Richmond Journal of Law & Technology Volume XXIII, Issue 3

RANSOMWARE – PRACTICAL AND LEGAL CONSIDERATIONS FOR CONFRONTING THE NEW ECONOMIC ENGINE OF THE DARK WEB

By: James A. Sherer,* Melinda L. McLellan,** Emily R. Fedeles,*** and Nichole L. Sterling****

Cite as: James A. Sherer, Melinda L. McLellan, Emily R. Fedeles, and Nichole L. Sterling, *Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 Rich. J.L. & Tech. Ann. Survey (2017), http://jolt.richmond.edu/2017/04/30/volume23_annualsurvey_sherer/.

I. INTRODUCTION

[1] Ransomware is malicious software that encrypts data on a device or a system, then bars access to, or recovery of, that data until the owner has paid a ransom.[1] This type of threat has existed in some shape or form

* James A. Sherer is a Partner in the New York office of Baker & Hostetler LLP.
** Melinda L. McLellan is a Partner in the New York office of Baker & Hostetler LLP.
*** Emily R. Fedeles is an Associate in the New York office of Baker & Hostetler LLP.
**** Nichole L. Sterling is an Associate in the New York office of Baker & Hostetler LLP.

[1] *See* Krzysztof Cabaj & Wojciech Mazurczyk, *Using Software-Defined Networking for Ransomware Mitigation: the Case of CryptoWall*, 30 IEEE NETWORK 14 (2016).

since at least 1989,[2] but over the past two years the frequency and scope of attacks have increased to alarming levels. In response, the U.S. Federal Trade Commission (FTC) identified Ransomware as "one of the most serious online threats facing people and businesses" in 2016 as well as "the most profitable form of malware criminals use,"[3] and the FBI developed a special working group dedicated to fighting it.[4]

[2] Considering that Ransomware emerged "at the dawn of the Internet revolution,"[5] even before the development of formalized Internet law and policy, attorneys have now had a bit of time to become familiar with its operation and effects and to contemplate reasonable and legitimate responses to Ransomware attacks. Despite the intervening decades, and although Ransomware as a process and business are (somewhat) better understood, the legal implications of Ransomware attacks are still up for debate, and there is no simple answer to the question of how Ransomware victims can, or should, deal with an attack.

[3] This digital menace poses constantly evolving threats, which adds to the challenges victims confront when attempting to implement current

[2] *See* JAMES SCOTT & DREW SPANIEL, THE ICIT RANSOMWARE REPORT: 2016 WILL BE THE YEAR RANSOMWARE HOLDS AMERICA HOSTAGE 3–4 (2016).

[3] Ben Rossen, *How to Defend Against Ransomware*, FTC (Nov. 10, 2016), https://www.consumer.ftc.gov/blog/how-defend-against-ransomware, https://perma.cc/CJA5-BV2B.

[4] *See* Paul Merrion, *FBI Creates Task Force to Fight Ransomware Threat*, CQ ROLL CALL, Apr. 4, 2016, 2016 WL 2758516.

[5] Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 DUKE L.J. 1045, 1045 (2001).

guidance and benchmarked response efforts to Ransomware. These challenges are not only rooted in functionality and potential damage, but also due to the emergence of a viable business model facilitating Ransomware's exponential growth as a tool for criminals. We will explore these challenges by providing an overview of Ransomware's development and spread and then examining the current, albeit unsettled, legal landscape surrounding Ransomware attacks and victim responses, to consider what the future might hold for regulation in this space.

II. A HISTORY OF RANSOMWARE

[4] As noted above, Ransomware has been around in one form or another for at least ten years,[6] and as early as 1989 in the U.S.[7] and Europe.[8] The first recorded example was biologist Joseph Popp's "AIDS Trojan": Popp developed the virus and "passed 20,000 infected floppy disks out at the 1989 World Health Organization's AIDS conference."[9] Ransomware subsequently faded as a notable security concern for more

[6] *See* Amin Kharraz et al., *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, *in* DIMVA 2015 PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON DETECTION OF INTRUSIONS AND MALWARE, AND VULNERABILITY ASSESSMENT 3 (Springer 2015).

[7] *See* James Scott & Drew Spaniel, *supra* note 2, at 4.

[8] NICOLE VAN DER MEULEN ET AL., EUROPEAN PARLIAMENT POLICY DEP'T FOR CITIZENS' RIGHTS & CONSTITUTIONAL AFFAIRS, CYBERSECURITY IN THE EUROPEAN UNION AND BEYOND: EXPLORING THE THREATS AND POLICY RESPONSES 35 (2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf, https://perma.cc/6M58-B4TW.

[9] James Scott & Drew Spaniel, *supra* note 2, at 6.

than a decade before making another brief appearance in 2005.[10] Then, in the wake of an economic recession, Ransomware came back with a vengeance, making a dramatic entrance as it "resurged in 2013;"[11] it has continued to flourish ever since. Interestingly, Ransomware's recent reemergence may be explained, in part, by the success of other hacking efforts. The historical model for the most obvious cybercrimes had been stealing and selling data (usually credit card numbers), but this fraud became so prevalent that the going rate for stolen payment card information has dropped precipitously over the past five years.[12] In response, "[t]o keep cybercrime profitable, criminals needed to find a new cohort of potential buyers, and they did: all of us."[13]

[5] Although experts rightly emphasize the significant problem Ransomware presents today, the risks have not always been so grave in the hostage-software industry. As Doug Pollack noted, "ironically, until [the 2005 resurgence], most [Ransomware] was fake. Fraudulent spyware removal tools and performance optimizers scared users into paying to fix problems that didn't really exist."[14] Regardless, most present-day (and,

[10] *See id*.

[11] *See* VAN DER MEULEN, *supra* note 8, at 35.

[12] *See* Josephine Wolff, *The New Economics of Cybercrime*, THE ATLANTIC (June 7, 2016), http://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/, https://perma.cc/5L3U-47CT.

[13] *Id*.

[14] DOUG POLLACK, RANSOMWARE 101: WHAT TO DO WHEN YOUR DATA IS HELD HOSTAGE 7 (2016) (ebook), http://lpa.idexpertscorp.com/acton/attachment/6200/f-051f/1/-/-/-/-/IDE_eBook_Ransomware_082616_v1.pdf?cm_mmc=Act-On%20Software-_-email-_-ID%20Experts%20Download%20-

likely, future) Ransomware *is* serious business, both in the effects it has on victims and in the underground infrastructure that buttresses Ransomware's propagation. Moreover, the scourge of Ransomware is growing steadily, with some researchers noting 500% yearly increases.[15] Other experts focus on the exponential reach of Ransomware, noting that it "infects one computer but…often spreads across network drives to infect other computers as well."[16]

[6] In the face of an inarguably immense and expanding problem, an understanding of the relevant legal issues is crucial for practitioners who will encounter Ransomware and its effects. That said, evaluating the applicable legal framework requires knowledge of Ransomware's mechanics, which may vary widely by the type, source, and purpose of the Ransomware—not to mention the specific effects it may have on a given organization.

III. RANSOMWARE AS A PROCESS

[7] Malware is malicious software, but that category "encompasses a wide range of program types including viruses, worms, logic bombs,

%20Ransomware%20101%3A%20What%20to%20Do%20When%20Your%20Data%20is%20Held%20Hostage-_-Download%20Now&sid=TV2:dA7ip6myT, https://perma.cc/327S-TXFL.

[15] *See* Kharraz, *supra* note 6, at 1, 4.

[16] *See* Azad Ali et al., *Recovering from the Nightmare of Ransomware – How Savvy Users Get Hit with Viruses and Malware: A Personal Case Study*, 17 ISSUES IN INFORMATION SYSTEMS 58, 61 (2016).

Trojan horses, keyloggers, zombie programs, and backdoors."[17] One subcategory of Malware is "Scareware," or Malware that "takes advantage of people's fear of revealing their private information, losing their critical data, or facing irreversible hardware damage."[18] Ransomware is a subset of Scareware; specifically a "category of malicious software which, when run, disables the functionality of a computer in some way,"[19] making it essentially "a digital version of hostage taking."[20] Ransomware is also classified as a type of viral software, which is software that may be grouped into separate "families" and differentiated by whether it presents only the superficial trappings of a threat or poses an actual problem.[21] We may divide the types of Ransomware that pose an actual threat into two main groups: "one-off" variants used in an ad-hoc fashion, and software that serves as an extension of the broader criminal infrastructure into which victims pay their ransom.

---

[17] Robert J. Kroczynski, *Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited?*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 817, 823 (2008).

[18] *See* Kharraz, *supra* note 6, at 1.

[19] Gavin O'Gorman & Geoff McDonald, *Ransomware: A Growing Menace*, SYMANTEC CORP. (2012) at 2, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf, https://perma.cc/F6UF-UDUL.

[20] Eric Jardine, *A Continuum of Internet-Based Crime: How the Effectiveness of Cybersecurity Policies Varies across Cybercrime Types*, RESEARCHGATE, 10 (Jan. 2016), *reprinted in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 421 (F. Xavier Olleros & Majinda Zhegu eds., 2016).

