's or a business associate's computer systems represents a "security incident" under the HIPAA Security Rule and may also result in an impermissible disclosure of PHI in violation of the HIPAA Privacy Rule.

strange senders, users must understand that even emails from "known" recipients can be manipulated through email spoofing (a process in which an email header is changed to conceal its origin or appear as if it was sent from a trusted source)[46] or originate from unwitting accomplices (if their email credentials have been compromised) in assisting hackers establishing a digital beachhead inside an organization.[47] Illustrating the latter, hackers compromised a provider's outside vendor who was engaged to send information such as newsletters, educational information, invitations, and announcements to patients, business associates, event attendees, website contacts, and other people associated with the provider. The intruders then used this access to send malware-laced emails that appeared to be legitimate since they originated from the provider to the provider's contact database. The incident reportedly affected over 23,000 individuals according to information reported under HIPAA to the federal government.[48]

In addition, maintaining all currently available software and hardware security patches will reduce the attack surface available to ransomware and other threats. Other technical defenses such as firewalls, application white-listing, network segmentation, and software restriction policies can limit or slow the proliferation of ransomware from affecting an entire network.[49] Finally, backups should be regularly maintained and tested for availability and integrity.

To Pay or Not to Pay, That Is the Question.

Fewer than 10% of hospitals surveyed by the Health Information and Management Systems Society (HIMSS) reported that they would pay a ransom demand. Roughly half said they would not pay, and the remaining 40% were unsure.[50] This sentiment mirrors IT executives generally; 84% of whom at companies that have never faced a ransomware attack said they would not pay. Interestingly, the same survey found that 43% of IT executives that had experienced a ransomware attack did, in fact, pay an average of $7,500.[51]

Illustrating the dangers of paying for files to be restored, at least one hospital system reported paying a ransom, only for the attackers to refuse to decrypt the files until more money was paid.[52] Ironically, this attempt to double-down on a ransom demand may ultimately backfire; after all, if paying the ransom does not guarantee safe return of the data, the incentive to pay quickly evaporates.[53] This development is not unique to health care ransomware, as the FBI has reported that ransom payments followed by no restoration has occurred in other industries.[54] Moreover, some believe that hospitals' willingness to pay ransoms has invited more attacks specifically targeted at the health care sector.[55] In this regard, Senator Barbara Boxer has expressed concern shared by others that, "by hospitals paying these ransoms, we are creating a perverse incentive for hackers to continue these dangerous attacks."[56]

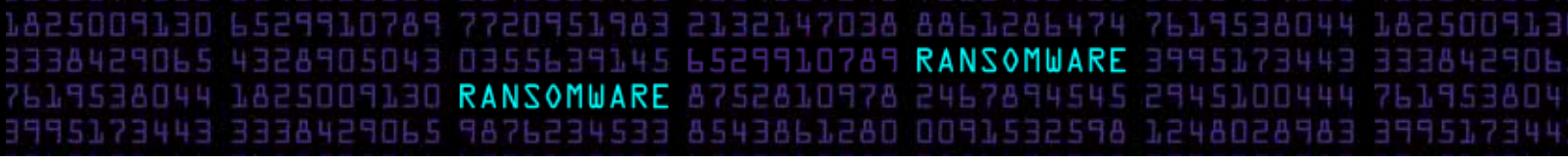
HIPAA Implications of a Ransomware Attack

The presence of ransomware on a covered entity's or a business associate's computer systems represents a "security incident" under the HIPAA Security Rule and may also result in an impermissible disclosure of PHI in violation of the HIPAA Privacy Rule.[57] Once ransomware is detected, an affected organization should initiate its security incident response and reporting procedures. Initially, this should include determining: (1) the scope of the incident to identify the networks, systems, or applications affected; (2) the origin of the incident; (3) whether the incident is finished, ongoing, or has cascaded into other security incidents; and (4) how the incident occurred.[58] Subsequent incident response activities should include containing the incident, eradicating the malware, remediating the vulnerability that caused the infection, restoring lost or affected data from backups, and post-incident security reviews to determine if any further compliance activity is required or warranted.[59]

Technically speaking whether or not a ransomware infection constitutes a "breach" under the Privacy Rule is a fact-specific determination, but in almost all cases it is likely that a breach has occurred in light of the Department of Health and Human Services Office for Civil Rights' (OCR's) statement that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."[60]

Providers, their business associates, and others who handle electronic data must continually adapt to meet this ever-changing threat environment or face the possibility that they too will be forced to pay their own modern-day King's Ransom.