[21] *See* Kharraz, *supra* note 6, at 2.

A. Locker Ransomware

[8] Beginning with the functional mechanics of the software, Ransomware attacks can be segregated by form. Early variants[22] were primarily *Locker* Ransomware, and were identified as such (e.g., WinLocker, which would lock up a user's screen, and Master Boot Record, which would interrupt a user's normal operating system).[23] The Locker approach "restricts user access to infected systems by locking up the interface or computing resources within the system,"[24] thereby blocking off access to the computer or denying access to files.[25] Locker Ransomware may display "a message that demands payment to restore functionality,"[26] such that it appears similar to the other Ransomware variants discussed below, but operates quite differently.

[9] If the victim's operating system is imagined as a storage unit, where the worth of the operating system lies in the items contained within

[22] *See, e.g.*, William Largent, *Ransomware: Past, Present, and Future*, TALOS BLOG (Apr. 11, 2016, 9:01 AM), http://blog.talosintel.com/2016/04/ransomware.html, https://perma.cc/QU27-WDRK (last visited Feb. 6, 2017).

[23] *See* Ian T. Ramsey & Edward A. Morse, Cyberspaxe Law Comm. Winter Working Grp., Ransoming Data: Technological and Legal Implications of Payments for Data Privacy 4–5 (Jan. 29-30, 2016) (unpublished manuscript) (on file with author), http://www.stites.com/uploads/learning-center/Ramsey_Ransoming-data_Jan2016.pdf, https://perma.cc/H4BZ-UHY3.

[24] Pollack, *supra* note 14, at 7.

[25] *See* Largent, *supra* note 22.

[26] *See* O'Gorman & McDonald, *supra* note 19, at 2.

the unit, Locker Ransomware operates by effectively changing the lock on the door, or, in some cases, changing the mechanism by which the lock engages. The items within the storage unit remain untouched, and the victim is asked to pay to have the door unlocked (or to have the locking mechanism restored to its original form), but victims in such Locker Ransomware cases have other options for regaining access. For example, they can try to bypass the door by (metaphorically) drilling out the lock, taking the door off its hinges, or just removing the walls from around the unit's contents.

B. Crypto Ransomware

[10] Cryptographic approaches to Ransomware operate differently, though the initial message—pay us or you cannot access your data—looks the same at first blush. Rather than focusing solely on the lock, however, these variants[27] employ a Crypto Ransomware or CryptoLocker approach.[28] Here, the Ransomware "encrypts files on the target system so that the computer is still usable, but users can't access their data."[29] This type of Ransomware typically "uses RSA 2048 encryption to encrypt files," making "cracking the lock" to avoid paying ransom an

[27] *See, e.g.*, Largent, *supra* note 22.

[28] *See id*.

[29] Doug Pollack, *Trading in Fear: The Anatomy of Ransomware*, ID EXPERTS (May 2, 2016), https://www2.idexpertscorp.com/blog/single/trading-in-fear-the-anatomy-of-ransomware, https://perma.cc/7VTU-5QAC.

impossibility; for an average desktop computer, this approach would take "around 6.4 quadrillion years."[30]

[11] Continuing with the storage unit metaphor, a Crypto Ransomware approach may or may not tamper with the lock on the front door. Instead, Crypto Ransomware sizes up each item within the unit, systematically determining the relative value of the files to the user. These may include, for example, unstructured data comprised of user photos, Word documents, Excel files, or PDFs. Once those files are identified by extension, the program goes to work, encrypting each file and rendering it unusable pending payment of the ransom—unless, as we discuss below, (1) the user can find a workaround solution online; or (2) the ransom *is* paid but no key is provided.

[12] When it comes to Crypto Ransomware, there is no option to drill out the lock, take the door off the hinges, or tear down the wall; each file is locked up separately and indefinitely.[31] Accordingly, this type of Ransomware poses a very different kind of threat and, as such, is handled quite differently by experienced security professionals tasked with solving the problem.

[13] Crypto Ransomware doesn't stop there. Certain variants add insult to injury, as some may, "while encrypting files, search[] and steal[]

[30] ADAM ALESSANDRINI, RANSOMWARE HOSTAGE RESCUE MANUAL 2, (2015), http://resources.idgenterprise.com/original/AST-0147692_Ransomware-Hostage-Rescue-Manual.pdf, https://perma.cc/9V7T-L4YA.

[31] Considerations associated with quantum computing and decryption are outside the purview of this paper.

[B]itcoins from the user."[32] Others, called "Doxware," may focus on areas normally associated with user privacy such as conversations, photos, and other sensitive files; and threaten to release them publicly unless the ransom is paid.[33] Still another form of Crypto Ransomware, Shadowlock, "forces users to complete consumer surveys of products and services as the ransom payment."[34]

[14] Although Ransomware's efficacy has improved over the decades since its introduction, many earlier forms are still in use.[35] This may be due in part to its inherent longevity, as one key element of older Ransomware's functionality is the malicious way in which its self-propagating features make it incredibly difficult to eliminate. Some legacy Ransomware variations are no longer in circulation, but certain "[m]alware that was released years—in some cases, decades—ago is still alive and well today,"[36] making awareness of modern Ransomware's progenitors required knowledge for practitioners active in this space.

[32] Ramsey & Morse, *supra* note 23, at 5.

[33] Chris Ensey, *Ransomware Has Evolved, And Its Name Is Doxware*, DARKREADING (Jan. 4, 2017, 07:30 AM) http://www.darkreading.com/attacks-breaches/ransomware-has-evolved-and-its-name-is-doxware/a/d-id/1327767, https://perma.cc/VGJ6-HUHD (noting also that this would be one way of getting back access to at least some of the hostage files).

[34] *Technical Intricacies of Ransomware and Safeguarding Strategies*, FALL 2016 E-NEWSLETTER (Digital Mountain, Santa Clara, C.A.), 2016, at 1, http://digitalmountain.com/enews/FALL_2016_Article2.pdf, https://perma.cc/8CKR-3Q3A.

[35] *See* Largent, *supra* note 22.

[36] *Id*.

C. Ransomware Delivery

[15] Despite the automated nature of Ransomware's self-propagation, the spread of most Ransomware is still a personal process that relies on human error.[37] The FBI notes specifically that "Ransomware is frequently delivered through spear phishing emails" to end users.[38] Other common methods of installing Ransomware are "exploit kits,"[39] "Web exploits and drive-by downloads,"[40] "infected removable drives, infected software installers,"[41] and "mass phishing campaigns."[42] In a "mass phishing campaign,"[43] malware is "installed on a user's computer without their knowledge when that user browses to a compromised website,"[44] and is

[37] *See id*.

[38] *See* U.S. DEP'T OF JUSTICE, PROTECTING YOUR NETWORKS FROM RANSOMWARE 2, https://www.justice.gov/criminal-ccips/file/872771/download, https://perma.cc/3GT6-ARH.

[39] *See* Largent, *supra* note 22, at 1.

[40] *See* O'Gorman & McDonald, *supra* note 19, at 4.

[41] *See Practical Steps to Thwart Ransomware and other Cyberbreaches*, YOURABA (Dec. 2016), http://www.americanbar.org/publications/youraba/2016/december-2016/be-prepared-to-thwart-ransomware-and-other-cyber-attacks.html, https://perma.cc/U5G4-VX97.

[42] *See* Largent, *supra* note 22.

[43] *Id*.

[44] *See* O'Gorman & McDonald, *supra* note 19, at 4.

using "outdated browsers, browser plugins, and other software."[45] These techniques may be referred to as "malvertising" where "[c]ybercriminals leverage compromised advertising networks to serve malicious advertisements on legitimate websites which subsequently infect the visitors...[later] redirecting the user to an Exploit Kit (EK) landing page."[46]

[16] In addition to leveraging self-propagation, Ransomware schemes also may rely on the "spray and pray" technique, or sending out massive quantities of malware-infected emails in hopes of hitting "as many individual targets…as quickly as possible" by virtue of sheer volume.[47] Still other types of Ransomware have begun to deploy an even more personal approach, tailoring messages to appear as genuine as possible; often through social engineering research used to gain knowledge of a company's operational structure, invoicing and remittance practices, and even individuals' writing styles.[48] Increasingly, "e-mails are highly

[45] FED. BUREAU OF INVESTIGATION, RANSOMWARE, www.blockchainalliance.org/docs/Ransomware_e-version.pdf, https://perma.cc/66XL-V4J7.

[46] Deepen Desai, *Malvertising, Exploit Kits, ClickFraud & Ransomware: A Thriving Underground Economy*, ZSCALER (Apr. 21, 2015), https://www.zscaler.com/blogs/research/malvertising-exploit-kits-clickfraud-ransomware-thriving-underground-economy, https://perma.cc/C4PN-TM4C.

[47] *See* Largent, *supra* note 22.

[48] *See Ransomware on the Rise: Norton Tips on How to Prevent Getting Infected*, NORTON BY SYMANTEC, https://us.norton.com/ransomware/article, https://perma.cc/7MZU-XYVU.

targeted to both the organization and individual, making scrutiny of the document and sender important to prevent exploitation."[49]

D. Personality and Psychology

[17] The customization of these programs is reflected in a variety of features that are now common to Ransomware schemes. For example, certain programs display multiple language options so "language is not a barrier to payment, [allowing] the user [to] access ransom instructions in English, French, German, Russian, Italian, Spanish, Portuguese, Japanese, Chinese and Arabic"[50] and making sure that the Ransomware "experience" is appropriately localized for the victim.[51] Once the Ransomware is downloaded, it disables the victim's machine "by disallowing execution of various programs," demanding ransom, and even "using local police images" –the program geo-locates the user's internet protocol address and associates that address with location-specific law enforcement decals and insignia deployed from a central command-and-control server.[52]

[18] In connection with this locality-based personalization, Ransomware may use psychological tactics to induce guilt or shame in

[49] *See* FED. BUREAU OF INVESTIGATION, *supra* note 45.

[50] Ramsey & Morse, *supra* note 23, at 5.

[51] *See* Azad Ali et al., *supra* note 16, at 62.

[52] O'Gorman & McDonald, *supra* note 19, at 5.

individual victims.[53] For example, ransom notes may include salacious details to frighten users, sometimes claiming that the victim has violated federal statutes and/or threatening imprisonment for alleged visits to websites "containing pornography, child pornography, zoophilia and child abuse."[54] These ransom notes are then spread throughout the computer's operating system, often propagating hundreds of copies on a given computer to ensure the user's attention is drawn to the threat.[55]

[19] Alternatively, "some versions of Ransomware are now designed to seek out the files on a victim's computer that are most likely to be precious, such as a large number of old photographs, for example, tax filings, or financial worksheets."[56] Other variants "just delete[] files instead of encrypting them."[57] Finally, some "variants display a countdown timer to the victim, threatening to delete the key/decryption tool if payment is not received before the timer reaches zero or, in other cases, increase the price of the ransom."[58]

---

[53] *See* Haley S. Edwards, *A Devastating Type of Hack Is Costing People Big Money*, TIME (Apr. 21, 2016), http://time.com/4303129/hackers-computer-ransom-ransomware/, https://perma.cc/AAQ3-52BB.

[54] O'Gorman & McDonald, *supra* note 19, at 2.

[55] *See* Ali et al., *supra* note 16, at 61–62.

[56] Edwards, *supra* note 53.

[57] Tom Spring, *Dirt Cheap Stampado Ransomware Sells on Dark Web for $39*, THREATPOST (July 14, 2016, 12:35 PM), https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/, https://perma.cc/A4HS-ZF3H.

[58] Largent, *supra* note 22.

[20] Even setting aside the nuances of these personal approaches, it is nearly impossible for security experts to keep pace with Ransomware advances generally, as "hackers are releasing over 100,000 new [R]ansomware variants daily,"[59] and "'evil genius' [R]ansomware ideas are 'coming out on a regular basis.'"[60] Perhaps even more challenging for law enforcement and security specialists, the level of technological expertise required to engineer a Ransomware attack has decreased significantly; at this point, deploying Ransomware is "relatively low budget, low stakes, and [doesn't] require much skill to pull off."[61] Indeed, in one instance, a recent drop in price to US$39 for Ransomware software concerned experts who believed "the low price coupled with its potency could trigger a wave of new infections."[62]

[21] Evolving with the times, recent Ransomware variants have focused on smartphones and other connected devices, including those that are a part of the "Internet of Things."[63] The first instances of "mobile-focused

[59] Pollack, *supra* note 14, at 5.

[60] Ricci Dipshan, *Danger Ahead: 3 New Ransomware Developments in 2016; From Hybrid Ransomware to Attacks on Mobile Devices and New Entrants in the Field, Experts Warn of a Difficult Year Ahead*, LAW TECH. NEWS (May 31, 2016).

[61] Edwards, *supra* note 53.

[62] Spring, *supra* note 57.

[63] *See, e.g.*, Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J. L. & TECH. 9, ¶ 1 (2016), http://jolt.richmond.edu/v22i3/article9.pdf, https://perma.cc/VSZ7-85LE.

Ransomware came out in 2013,"[64] buoyed in part "by the practice of users downloading pirated apps from unsanctioned app stores."[65] As noted by another commentator, "[R]ansomware criminals can achieve some profit from targeting any system: mobile devices, personal computers, industrial control systems, refrigerators, portable hard drives, etc. The majority of these devices are not secured in the slightest against a [R]ansomware threat."[66]

IV. THE BUSINESS OF RANSOMWARE

> You always wanted a Ransomware but never wanted two pay Hundreds of dollars for it? This list is for you!?? Stampado is a cheap and easy-to-manage ransomware, developed by me and my team. It's meant two be really easy-to-use. You'll not need a host. All you will need is an email account.[67]

[22] The mentality behind Ransomware seems to have deep-rooted cultural underpinnings, likened by some authors to medieval roadways that became host "to travelling footpads referred to as highwaymen."[68] Methodologically, the purveyors of Ransomware bear little resemblance to hackers "who attempt to exfiltrate or manipulate data where it is stored, processed, or in transmission;" instead, "ransomware criminals only

[64] *See* VAN DER MEULEN, *supra* note 8, at 45.

[65] Dipshan, *supra* note 60.

[66] *See* Scott & Spaniel, *supra* note 2, at 4.

[67] Spring, *supra* note 57.

[68] Scott & Spaniel, *supra* note 2, at 3.

attempt to prevent access to the data."[69] In short, Ransomware aims to disrupt.

[23] Ransomware differs from many other types of hacking on a number of levels. It has been called a "business model"[70] that has "quickly risen to dominance"[71] within the "cybercriminal market in the past few years"[72] and has "emerged as one of the most serious online threats facing businesses."[73]

[24] Often, a Ransomware attempt betrays the fact that its author "lack[s] the technical complexity to perform successful attacks;"[74] some versions have been described as lacking technical savvy, and others as "not very well developed" beginner-level efforts.[75] Perhaps because of a general lack of know-how, and Ransomware's reputation as offering "easier money than hacking into personal information to use for identity theft,"[76] a cottage industry has mushroomed. Certain criminals "now have

[69] *See id.* at 4.

[70] *See* Jon Neiditz, *Ransomware in Society and Practice*, PRACTISING LAW INST. 39, 41.

[71] *Id.*

[72] *Id.*

[73] Ben Rossen, *Ransomware – A Closer Look*, FED. TRADE COMM'N (Nov. 10, 2016, 11:05 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look, https://perma.cc/3HX4-NDE3.

[74] Kharraz, *supra* note 6, at 2.

[75] Dipshan, *supra* note 60.

the resources to hire professional developers to build increasingly sophisticated malware" on their behalf.[77] Providers, "usually based in Russia, Ukraine, Eastern Europe and China, have begun licensing what's known as 'exploit kits'—all-inclusive Ransomware apps—to individual hackers for a couple hundred dollars a week,"[78] or even "[US]$50 for a set period time of use,"[79] frequently taking a "cut of the profits from payouts."[80]

[25] Known as "Ransomware-as-a-service" (or RaaS), there are now "products, such as CerberRing, which provide[] less-tech savvy criminals a corridor into cybercrime, and yield[] criminal affiliates (often tasked with distributing the [R]ansomware) a healthy portion of the profits."[81] Interestingly enough, because Ransomware is such big business, some Ransomware enterprises actually offer "customer service which victims can contact to negotiate"[82] and similar structures that make both launching the attacks, and paying the ransoms, easier.[83]

---

[76] THOMPSON INFORMATION SERVICES, *Malware Attack Causes System Shutdown at Medstar*, 15 NO. 4 GUIDE MED. PRIVACY & HIPAA NEWSL. 2, at 1 (May 2016) [hereinafter *Malware Attack*]

[77] Rossen, s*upra* note 73.

[78] Edwards, *supra* note 53.

[79] Spring, *supra* note 57.

[80] Largent, *supra* note 22.

[81] *See Technical Intricacies of Ransomware and Safeguarding Strategies*, DIGITAL MOUNTAIN (Fall 2016) http://digitalmountain.com/enews/FALL_2016_Article2.pdf, https://perma.cc/QV3V-ESJQ.

[82] Pollack, *supra* note 14, at 14.

[26] Some commentators note that there is "some honour among thieves," where "hackers almost always honour their word and provide the encryption key to those who make timely online payments."[84] Others disagree, noting that a decision to pay does not consistently restore functionality, and "[t]he only reliable way to restore functionality is to remove the malware."[85] For many this is truly unfortunate, as "[t]he costs of downtime often exceed the cost of ransom."[86]

[27] Ransomware infrastructure has "begun to mimic the way modern software is developed: there are criminal engineers and manufacturers, retailers, and 'consumers'—[those] hackers on the lookout for the newest, most effective product."[87] In some cases, when a ransom is paid functionality may be restored but in an inconsistent manner (e.g., accounting data may be returned, but mapped drive data is not); in at least one of those cases, the victim determined that the "help" offered by the Ransomware attacker could instead lead to the loss of more data.[88]

---

[83] *See* Brian Krebs, *CryptoLocker Crew Ratchets Up the Ransom*, KREBS ON SECURITY (Nov. 6, 2013, 12:13 AM), http://krebsonsecurity.com/tag/cryptolocker-decryption-service/, https://perma.cc/7369-JSKT.