This analysis becomes more complicated when the ransomware affects ePHI that already is encrypted. In such cases, the affected organization must undertake the fact-specific inquiry into whether the encryption solution used "has rendered the affected PHI unreadable, unusable, and indecipherable to unauthorized persons."[61] Certain full disk encryption solutions may render data "unreadable, unusable, and indecipherable" while the device is powered down in sleep mode or turned off. However, many of these encryption solutions are designed to "transparently" encrypt and decrypt files at login or as they are accessed by the user. If an authorized user has unlocked the device, (and hence, the data contained on it is decrypted and "unsecured"), and it becomes infected by ransomware, the encryption solution is effectively bypassed. As with other instances where unsecured data is exposed to ransomware encryption, it is very likely that a breach has occurred.[62]



Thus, the implementation of even fully "encrypted" devices containing PHI could be the source of a "breach" under certain circumstances when compromised by ransomware.

OCR already has levied fines for potential HIPAA violations when digital devices containing PHI have been lost or stolen without any need to verify that the PHI they contained was ever actually accessed or used.[63] In addition, at least one provider entered into a Resolution Agreement to settle a possible HIPAA violation arising from the breach of unsecured electronic protected health information affecting 2,743 individuals due to malware (other than ransomware) compromising the security of its information technology resources.[64]

Downstream Monetization of Ransomware Spoils

In addition to monetizing the restoration of encrypted files, attackers also derive value from the re-selling of the health care data itself. A form of ransomware called "Crysis" recently emerged that can remove data from, and take over administrative control of, compromised computers.[65] According to statistics reported by OCR, since late 2009 nearly 1,500 breach incidents have potentially exposed the medical data of over 155 million individuals in the United States.[66] Although ransomware has not been directly implicated, in late June 2016, a hacker was offering to sell three separate health care "databases" consisting of the electronic medical records of 48,000, 210,000 and 397,000 patients from institutions in Missouri, the "Central/Midwest United States," and Georgia, respectively.[67] The prices range between 151 BTC (approximately $100,000) to 607 BTC (approximately $395,000).[68]

Conclusion

The proliferation of electronic medical records along with other trends towards the digitization of health care information, coupled with the critical need for these systems to maintain ordinary operations has made health care a ripe target for ransomware in particular.[69] Ransomware will continue to proliferate as long as it remains profitable. As older versions become more easily detected and sometimes defeated, newer, stealthier, and possibly more destructive variants will continue to emerge. Providers, their business associates, and others who handle electronic data must continually adapt to meet this ever-changing threat environment or face the possibility that they too will be forced to pay their own modern-day King's Ransom. C

About the Author

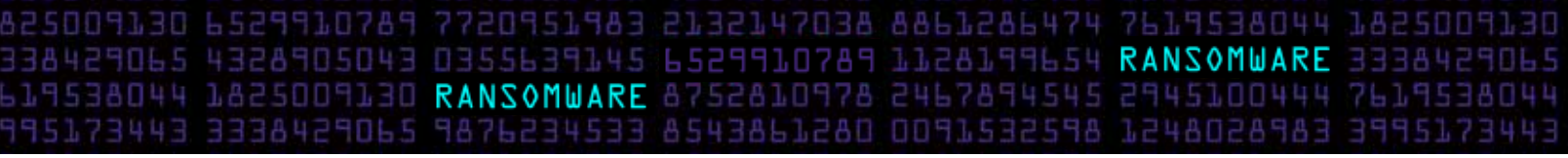
Leonardo Tamburello is co-chair of McElroy Deutsch Mulvaney & Carpenter LLP's Data Security and Privacy Practice Group. He obtained his BA in English with Honors from Rutgers University in 1994 and his JD from Rutgers School of Law—Newark in 1997. Mr. Tamburello has focused his work in health care law, with particular emphasis on emerging privacy and technology issues in the health care sector. He is also recognized as a Certified Information Privacy Professional/US (CIPP/US) by the International Association of Privacy Professionals.

Thanks go out to the leaders of the Health Information Technology Practice Group for sponsoring this feature article: Amy S. Leopard, Bradley Arant Boult Cummings LLP, Nashville, TN (Chair); **Alisa Lieberman Chestler,** Baker Donelson Bearman Caldwell & Berkowitz PC, Washington, DC (Vice Chair—Research & Website); **Kimberly Bullock Gatling,** Smith Moore Leatherwood LLP, Greensboro, NC (Vice Chair—Publications); **Gerard M. Nussbaum,** Kurt Salmon, Chicago, IL (Vice Chair—Membership); **Lisa Pierce Reisz,** Vorys Sater Seymour and Pease LLP, Columbus, OH (Vice Chair—Educational Programs); **Linda S. Ross,** Trinity Health, Livonia, MI (Vice Chair—Strategic Planning and Special Projects); **McKenzie A. Livingston,** Broad and Cassel, Miami, FL (Social Media Coordinator).