[84] Jardine, *supra* note 20, at 10.

[85] O'Gorman & McDonald, *supra* note 19, at 2.

[86] Pollack, *supra* note 14, at 5.

[87] Edwards, *supra* note 53.

[88] *See* Azad Ali et. al., *supra* note 16, at 64.

[28] Ransomware may be preferred by criminals because it cuts out the middle-man. [89] It bypasses many of the annoyances associated with hacking to steal data that then must be monetized. Where "intellectual property, or other sensitive information that is stolen outright....is often 'fenced' on the Dark Web, then the buyer has to turn it into a false identity that can be used to fraudulently obtain goods or services."[90] In contrast, Ransomware has victims who "pay the criminal directly, the payment happens within hours or days in untraceable currency, and there is no chain of custody to point to the criminals because the data stays on the victim's system the whole time."[91] Indeed, deploying Ransomware is especially convenient for criminals, as its operation "often means dealing not with a small group of fellow criminals, but instead with a much larger population of lay users who are unlikely to disappear behind bars."[92]

V. RANSOMWARE'S DIRECT IMPACT

[29] In some cases, specific industries have been singled out as popular targets. For instance, at the time of writing, "[R]ansomware is the

[89] *See* SENTINEL ONE, *Ransomware is Here: What You Can Do About It?* 2, https://go.sentinelone.com/rs/327-MNM-087/images/Sentinel%20One_Ransomware%20is%20Here.pdf, https://perma.cc/3H46-QJCB.

[90] Pollack, *supra* note 14, at 5.

[91] *Id*.

[92] Wolff, *supra* note 12.

dominant current information security threat to health care providers."[93] Ransomware may target "victims like healthcare providers whose complex independent networks and critical need for real-time information can make reliance on backups difficult and potentially life-threatening."[94] These types of targets ("hospitals in particular" but also "other firms heavily dependent on computers"[95]) tend to focus on paying off the attacker to make the problem go away, whereas other types of companies may be amenable to "resisting the attack and rebuilding entire systems."[96] If the demands are not met, in the most extreme examples, a victim might be "forced back into the 1980s: digital typewriters, notebooks, fax machines, post-it notes, paper checks and the like."[97] In the face of these challenges, many organizations and individuals simply pay. Some do so without fanfare, and experts claim it "would shock you [] how many companies have quietly gone ahead and paid for information to be returned."[98] Others, like PayPal, have made public the fact that they will pay for stolen data to protect their customers.[99]

[93] Neiditz, *supra* note 71, at 7 (citing Danny Palmer, *Ransomware is Now the Biggest Cybersecurity Threat*, ZDNET (May 6, 2016), http://www.zdnet.com/article/ransomware-is-now-the-top-cybersecurity-threat-warns-kaspersky/, https://perma.cc/84XM-57M3).

[94] *Id*. at 9.

[95] Merrion, *supra* note 4.

[96] *Id*.

[97] Largent, *supra* note 22.

[98] Wolff, *supra* note 12.

[99] *See* Sean Sposito, *PayPal, OthersBuy Stolen Data from Criminals to Protect Users*, SAN FRANCISCO CHRON. (Jan. 8, 2016),

[30] One commentator noted that attorneys increasingly are "targets of [R]ansomware;" in the past several years, a number of "large and small law firms in the United States and Canada have had their office computer systems compromised by [R]ansomware."[100] Some professionals "suspect that paying gets you listed on the Dark Web as an easy target, setting you up for more attacks."[101] At least in some cases, the FBI appears to agree.[102] Ransomware's effects are not just monetary, as the loss of the files themselves (or the cost of ransom) may be eclipsed by the loss of "client trust, relationships, and reputation."[103]

VI. RANSOMWARE'S INDIRECT IMPACT

[31] One commentator notes that Ransomware is an exception (and perhaps portends a wave of such exceptions) to the traditional "data

http://www.sfchronicle.com/business/article/PayPal-others-buy-stolen-data-from-criminals-to-6744699.php, https://perma.cc/XLE9-AX3Q.

[100] Daniel Crothers, *Cybersecurity for Lawyers – Part IV: Is Payment of Ransom in Your Budget?,* 63 THE GAVEL 24, 24 (2016).

[101] Pollack, *supra* note 14, at 11 (quoting unnamed consultant "D").

[102] *See* Mathew J. Schwartz, *Please Don't Pay Ransoms, FBI Urges,* DATA BREACH TODAY (May 4, 2016), http://www.databreachtoday.com/blogs/please-dont-pay-ransoms-fbi-urges-p-2120, https://perma.cc/8ZND-KM2J.

[103] *See* A.B.A., *Practical steps to thwart ransomware and other cyberbreaches*, YOURABA (Dec. 2016), http://www.americanbar.org/publications/youraba/2016/december-2016/be-prepared-to-thwart-ransomware-and-other-cyber-attacks.html, https://perma.cc/LFT2-UP9E.

security breach" concept with which we have all become familiar.[104] Whereas a traditional "breach" typically entails the acquisition of data, Ransomware allows wrongdoers to control, damage, and interrupt systems; deny access to data; and destroy or otherwise harm the data's integrity—all *without* actual acquisition of the data.[105]

[32] Although some contend that "no information is actually stolen during a [R]ansomware attack,"[106] others argue that falling victim to Ransomware "could also be considered a data breach, even though the data never leaves the victim's systems."[107]

[33] The issue of whether Ransomware constitutes a breach was raised at the 2016 Healthcare Compliance Association conference.[108] There, Iliana Peters of the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) "pointed out that HIPAA regulations define a data breach as 'impermissible acquisition, access, use or disclosure of PHI [protected health information](paper or electronic) which compromises the security or privacy of the PHI.'"[109] Additional HIPAA guidance from the OCR also notes that some Ransomware may

[104] *See* Neiditz, *supra* note 70, at 41.

[105] *See id*.

[106] Jardine, *supra* note 20, at 10-11.

[107] DOUG POLLACK, RANSOMWARE 101: WHAT TO DO WHEN YOUR DATA IS HELD HOSTAGE, 5 (2016) (ebook).

[108] *See id*.

[109] *Id*.

"exfiltrate" the data,[110] which further complicates a simple explanation for the mechanics of a Ransomware attack. The OCR also noted that "[h]ospitals and other healthcare providers hit by [R]ansomware attacks should notify affected individuals, the federal government and perhaps the news media unless there is a 'low probability' any personal health information was disclosed."[111] That "guidance makes clear that a [R]ansomware attack usually results in a 'breach' of healthcare information under the HIPAA Breach Notification Rule," noted OCR's Executive Director, Jocelyn Samuels.[112]

[34] In contrast, some argue that data breach notification statutes were implemented with a focus on informing citizens that their personal information may have been compromised, offering "valuable warnings to assist victims in protecting themselves" and otherwise corralling information that has been set loose in the outside world.[113] The July 2016 HHS guidance also indicates that the question of "whether notification is

[110] *See Fact Sheet: Ransomware and HIPAA*, DEPT. OF HEALTH & HUM. SERV., http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf, https://perma.cc/G6ZV-S87S (last visited Feb. 8, 2017).

[111] Paul Merrion, *HHS Clarifies When Ransomware Attacks Trigger HIPAA Notification*, CQ ROLL CALL, July 13, 2016, 2016 WL 3709987 [hereinafter *HHS Clarifies*].

[112] Jocelyn Samuels, *Your Money or Your PHI: New Guidance on Ransomware,* OPENHEALTH NEWS, July 11, 2016, http://www.openhealthnews.com/news-clipping/2016-07-11/your-money-or-your-phi-hhs-issues-new-guidance-ransomware, https://perma.cc/Q7P7-P8WL.

[113] John Neiditz & David Cox, *Beyond Breaches: Growing Issues In Information Security*, INTEGRO (2016), https://integrogroup.com/uploads/white_papers/06_16_Beyond-Breaches.pdf, https://perma.cc/U5EJ-SAC8.

required comes down to a 'fact-specific determination.'"[114] In some cases, a forensic investigation may provide evidence to support a company's conclusion that a ransomware attack did not expose any personal information, even if the incident resulted in a system shutdown or other functional difficulties. Many healthcare entities have reached this same conclusion under HIPAA.

VII. RESPONSE TO RANSOMWARE

[35] Although the following discussion examines conventional best practice approaches for dealing with Ransomware, but the preceding section should signal that there is no one-size-fits-all solution. As with many computer infections, a typical initial response to Ransomware may be to restart the computer in "safe mode" in an effort to disable a number of programs that might be causing issues.[115] In the case of Ransomware, however, this approach may backfire, allowing the malicious software to flourish by un-loading antivirus programs that otherwise may have stopped it.[116]

[36] The next step in the response protocol is for victims to identify which "strain" of Ransomware they are dealing with, and then determine whether an "applicable decryption method" may be readily available to

[114] *HHS Clarifies*, *supra* note 111.

[115] *See generally* Azad Ali et. al., *supra* note 16, at 66 (describing the authors' personal experience with ransomware mechanisms).

[116] *See id*.

help unlock or decrypt files.[117] Whether this approach will be successful depends on the sophistication of the Ransomware. Certain generic, readily available strains that are still freely disseminated among would-be hackers may be defeated with relative ease, and the fact that a given strain of Ransomware is still in circulation is not proof of its viability or effectiveness.[118] To give one example, "the makers of Jigsaw ransomware have continued their assault against victims despite the fact its encryption scheme has been defeated by security researchers."[119]

[37] If these initial efforts are unsuccessful, certain victims may be inclined to pay the ransom. Experts may caution against paying the ransom prematurely, but for many, a relatively paltry Ransomware demands (demands often range from US$200 to US$2,000) may be seen as "nuisance fee" more than anything else.[120] The "To Pay or Not to Pay"[121] characterization of a standard response to Ransomware is apt, though this decision-making process may mean waiting to decide until

[117] *See* Adam Alessandrini, *Ransomware Hostage Rescue Manual*, KNOWBE4 (2015) at 8, http://resources.idgenterprise.com/original/AST-0147692_Ransomware-Hostage-Rescue-Manual.pdf, https://perma.cc/KNS8-BT5N.

[118] *See id.* at 7.

[119] Tom Spring, *Dirt Cheap Stampado Ransomware Sells on Dark Web for $39*, THREATPOST, July 14, 2016, https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/, https://perma.cc/2LAV-63HE.

[120] *See* Crothers, *supra* note 100 at 24.

[121] *See* Scott & Spaniel, *supra* note 2, at 3.

after an initial deadline is extended.[122] Waiting may result in a doubling of the ransom[123] or even an exponential increase—up to US$20,000 in some instances.[124] And in some cases there really is no choice. As noted in a recent report, "[f]or variants of [R]ansomware that rely on types of strong asymmetric encryption that remain relatively unbreakable without the decryption key, victim response is sharply limited to pay[ing] the ransom or los[ing] the data. No security vendor or law enforcement authority can help victims recover from these attacks."[125]

[38] Paying a ransom may, therefore, make logical sense, given that "Ransomware attacks, especially those against individual users, only demand a few hundred dollars at most from the victim" and "[f]rom law enforcement's perspective, a home burglary results in greater loss than a singular [R]ansomware attack."[126] At least one commentator noted cynically that, because "[s]ecurity has always been a business decision, [s]ome companies would rather pay a lower fee for ransom than pay for the cost of having a robust security stance."[127] Others note that "to save

[122] *See* Ondrej Kehel, *Ransomware: To Pay or Not To Pay*, LEXISNEXIS, Aug. 16, 2016, https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2016/08/16/ransomware-to-pay-or-not-to-pay.aspx, https://perma.cc/V2JJ-YHPT.

[123] *See* Azad Ali et. al., *supra* note 16, at 64.

[124] *See* Jardine, *supra* note 20, at 10.

[125] Scott & Spaniel, *supra* note 2, at 4.

[126] *Id*. at 5.

[127] Michael Sutton, *Big Business Ransomware: A Lucrative Market in the Underground Economy*, DARKREADING, July 1, 2016, http://www.darkreading.com/vulnerabilities---

money, some organizations don't include all their important files in their backups, or don't run their backups often enough."[128]

[39] However, notwithstanding the low dollar value of most demands, taken in the aggregate, these attacks cost real money. "[L]osses for victims from a single strain of the CryptoWall malware were close to $18 million,"[129] and another Ransomware attacker earned roughly $1 million.[130] Given that "nearly 30 percent of CryptoLocker and CryptoWall victims pay the ransom,"[131] there remains the concern that "hackers [will]

threats/big-business-ransomware-a-lucrative-market-in-the-underground-economy/a/d-id/1326144, https://perma.cc/3GUA-Z8UE.

[128] Maria Korolov, *Will Your Backups Protect You Against Ransomware?*, CSO (May 31, 2016) http://www.csoonline.com/article/3075385/backup-recovery/will-your-backups-protect-you-against-ransomware.html, https://perma.cc/LM56-ZMY5.

[129] Doug Pollack, *How Ransomware Could Hold Your Business Hostage*, IDEXERTS, Apr. 29, 2016, https://www2.idexpertscorp.com/blog/single/how-ransomware-could-hold-your-business-hostage, https://perma.cc/VK9J-B4J5.

.

[130] *See* Haley Sweetland Edwards, *A Devastating Type of Hack is Costing People Big Money*, TIME (Apr. 21, 2016), http://time.com/4303129/hackers-computer-ransom-ransomware/, https://perma.cc/VS8M-CDZW.

[131] Nicole van der Meulen et. al., *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, EUROPEAN PARLIAMENT at 35 (2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf, https://perma.cc/242L-VJTM (citing Richard Pinson, *Computer threat: Cryptolocker virus is ransomware*, NASHVILLE BUSINESS JOURNAL, Aug. 10, 2015 http://www.bizjournals.com/nashville/blog/2015/08/computer-threatcryptolocker-virus-is-ransomware.html, https://perma.cc/69SN-RD2Y (last visited Oct. 12, 2015)).

continue to ask for higher and higher ransoms."[132] Early payment schemes involved payment through "an SMS text message or regular call to a premium rate number" where such charges could be "as high as $460."[133] A second iteration of payment schemes moved to prepaid electronic payment systems such as Paysafecard, Ukash, and Moneypak, where Ransomware victims are required to purchase special PIN numbers.[134]

[40] Regardless of whether it makes business sense for victims to pay a victim to pay a given ransom, victims must also consider whether they *may* pay. Unhelpfully, regulatory authorities have expressed varying opinions on that point and have not provided definitive guidance as to whether victims should pay. The FTC notes that "[l]aw enforcement doesn't recommend paying the ransom" while warning that "it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back."[135] In contrast, Joseph Bonavolonta, the head of the FBI's Cyberand Counterintelligence Program in 2015, stated that the FBI "often advise[s] people just to pay the ransom."[136] Rick

[132] Michael Sutton, *Big Business Ransomware: A Lucrative Market in the Underground Economy*, DARKREADING (July 1, 2016 11:20 AM) http://www.darkreading.com/vulnerabilities---threats/big-business-ransomware-a-lucrative-market-in-the-underground-economy/a/d-id/1326144, https://perma.cc/63LK-7855.

[133] O'Gorman & McDonald, *supra* note 19, at 4.

[134] *See id*.

[135] Ben Rossen, *How to Defend Against Ransomware*, FEDERAL TRADE COMMISSION, Nov. 10, 2016, https://www.consumer.ftc.gov/blog/how-defend-against-ransomware, https://perma.cc/7VVN-WG2L.

[136] Scott & Spaniel, *supra* note 2, at 5.

Kam, president of ID Experts, also opined that "it is often easier just to pay the ransom than to do without the data."[137] Anecdotally, the authors have heard a wide range of opinions with respect to whether paying the ransom is a sound approach. Indeed, given the exploding number of attacks and diversity of outcomes, it is increasingly challenging to offer affected companies or individuals clear recommendations on how to assess the likelihood of success when it comes to answering a Ransomware demand.

[41] In short, law enforcement guidance may boil down to a "[l]ook, we can't help you,"[138] response, even if some agencies indicate that "[m]ost…including law enforcement don't condone paying the ransom,"[139]and "[m]ost security vendors advise the public (who are not yet victims) to never pay the ransom and to focus on mitigation efforts instead."[140] The FBI, however, appears to be seeking "public-private partnerships," as the Bureau utilizes notifications it receives regarding Ransomware and other threats in an overall effort to build up more comprehensive forms of defense and prevention.[141]

VIII. PRACTICAL AND LEGAL CONSIDERATIONS

[137] *Malware Attack*, *supra* note 76, at 1.

[138] Edwards, *supra* note 54.

[139] Rossen, *supra* note 73.

[140] Scott & Spaniel, *supra* note 2, at 5.

[141] Merrion, *supra* note 4.

[42] In almost all cases, Ransomware ransom demands must be paid in a digital currency such as Bitcoin.[142] Bitcoin emerged in 2009[143] and has had unpredictable and profound effects, particularly with respect to the underground economy.[144] For many victims, receipt of a Bitcoin ransom demand is the first time they are exposed to the term, and very few have the necessary resources available to pay such a demand in a timely manner. Others who are aware of the threat—or who have a need for Bitcoin as a payment method for unrelated reasons—may "stockpile [B]itcoins in order to pay off cyber criminals who threaten to bring down their critical IT systems."[145] To provide one public example, Hollywood

[142] *See* Azad Ali et. al., *supra* note 16, at 63.