For more information about the Health Information and Technology Practice Group, visit www.healthlawyers.org/PGs or follow them on Twitter at @AHLA_HITsters.

Endnotes

1 Jack Beaudoin, *The Decade of Health IT*, Healthcare IT News (Dec. 20, 2016), *available at* http://www.healthcareitnews.com/news/decade-health-it.
2 Office of the National Coordinator for Health Information Technology (ONC), *Percent of Hospitals, By Type, that Possess Certified Health IT,* Health IT Quick-Stat #52 (May 2016), *available at* http://dashboard.healthit.gov/quickstats/pages/certified-electronic-health-record-technology-in-hospitals.php.
3 ONC, *Office-based Physician Electronic Health Record Adoption: 2004-2014,* Health IT Quick-Stat #50, Sept. 2015, *available at* http://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php.
4 ONC, *Breaches of Unsecured Protected Health Information*, Health IT Quick-Stat #53, Feb. 2016, *available at* http://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php.
5 Nicholas Griffin, *Locky Ransomware—Encrypts Documents, Databases, Code, Bitcoin Wallets, and More . . .* , Forcepoint (Feb. 19, 2016), *available at* https://blogs.forcepoint.com/security- labs/locky-ransomware-encrypts-documents-databases-code-bitcoin-wallets-and-more.
6 Gus Lubin & Shlomo Sprung, *The 18 Largest Ransoms Ever Paid*, Business Insider, (Sept. 12, 2012), *available at* http://www.businessinsider.com/the-biggest-ransoms-ever-2012-9?op=1.
7 Mohammed Ibrahim, *Enriched by Record Ransom, Somali Pirates Free Tanker*, N.Y. Times, Jan. 18, 2010, *available at* http://nyti.ms/294eHxZ.
8 Miguel Ángel Mendoza, *The evolution of ransomware: From PC Cyborg to a service for sale*, welivesecurity, (Sept. 18, 2015), *available at* http://www.welivesecurity.com/2015/09/18/evolution-ransomware-pc-cyborg-service-sale/.
9 Brian Lee, *Ransomware: Unlocking the Lucrative Criminal Business Model,* Palo Alto Networks: Unit 42, at 14, *available at* https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report.
10 Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware,* Wired (Mar. 30, 2016), *available at* https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.
11 *Id.*
12 U.S. Dep't of Justice, I-062315-PSA, Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes (June 23, 2015), *available at* https://www.ic3.gov/media/2015/150623.aspx.
13 Dan Goodin, *New and Improved CryptXXX Ransomware Rakes in $45,000 in 3 Weeks,* ARS Technica (June 27, 2016), *available at* http://arstechnica.com/security/2016/06/new-and-improved-cryptxxx-ransomware-rakes-in-45000-in-3-weeks/.
14 David Fitzpatrick & Drew Griffin, *Cyber-extortion Losses Skyrocket, Says FBI,* CNN (Apr.15, 2016), *available at* http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/.
15 Sean Gallagher, *OK, Panic—Newly Evolved Ransomware is Bad News for Everyone,* ARS Technica (Apr. 8, 2016), *available at* http://arstechnica.com/security/2016/04/ok-panic-newly-evolved-ransomware-is-bad-news-for-everyone/.