[143] *See* Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun, *Bitter to better—how to make bitcoin a better currency*, International Conference on Financial Cryptography and Data Security, pp. 399-414. Springer Berlin Heidelberg (2012). *See also, Who is Satoshi Nakamoto*, CoinDesk, Feb. 19, 2016, http://www.coindesk.com/information/who-is-satoshi-nakamoto/, https://perma.cc/6JP8-NLRU.

[144] *See generally* Andy Greenberg, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, FORBES (Sept. 5, 2013), https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/#3cd73b93adf7, https://perma.cc/ZEA2-JPDR (explaining why Bitcoin is used for underground transactions).

[145] Jamie Doward, *City Banks Plan to Hoard Bitcoins to Help Them Pay Cyber Ransoms*, THE GUARDIAN, Oct. 22, 2016, https://www.theguardian.com/technology/2016/oct/22/city-banks-plan-to-hoard-bitcoins-to-help-them-pay-cyber-ransoms, https://perma.cc/PG4H-2TVL.

Presbyterian Medical Center recently paid $17,000 in Bitcoin in response to a ransom demand.[146]

[43] Unfortunately, making a Bitcoin payment is not a straightforward prospect for most organizations. The process is rife with potential legal and practical problems, because the company will likely "need to buy Bitcoins from an online exchange. The exchange will require you to supply a bank account or debit card number to fund the transaction, which creates an immediate risk because Bitcoin exchanges are notorious for being hacked."[147]

[44] To add another layer of complexity, in its March 25, 2014 Virtual Currency Guide, the United States Internal Revenue Service declared that a virtual currency such as Bitcoin is considered property, not currency, and thus its use is a taxable event.[148] Further, "[a] payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property."[149] "The basis of virtual

[146] *See* Robert Mclean, *Hospital Pays Bitcoin Ransom After Malware Attack*, CNN, Feb. 17, 2016, http://money.cnn.com/2016/02/17/technology/hospital-bitcoin-ransom/, https://perma.cc/78FT-GUMM.

[147] Doug Pollack, *Tradable, Untraceable, Sometimes Unavoidable: The Business of Bitcoin*, ID EXPERTS, June 20, 2016, https://www2.idexpertscorp.com/blog/single/tradable-untraceable-sometimes-unavoidable-the-business-of-bitcoin, https://perma.cc/VM4R-R2Y4.

[148] *See* Ramsey & Morse, *supra* note 23, at 7.

[149] *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property of U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, IRS, Mar. 25, 2014, https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance, https://perma.cc/JP66-2H87.

currency…is the fair market value of the virtual currency in U.S. dollars as of the date of receipt", which means that a taxpayer could end up with a taxable gain or loss, depending on the net outcome.[150]

[45] Concurrently, Ransomware perpetrators who demand Bitcoin ransoms run the risk of also violating financial services laws and regulations prohibiting the operation of unlicensed banks—or at least causing such violations.[151] "[T]he U.S. Attorney for the Southern District of New York issued a press release concerning [a] criminal prosecution against Anthony R. Murgio and Yuri Lebedev for running an unlicensed Bitcoin exchange used by victims of CryptoWall [R]ansomware to pay ransoms [to their attackers] via TOR (The Onion Router)."[152] The two men were accused of having operated Coin.mx, a Bitcoin exchange service, in violation of federal anti-money laundering laws and regulations and that, "in doing so, they knowingly exchanged cash for people whom they believed may be engaging in criminal activity."[153] It is alleged that, in total, "between approximately October 2013 and January 2015, Coin.mx exchanged at least [US]$1.8 million for Bitcoins on behalf of tens of

[150] I.R.S. Notice 2014-21 at 3, Mar. 25, 2014, https://www.irs.gov/irb/2014-16_IRB/ar12.html, https://perma.cc/MX9U-WCWN.

[151] *See* Ramsey & Morse, *supra* note 23, at 5.

[152] *Id.*

[153] *Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange*, FBI, July 21, 2015, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/manhattan-u.s.-attorney-announces-charges-against-two-florida-men-for-operating-an-underground-bitcoin-exchange, https://perma.cc/Z85B-LT87.

thousands of customers."[154] In addition, during this time, Murgio allegedly "transferred hundreds of thousands of dollars to bank accounts in Cyprus, Hong Kong, and Eastern Europe, and received hundreds of thousands of dollars from bank accounts in Cyprus and the British Virgin Islands, in furtherance of the operations of his unlawful business."[155] In doing so, the operators of Coin.mx were said to have "knowingly enabled the criminals responsible for those attacks to receive the proceeds of their crimes" thereby violating federal anti-money laundering laws, because they "never filed any suspicious activity reports regarding any of the transactions."[156]

[46] As part of its efforts to combat global terrorism, the U.S. actively works to prevent terrorists from accessing and using its financial system.[157] Payments to criminals using Ransomware to hold data hostage may run afoul of banking laws and policies as well as related statutes and regulations. Individuals and organizations choosing to make ransom payments to end Ransomware attacks could be subject to international sanctions programs administered in the U.S. by the Office of Foreign Assets Control (OFAC), though such enforcement has not yet been tested as of this writing. Under these sanctions programs, ransom payments to certain entities are illegal, as noted by Samuel Cutler:

---

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *See* David S. Cohen, *Kidnapping for Ransom: The Growing Terrorist Financing Challenge*, COUNCIL ON FOREIGN RELATIONS, Oct. 5, 2012, http://www.cfr.org/terrorist-financing/remarks-treasury-under-secretary-cohenkidnapping-ransom-growing-terrorist-financing-challenge/p29376, https://perma.cc/6X6P-NKHJ.

> It's important to begin from the fact that ransom payments to [Foreign Terrorist Organizations] FTOs or Specially Designated Global Terrorists ("SDGTs") identified by [OFAC] are illegal under U.S. law. Monetary contributions to FTOs are considered material support under 18 U.S.C. 2339B, while transfers to SDGTs are violations of economic sanctions imposed pursuant to the International Emergency Economic Powers Act ("IEEPA").
>
> Furthermore, as the Financial Action Task Force ("FATF") notes in discussion of ransom payments to the Islamic State in Iraq and the Levant ("ISIL"), "[U.N. Security Council] Resolution 2161 applies to both direct payments and indirect payments through multiple intermediaries, of ransoms to groups or individuals on the Al-Qaida Sanctions List. These restrictions apply not only to the ultimate payer of the ransom, but also to the parties that may mediate such transfers, including insurance companies, consultancies, and any other financial facilitators."[158]

[47] So far, the act of paying to remove Ransomware has not been prosecuted under 18 U.S.C. 2339B[159] or IEEPA, but U.S. law enforcement officials encourage victims of Ransomware to report the attacks and are actively seeking to uncover the people behind these attacks. It remains to

[158] Samuel Cutler, *Could the Administration's New Hostage Policy Leave Banks Vulnerable?*, SANCTION LAW, June 24, 2015, http://sanctionlaw.com/could-the-administrations-new-hostage-policy-leave-banks-vulnerable/, https://perma.cc/5B9Z-KX23.

[159] *See* 18 U.S.C. § 2339B (2012).

be seen whether a substantial Ransomware-related payment that was determined to have been made to a person or group on an OFAC list may result in legal action.[160]

[48] In addition, an Executive Order issued in April 2015 "expand[s] the [existing] sanctions regime to block the property and interests of persons engaging in 'significant malicious cyber-enabled activities'" outside of the U.S. that constitute a significant threat to the country as "determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State."[161] Activities deemed significant "have the purpose or effect of" seriously harming or compromising critical infrastructure; disrupting the availability of computers and networks; and misappropriating funds, trade secrets, personal identifiers, or financial information.[162] Moreover, "[t]he blocking extends to assets of those who 'have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity [proscribed by the order] or any person whose property and interests are blocked pursuant to this order,'" which could implicate individuals and institutions that choose to pay to remove Ransomware.[163] Ransomware disrupts the availability of computers and networks, has the ability to compromise critical infrastructure, and may

[160] *See id*.

[161] Ramsey & Morse, *supra* note 23, at 14.

[162] *See* Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015).

[163] Ramsey & Morse, *supra* note 23, at 14 (quoting Exec. Order No. 13,694, 80 Fed. Reg. at 18078).

allow for the misappropriation of information; these and other risks are among the considerations presented in the Order.[164]

[49] In addition, the U.S. government's hostage policy may be instructive in determining whether a Ransomware payment is likely to be prosecuted. The government itself will not pay ransoms to release human hostages, but the relevant policy explicitly states that families will not be prosecuted for paying ransoms in exchange for hostages, even if these payments are made to FTOs or other individuals or groups on the government's sanctions lists.[165] Former President Obama noted that "no family of an American hostage has ever been prosecuted for paying a ransom for the return of their loved ones."[166] Whether that U.S. policy would extend to *photos* of an individual's loved ones held hostage by Ransomware is an entirely different question—one that may well test the limits of the government's humanitarian leniency in this regard.

---

[164] *See id*.

[165] *See* Cutler, *supra* note 158; *see also Statement by the President on the U.S. Government's Hostage Policy Review*, THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY, June 24, 2015, https://www.whitehouse.gov/the-press-office/2015/06/24/statement-president-us-governments-hostage-policy-review, https://perma.cc/W5J4-UNFK ("[T]he United States government will not make concessions, such as paying ransom, to terrorist groups holding American hostages…. At the same time, we are clarifying that our policy does not prevent communication with hostage-takers – by our government, the families of hostages, or third parties who help these families").

[166] *See Statement by the President on the U.S. Government's Hostage Policy Review*, *supra* note 165.

[50] Current U.S. hostage policy also offers no exemption from prosecution for organizations making or facilitating ransom payments.[167] The FBI notes in its Ransomware guidance that "by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."[168] Moreover, intermediaries cannot be used to avoid OFAC sanctions, which include freezing assets, forfeiture of assets, preventing payment transfers, fines, and imprisonment.[169] In Ransomware attacks, it may be impossible to ascertain who exactly is holding the data hostage, which in turn prevents the victim from determining in advance whether a ransom payment could result in sanctions for the organization.

[51] Ultimately, it seems unlikely that individuals will be penalized for making small payments to regain access to personal data affected by Ransomware; enforcement is challenging on a practical level, as the anonymity of virtual currencies makes it difficult—if not impossible—to know whether payments are going to individuals or groups on sanctions lists.[170] Large organizations considering whether to pay higher amounts to

[167] *See, e.g.*, *Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange*, *supra* note 153. DOUBLE CHECK THIS TO SEE IF ACTUALY 18 USC 2339

[168] *Incidents of Ransomware on the Rise: Protect Yourself and Your Organization,* FBI, April 29, 2016, https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise, https://perma.cc/83FC-G2W8 (citing Federal Bureau of Investigation Cyber Division Assistant Director James Trainor).

[169] *See OFAC FAQs: Sanctions Compliance*, U.S. DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx, https://perma.cc/2ACP-XZ7V (last visited Mar. 31, 2017).

[170] *See* Jardine, *supra* note 20, at 11.

meet demands from Ransomware attackers may face a more aggressive enforcement landscape. In some cases, organizations have engaged third parties to pay virtual currency ransom demands on their behalf. Ransomware payoffs and other hacking-related expenses may be funneled through intermediaries that "are often part of a larger contract for countersurveillance work, ensuring corporate accounting departments don't need to green-light individual black market buys."[171] With respect to the concept of paying ransom generally, it is worth considering the court's ruling in *United States v. Kozeny*,[172] in which the "United States District Court for the Southern District of New York [found] that only extortion or duress under the threat of *imminent physical harm* would excuse[] the conduct" (emphasis added).[173] It is difficult to imagine extending that line of reasoning to include threats to important documents or photos, especially given that industry best practices for business continuity include maintaining robust backups that would protect against just this threat.[174]

[52] As noted by some practitioners,[175] counsel's advice on preventing and responding to Ransomware attacks may implicate Model Rule 1.1 –

---

[171] Sposito, *supra* note 99.

[172] *See* United States v. Kozeny, 582 F. Supp. 2d 535, 540 (S.D.N.Y. 2008).

[173] Ramsey & Morse, *supra* note 23, at 19 (emphasis added).

[174] *See* Korolov, *supra* note 128.

[175] *See, e.g.*, Ivan Hemmans & David G. Ries, *Cybersecurity: Ethically Protecting Your Confidential Data in a Breach-A-Day World* (PowerPoint), at slides 18–21, April 27, 2016, http://www.americanbar.org/content/dam/aba/multimedia/cle/materials/2016/04/ce1604lpi.authcheckdam.pdf, https://perma.cc/V4T7-TAFT.

Competence, as amended by Comment 8, where "…a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…"[176] Although the recent explosion in Ransomware attacks is a relatively new phenomenon, there is no shortage of resources lawyers can use to become familiar with the threats posed by Ransomware and, consequently, to their clients' data. For example, the FBI has issued guidance that provides "key areas to focus on with Ransomware [such as] prevention, business continuity, and remediation."[177]

[53] With respect to potential regulatory enforcement, the FTC has warned that "a company's failure to update its systems and patch vulnerabilities known to be exploited by Ransomware could violate Section 5 of the FTC Act."[178] In addition, the Gramm-Leach-Bliley Act (GLBA) includes requirements concerning the disclosure by financial institutions of fraudulent access to customer information.[179] The GLBA

---

[176] *Comment on Rule 1.1*, AMERICAN BAR ASSOCIATION: THE CENTER FOR PROFESSIONAL RESPONSIBILITY, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html, https://perma.cc/GC6Q-4FN6 (last visited Feb. 12, 2017).

[177] *FBI Internet Crime Complaints*, FLORIDA ATLANTIC UNIVERSITY, http://www.fau.edu/police/images/FBI%20Internet%20Crime%20Complaints.pdf, https://perma.cc/5LLL-JGCE (last visited Feb. 12, 2017); *see also Incidents of Ransomware on the Rise: Protect Yourself and Your Organization*, *supra* note 168.

[178] Rossen, *supra* note 73.

[179] *See* 15 U.S.C. § 6803; *see also Ransomware – Legal Liability and Enforcement*, FALL 2016 E-NEWSLETTER (Digital Mountain, Santa Clara, C.A.), Oct. 24, 2016,

Safeguards Rule may be used "in conjunction with the FTC's Section 5 authority to bring actions against financial institutions that fail to properly protect consumer financial information."[180] Covered Entities under HIPAA are themselves subject to the Security Rule which, among a myriad of requirements to safeguard patient data, obligates Covered Entities to implement a data backup plan.[181] HIPAA compliance guides indicate that HIPAA security requirements extend to Ransomware, noting "...the possibility of a [R]ansomware attack must now be covered in any risk assessment."[182]

[54] Ransomware attacks also create eDiscovery conundrums. Ransomware as an application has been considered in a number of cases, including with respect to assessing a defendant's behavior to determine whether parole was violated,[183] and in an arbitration regarding the ownership of a domain name.[184] Given the potential for increasingly complex conflicts in this space, practitioners should consider the

http://digitalmountain.com/enews/FALL_2016_Article3.pdf, https://perma.cc/7YWZ-C3GP.

[180] *Ransomware – Legal Liability and Enforcement*, *supra* note 179.

[181] *Fact Sheet: Ransomware and HIPAA*, *supra* note 110.

[182] *Malware Attack*, *supra* note 76 (quoting John Parmigiani, HIPAA consultant and editorial advisory board member).

[183] *See, e.g.*, United States v. Haymond, No. 08-CR-201-TCK, 2016 WL 4094886, at *2 (N.D. Okla. Aug. 2, 2016).

[184] *See* Virginia College Savings Plan v. Zhouda, 2016 WL 5920046 (UDRP-ARB Dec), at *2–3 (Lowry, Arb.).

implications of Ransomware on eDiscovery across a variety of scenarios. These include situations in which Ransomware is the source of a given dispute, as well as when Ransomware becomes a complicating factor in the eDiscovery process.[185]

[55] Although eDiscovery has not been directly addressed in published decisions that contain a Ransomware element, the duty to preserve remains inviolate.[186] If a matter involves Ransomware, and whether that matter affects the data itself or has secondary implications with respect to the data's unavailability (such as when a hospital is attacked and patients are rerouted to other locations),[187] eDiscovery considerations should be front-of-mind for practitioners. Not only will claims or defenses associated with the Ransomware attack necessarily implicate the technology used, the practices that may have enabled (or failed to prevent) the attack (e.g., the infection vector, the data affected, or the target's backup environment) all may be relevant to the case, thus subject to discovery and requiring preservation.

[56] Yet another potential risk concerns the possibility that Ransomware could negatively impact eDiscovery collection, preservation, and later discovery efforts. The data preserved by eDiscovery collections

[185] *See generally* Ed Silverstein, *Law Firm Among the Latest Victims of Ransomware Attack*, LAW TECHNOLOGY NEWS, Mar. 11, 2015, www.legaltechnews.com/id=1202720266972/Law-Firm-Among-the-Latest-Victims-of-Ransomware-Attack, https://perma.cc/4QVA-3Z4B (detailing a law firm's recent ransomware attack).

[186] *See* Univ. of Montreal Pension Plan v. Bank of Am. Sec., LLC, 685 F. Supp. 2d 456, 462 (S.D.N.Y. 2010).

[187] *See* Korolov, *supra* note 128.

often includes highly refined sets of important, often "entirely new stores of extraordinarily sensitive information"[188] that are retained for legal hold purposes regardless of the company's standard data retention policies and information governance practices.[189] As discussed above, law firms have become a lucrative target for criminals using Ransomware;[190] among other valuable data sources, information preserved pursuant to litigation holds often is maintained by law firms that are representing multiple companies in a variety of matters. Law firms and other organizations—including vendors that provide preservation-related services—that have custody of these eDiscovery data sets should be cognizant of the risks created by atypical retention practices. These data sets are no less susceptible to Ransomware than their "standard" counterparts—and may even be more attractive targets, given the one-off nature of eDiscovery collections as well as the highly sensitive data they contain. Further, Ransomware may "preserve" data in a sense, but the data cannot be made available for production or may not exist in a usable format, which can add to the eDiscovery conundrums noted above.