16 Trustwave, 2015 Trustwave Global Security Report (June 9, 2015), *available at* https://www2.trustwave.com/GSR2015.html.
17 Akanksha Jayanthi, *To pay or not to pay ransom: A tale of two hospitals,* Becker's Health IT and CIO Review (Mar. 28, 2016), *available at* http://www.beckershospitalreview.com/healthcare-information-technology/to-pay-or-not-to-pay-ransom-a-tale-of-two-hospitals.html.
18 Chad Perrin, *The CIA Triad,* TechRepublic (June 30, 2008), *available at* http://www.techrepublic.com/blog/it-security/the-cia-triad/.
19 Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164.306(a)(1) (2013).
20 Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating,* L.A. Times, Feb. 18, 2016, *available at* http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.
21 *What is Phishing?* PhisTank, *available at* https://www.phishtank.com/what_is_phishing.php.
22 Matthew Mesa, *Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware to Target Execs,* ProofPoint (Apr. 5, 2016), *available at* https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs.
23 *Id. See also* Norton by Symantec, *Spear Phishing: Scam, Not Sport, available at* https://us.norton.com/spear-phishing-scam-not-sport/article.
24 Mesa, *supra* note 22.
25 PhishMe, *Q1 2016 Sees 93% of Phishing Emails Contain Ransomware*, PhisMe (June 4, 2016), *available at* http://phishme.com/q1-2016-sees-93-phishing-emails-contain-ransomware/.
26 *Id.*
27 Cammy Harbison, *New Ransomware Installers Can Infect Computer Systems Without Users Clicking Anything, Says Researchers,* iDigitalTimes (Mar. 29, 2016), *available at* http://www.idigitaltimes.com/new-ransomware-installers-can-infect-computers-without-users-clicking-anything-say-522756.
28 Dan Goodin, *Big-name sites hit by rash of malicious ads spreading crypto ransomware,* ARS Technica (Mar. 15, 2016), *available at* http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/.
29 Zheng Bu, *Zero-day attacks are not the same as zero-day vulnerabilities,* FireEye (Apr. 24, 2014), *available at* https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html.
30 Dissent, *Lording It Over the Healthcare Sector: Health Insurer Database with 9.3M Entries Up for Sale*, DataBreaches.net (June 27, 2016), *available at* https://www.databreaches.net/lording-it-over-the-healthcare-sector-health-insurer-database-with-9-3m-entries-up-for-sale/.
31 Danny Palmer, *$500 zero-day ransomware attack takes council offline for nearly a week*, ZDNet.com (Feb. 2, 2016), *available at* http://www.zdnet.com/article/zero-day-ransomware-attack-takes-council-offline-for-a-nearly-week/.
32 Sean Gallagher, *Two more healthcare networks caught up in outbreak of hospital ransomware*, ARS Technica (Mar. 29, 2016), *available at* http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/.
33 Craig Timberg & Ellen Nakashima, *Government Computer Running Windows XP Will be Vulnerable to Hackers After April 8*, Wash. Post, Mar. 16, 2014, *available at* https://www.washingtonpost.com/business/technology/government-computers-running- windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html.
34 Cammy Harbison, *Ransomware is Hitting Dozens of Healthcare Organizations; Why File- Encrypting Malware is Infecting Health Systems*, iDigitalTimes (Mar. 30, 2016), *available at* http://www.idigitaltimes.com/ransomware-hitting-dozens-healthcare-organizations-why-file-encrypting-malware-523219.
35 Gallagher, *supra* note 32; Tami Abdollah, *Hackers Broke Into Hospitals Despite Software Flaw Warnings*, Associated Press, *available at* http://bigstory.ap.org/article/86401c5c2f7e43b79d7decb04a0022b4/hackers-broke-hospitals-despite-software-flaw-warnings.
36 Zetter, *supra* note 10; Akanksha Jayanthi, *Methodist Hospital Ransomware Attack Ends Without Payment,* Becker's Health IT & CIO Review (Mar. 23, 2016), *available at* http://www.beckershospitalreview.com/healthcare-information-technology/methodist-hospital-ransomware-attack-ends-without-payment.html.
37 Gallagher, *supra* note 32.
38 Jayanthi, *supra* note 17.
39 Kaveh Waddell, *A Hospital Paralyzed by Hackers*, The Atlantic (Feb. 17, 2016), *available at* http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/.
40 Winton, *supra*, note 20.
41 45 C.F.R. § 164.308(a)(7)(ii).
42 Adam Alessandrini, Ransomware Hostage Manual (KnowBe4 2016).
43 U.S. Dep't of Justice, Incidents of Ransomware on the Rise (Apr. 29, 2016), *available at* https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise; Jayanthi, *supra* note 17.
44 Winton, *supra* note 20.