---

[188] James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, *Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, e-Discovery, and Information Governance into Due Diligence Practices*, 21 RICH J.L. & TECH 5, ¶ 36 (2015), http://jolt.richmond.edu/v21i2/article5.pdf, https://perma.cc/4KBL-2GZ6.

[189] This is often a mandatory "exception" in many Records and Information Management and Information Governance policies. *See* Vicki Miller Luoma, *Computer Forensics and Electronic Discovery: The New Management Challenge*, 25 COMPUTERS & SECURITY 91, 96 (2006) (When creating an "electronic document retention and deletion policy . . . [a]ny such policy must retain the flexibility to implement litigation holds by suspending routine document deletion" in the face of a reasonable anticipation of litigation).

[190] *See* Crothers, *supra* note 100.

IX. RANSOMWARE'S FUTURE

[57] Ransomware appears poised to evolve along the same lines as many other non-criminal programming efforts, increasingly adopting the aesthetic and practicality of popular software instances that rely on a modular design, allowing criminals to "use certain functions as-needed," and offering "much better efficiency" and the "ability to switch tactics as required in the event one method is discovered or is found to be ineffective."[191] This approach would retain certain core elements associated with functional, successful Ransomware variants in play while remaining nimble enough to affect new Internet of Things and mobile device usage.

[58] For example, replacing the usual "command and control" center and related Deep- or Dark-Web business model, future Ransomware might "simply transmit a beacon with a GUID (globally unique identifier) to a Command and Control domain, trying to reach this domain through common protocols/services…to transmit this data."[192] That is, Ransomware applications will be streamlined to suit a market seeking self-service options, exchanging a bespoke process for one that is both easier to replicate on a mass scale and cheaper to produce and distribute.[193]

[191] *Ransomware: Past, Present, and Future*, *supra* note 22.

[192] *See id*.

[193] Tom Spring, *Dirt Cheap Stampado Ransomware Sells on Dark Web for $39*, THREATPOST (July 14, 2016, 12:35 PM), https://threatpost.com/dirt-cheap-stampado-ransomware-sells-on-dark-web-for-39/119284/, https://perma.cc/5FLX-GBPM.

[59] As noted above, the volume and scope of attacks has expanded as demographics and usage patterns have shifted more and more Ransomware activity onto mobile and Internet of Things devices.[194] In addition, the software and strategy underlying Ransomware attacks has adapted to evade common protective measures; since good backups often are the best defense against serious damage in the event of an attack, newer Ransomware variations have been built to go after those backups as well, destroying "all Shadow Copy and restore point data on Windows systems."[195] Ransomware is being developed to target not only a given piece of hardware, but also the device's local and virtual environment, in an attempt to outwit the efforts of potential victims by guessing at where they might back up their data and undermining those preventative or responsive measures. Future Ransomware may well exploit would-be victims' digital networking or social connections, using information gleaned from online posts to identify additional targets who may value the same types of data and thus be willing to pay the same types of ransoms to secure its release.

[60] Although individuals will no doubt continue to fall victim to Ransomware, the trend seems to be toward attacks carried out on a more ambitious scale. Criminals are said to be "shying away from random attacks," shifting from a focus on individuals and "expanding [further] into the corporate world" where victims are more likely to have the financial wherewithal to pay larger sums.[196] In short, an "individual might

[194] *See* Ben Dickson, *What makes IoT ransomware a different and more dangerous threat?*, TECH CRUNCH, Oct. 2, 2016, https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/, https://perma.cc/8VEP-HUK4.

[195] Korolov, *supra* note 128.

[196] Sutton, *supra* note 127.

be limited to a [US] $500 ransom, but how about a manufacturer or a hedge fund?"[197] Criminals can leverage knowledge gained through experience in the ransom marketplace to seek out specific opportunities, determining, for example, that an average person's photos are worth $X; an investment manager's emails and personal diary are worth $Y; and a hedge fund's proprietary formulas, representing "need-to-know" intelligence that is jealously guarded, are worth $Z. Adept attackers have already demonstrated their ability to exploit victim psychology in the abstract; laser-like, focused shakedowns may be the next horizon for Ransomware attacks.

[61] In addition to diversified attack methodology, the potential *impacts* of Ransomware attacks are evolving. Beyond the hijacking or theft of stored financial records or customer files, targeting connected technology has the potential to wreak physical, "real life" havoc.[198] In the case of the Hollywood Presbyterian Medical Center Ransomware attack, for example, in addition to "forcing staff to go back to paper records and fax machines," the data loss may have impacted care as "emergency patients were diverted to other hospitals."[199] As we continue to rely more heavily on connected devices, it is not difficult to see how these types of disruptions

[197] *Id*.

[198] *See* Brian Buntz, *The 10 Most Vulnerable IoT Security Targets*, INTERNET OF THINGS INSTITUTE, July 27, 2016, http://www.ioti.com/security/10-most-vulnerable-iot-security-targets?NL=IOT-001UBER&Issue=IOT-001UBER_20160804_IOT-001UBER_796&sfvc4enews=42&cl=article_7&utm_rid=CPG03000004380699&utm_campaign=13637&utm_medium=email&elq2=6a8551b97117440a8d6f316007c6c548, https://perma.cc/8UH5-QPVT.

[199] Korolov, *supra* note 128.

could create serious problems across multiple industry sectors—the incipient arrival of driverless cars, for example, represents a potentially vulnerable technology that could be exploited for profit by data hostage-takers. An instance of Ransomware may be localized, but its effects can extend much further afield. Cars without accessible data could be paralyzed, regardless of whether they are in motion at the time the attack begins. Picture the movie *Speed*, replacing Sandra Bullock at the helm of a passenger-laden bus with a driverless car heading toward a cliff, doomed to disaster unless a ransom is paid.[200] Likewise, many hospital treatments rely on accurate patient data at critical moments. How much would an individual pay to ensure her blood type is communicated correctly or that his medical history warns doctors of possible drug interactions? If a patient were to die under such circumstances, how would a court assess liability for a failure either to prevent the Ransomware attack, or to pay the ransom promptly?

X. CONCLUSION

> "[Ransomware] is a volume business. It's simple, relatively anonymous and fast. Some people will pay, some will not pay, so what. With a wide enough set of targets there is enough upside for these types of attacks to generate a steady revenue stream."[201]

[200] *See generally* SPEED (Twentieth Century Fox Film Corp. 1994) (a film in which a police officer must drive a bus above 50 miles per hour in order to prevent a bomb from exploding on the bus).

[201] *Raynham Remains Offline in Computer Virus Mystery*, WICKED LOCAL (Mar. 11, 2016, 5:30 PM), http://www.wickedlocal.com/news/20160311/raynham-remains-offline-in-computer-virus-mystery, https://perma.cc/BWW8-J9DF (quoting Brian Contos, ICIT Fellow and VP & Chief Sec. Strategist at Securonix).

[62] Grey areas abound, but thoughtful preparation is the best defense; both to avoid a Ransomware attack in the first place, and to manage the issues that may arise when an attack occurs. Practitioners should not only be knowledgeable about Ransomware, which includes understanding Ransomware's operation, effects, and ramifications, but also vigilant in following the latest trends and tracking the ever-evolving threats. Ransomware is not going anywhere, and while the meteoric rise and spread of Ransomware has been startling as a singular issue, it also serves as a clear warning of things to come. There is still plenty of room for innovation and tremendous incentives for criminals to pursue these opportunities. In a marketplace flooded with stolen credit card numbers and digital credentials, selling ill-gotten personal information to identity thieves has become both more cumbersome and less lucrative than holding data hostage and demanding a ransom from its owner.[202]

[63] Given this environment, practitioners should take a proactive approach to understanding Ransomware, not only to counsel clients effectively, but also to safeguard their own sensitive data, both professional and personal. Such understanding demands a working knowledge of digital currencies and ransom payment options, although there is some debate as to whether employing intermediaries[203] may help address that particular challenge.[204] Regardless, the key will be education and vigilance to guide strategic responses to Ransomware incidents. In

---

[202] *See* Wolff, *supra* note 12.

[203] *See* Sposito, *supra* note 99.

[204] *See* Cutler, *supra* note 158.

addition to taking steps to *prevent* Ransomware attacks, practitioners must prepare to *respond* as effectively and efficiently as possible to this ever-evolving threat.[205]

[205] *See Practical Steps to Thwart Ransomware and Other Cyberbreaches*, YOUR ABA, Dec. 2016, http://www.americanbar.org/publications/youraba/2016/december-2016/be-prepared-to-thwart-ransomware-and-other-cyber-attacks.html, https://perma.cc/5RX3-WWJG.