45 *See* 45 C.F.R. § 164.308(a)(1). *See also* U.S. Dep't of Health and Human Servs. Office for Civil Rights, Six Basics of Risk Analysis and Risk Management 2 (2007), *available at* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.
46 Jack Detsch, *Why Hospitals Have Become Prime Targets for Ransomware Attacks*, The Christina Science Monitor (Apr. 20, 2016), *available at* http://www.csmonitor.com/World/Passcode/2016/0420/Why-hospitals-have-become-prime-targets-for-ransomware-attacks; Alan Henry, *How Spammers Spoof Your Email Address (and How to Protect Yourself)*, lifehacker (May 21, 2014), *available at* http://lifehacker.com/how-spammers-spoof-your-email-address-and-how-to-prote-1579478914.
47 Eric Auchard, *Exclusive: Big Data Breaches Found at Major Email Services – Expert*, Reuters (May 5, 2016), available at http://www.reuters.com/article/us-cyber-passwords-idUSKCN0XV1I6.
48 Jacqueline Belliveau, *Healthcare Ransomware Threat Leads to Data Security Incident*, Health IT Security.com (May 12, 2016), *available at* http://healthitsecurity.com/news/healthcare-ransomware-threat-leads-to-data-security-incident.
49 Alessandrini, *supra* note 42 (KnowBe4 2016).
50 David Pittman, *HIMSS survey on ransomware response*, Politico (Apr. 11, 2016), *available at* http://www.politico.com/tipsheets/morning-ehealth/2016/04/himss-survey-on-ransomware-response-213691.
51 *C-Suite Execs Say Won't Pay Ransom Attacks, Until They Get Hacked, Radware Survey Finds*, Radware (June 28, 2016), *available at* https://www.radware.com/newsevents/pressreleases/execs-wont-pay-ransom-attacks-til-hacked/.
52 Lee Matthews, *Hospital pays ransom, ransomware demands more money*, Geek (May 24, 2016), *available at* http://www.geek.com/tech/hospital-pays-ransom-ransomware-demands-more-money-1656035/.
53 Robert Lemos, *How greed could destroy the ransomware racket*, PCWorld (June 28, 2016), *available at* http://www.pcworld.com/article/3083772/security/how-greed-could-destroy-the-ransomware-racket.html.
54 Jennifer Orr Mitchell & Kurt R. Hunt, *Cybersecurity Alert: Ransomware Attacks on Rise*, Nat'l L. Rev. (June 14, 2016), *available at* http://www.natlawreview.com/article/cybersecurity-alert-ransomeware-attacks-rise.
55 Paul Szoldra, *Hospitals Keep Getting Attacked by Ransomware—Here's Why,* Tech Insider (June 1, 2016), *available at* http://www.techinsider.io/hospital-ransomware-hack-2016-5.
56 Robert Radick, *Ransomware, Cyberattacks, and Hacking in the Health Care Industry: Lessons from a Letter to the FBI*, Forbes (Apr. 14, 2016), *available at* http://www.forbes.com/sites/insider/2016/04/14/ransomware-cyberattacks-and-hacking-in-the- health-care-industry-lessons-from-a-letter-to-the-fbi/#abaf5973dd64.
57 45 C.F.R. § 164.304 (defining "security incident"), 45 C.F.R. § 164.402 (defining "breach"). *See also* U.S. Dep't of Health and Human Servs., Office for Civil Rights, *FACT SHEET: Ransomware and HIPAA* (2016), at 4, *available at* http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
58 *See* 45 C.F.R. § 164.308(a)(6); FACT SHEET, *supra* note 57, at 4-5.
59 FACT SHEET, *supra* note 57, at 5.
60 *Id.* at 5-6.
61 *Id.* at 8.
62 *Id.* at 8.
63 Jack Danahy, *Why Healthcare Ransomware Attacks are HIPAA Breaches*, Health IT Security.com (Apr. 14, 2016), *available at* http://healthitsecurity.com/news/why-healthcare-ransomware-attacks-are-hipaa-data-breaches. *See also* U.S. Dep't of Health and Human Servs., Office for Civil Rights, Resolution Agreement with Concentra Health Services, dated December 2, 2014, *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf?language=es.
64 U.S. Dep't of Health and Human Servs., Office for Civil Rights, Resolution Agreement with Anchorage Community Mental Health Services, Inc., dated December 2, 2014, *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf
65 Akanksha Jayanthi, *Why Crysis is healthcare's most threatening ransomware yet*, Becker's Health IT and CIO Review (June 24, 2016), *available at* http://www.beckershospitalreview.com/healthcare-information-technology/why-crysis-is-healthcare-s-most-threatening-ransomware-yet.html.
66 Niam Yaraghi, *Patient Privacy: Can Past Lessons Prevent Future Failures?*, Brookings Inst. (May 5, 2016), *available at* https://www.brookings.edu/blog/techtank/2016/05/05/patient-privacy-can-past-lessons-prevent-future-failures/.
67 *New Breach: 655,000 Healthcare Records (Patients) Being Sold*, Deep. Dot.Web (June 26, 2016), *available at* https://www.deepdotweb.com/2016/06/26/655000-healthcare-records-patients-being- sold/.
68 *Id.*
69 @JennHIStalk, *Could Ransomware's Rise be Healthcare's Downfall?,* HIStalk (Apr. 4,2016), *available at* http://histalk2.com/2016/04/04/could-ransomwares-rise-be-healthcares-downfall./