Tennessee Law Review

Volume 86
Issue 2 *Winter 2019*

Article 6

2019

WANNACRY, RANSOMWARE, AND THE EMERGING THREAT TO CORPORATIONS

Lawrence J. Trautman

Peter C. Ormerod

WANNACRY, RANSOMWARE, AND THE EMERGING THREAT TO CORPORATIONS

LAWRENCE J. TRAUTMAN*
PETER C. ORMEROD**

The WannaCry ransomware attack began on May 12, 2017, and is unprecedented in scale—quickly impacting nearly a quarter-million computers in over 150 countries. The WannaCry virus exploits a vulnerability to Microsoft Windows that was originally developed by the U.S. National Security Agency and operates by encrypting a victim's data and demanding payment of a ransom in exchange for data recovery. Security experts have indicated that a North Korea-linked group of hackers—who have also been implicated in cyberattacks against Sony Pictures in 2014, the Bangladeshi Central Bank in 2016, and Polish banks in February 2017—is behind the attack.

Ransomware threatens institutions worldwide, but the risks for businesses are starker—potentially catastrophic. This Article provides corporate executives with much of what they need to know about the evolving threats of malware and ransomware like Cryptolocker, Kelihos Botnet, Locky, Nymain, Petya, NotPetya, and WannaCry. First, we provide a brief definition and history of ransomware. Second, we look at the history of hospitals as ransomware targets. Third, we offer a description of the WannaCry virus, what is known about its development, method of action, and those who are believed to have deployed it; in this section, we also discuss methods to defend against this particular virus. Fourth, we discuss the Petya and NotPetya attacks. Fifth is a discussion of municipal ransomware attacks. Sixth, we review the myriad and unique risks that ransomware poses for corporations—including expected refinements of the technique, such as to effect corporate sabotage. Seventh, we discuss the duties and responsibilities of corporate directors and the Ormerod-Trautman data security economic model. Eighth and finally, we review the current cybersecurity legal landscape with a particular focus on corporate best practices and how business executives protect themselves against cybersecurity-related liability. We believe this Article contributes to the sparse existing literature about ransomware and related cyber threats posed to corporate boards and management.

INTRODUCTION

The WannaCry[1] ransomware attack was a global cyberattack that began on May 12, 2017, and its scale was unprecedented—quickly impacting more than 200,000 computers in over 150 countries.[2] In general terms, transnational crime syndicates "are adapting their business models by using so-called 'ransomware' to gain control over computer networks and then demand payment in exchange for restoration."[3] The WannaCry virus exploited a vulnerability in Microsoft Windows that was originally developed by the U.S. National Security Agency and operates by encrypting a victim's data and demanding payment of a ransom in exchange for data recovery.[4] Security experts have indicated that a North Korea-linked group of hackers—who have also been implicated in cyberattacks against Sony

---

* BA, The American University; MBA, The George Washington University; JD, Oklahoma City University School of Law. Mr. Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University. He may be contacted at Lawrence.J.Trautman@gmail.com.

** BA (magna cum laude), The George Washington University; JD, The George Washington University Law School. Mr. Ormerod is Assistant Professor and teaches constitutional, cyber, and business law at Western Carolina University. He may be contacted at peter@peterormerod.com.

The authors wish to extend particular thanks to the Academy of Legal Studies in Business (ALSB) for the opportunity to present this paper before the 93rd Annual Conference meeting in Portland, Oregon, August 11, 2018, and to the many ALSB colleagues who have offered comments and suggestions to earlier drafts of this manuscript. All errors and omissions are our own.

1. The virus is known by a variety of monikers, including "WannaCrypt," *see* Phillip Misner, *Customer Guidance for WannaCrypt Attacks*, MICROSOFT SECURITY RESPONSE CTR. (May 12, 2017), https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/, "WanaCrypt0r 2.0," *see* Thomas Brewster, *An NSA Cyber Weapon Might Be Behind a Massive Global Ransomware Outbreak*, FORBES (May 12, 2017), https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/, and "Wanna Decryptor," *see* Victoria Woollaston, *Wanna Decryptor Ransomware Appears to Be Spawning and This Time It May Not Have a Kill Switch*, WIRED (May 16, 2017), http://www.wired.co.uk/article/wanna-decryptor-ransomware.

2. Russell Goldman, *What We Know and Don't Know About the International Cyberattack*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html.

3. *See* Edward A. Morse & Ian Ramsey, *Navigating the Perils of Ransomware*, 72 BUS. LAWYER 287, 287 (2017), https://ssrn.com/abstract=2909280.

4 *See* Dan Goodin, *An NSA-Derived Ransomware Worm Is Shutting Down Computers Worldwide*, ARS TECHNICA (May 12, 2017), https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/.

Pictures in 2014, the Bangladeshi Central Bank in 2016, and Polish banks in February 2017—was behind the attack.[5]

Deputy Attorney General Rod Rosenstein issued a statement in October 2017, reporting that "the monetary costs of global annual cybercrime will double from $3 trillion in 2015 to $6 trillion in 2021. Those numbers are staggering; and recent events demonstrate why we need to work together to address the growing threat."[6] Ransomware threatens institutions worldwide, but the risks for businesses are starker—potentially catastrophic. This Article provides corporate counsel and executives with much of what they need to know about the current threats of ransomware like WannaCry. It proceeds in eight Parts. Part I provides a brief definition and history of ransomware. Part II looks at the history of hospitals as ransomware targets. In Part III, we offer a description of the Wannacry virus: what is known about its development, method of action, and those who are believed to have deployed it; in this Part, we also discuss methods to defend against this particular virus. Part IV discusses the Petya and NotPetya attacks. Part V discusses municipal ransomware attacks. In Part VI, we review the myriad and unique risks that ransomware poses for corporations—including expected refinements of the technique, such as to effect corporate sabotage. Part VII discusses the duties and responsibilities of corporate directors and the Ormerod-Trautman data security economic model. Finally, in Part VIII, we review the current cybersecurity legal landscape with a particular focus on corporate best practices and how business executives protect themselves against cybersecurity-related liability. We believe this Article contributes to

---

5. *See* Nicole Perlroth, *More Evidence Points to North Korea in Ransomware Attack*, N.Y. TIMES (May 22, 2017), https://www.nytimes.com/2017/05/22/technology/north-korea-ransomware-attack.html; *see also* Martha Finnemore & Duncan B. Hollis, Beyond Naming and Shaming: Accusations and International Law in Cybersecurity 15 n.77 (Mar. 6, 2019) (unpublished manuscript), https://ssrn.com/abstract=3347958; Lucia Constantin, *Recent Malware Attacks on Polish Banks Tied to Wider Hacking Campaign*, COMPUTERWORLD (Feb. 13, 2017), https://www.computerworld.com/article/3169386/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html; David E. Sanger & Katie Benner, *U.S. Accuses North Korea of Plot to Hurt Economy As Spy Is Charged in Sony Attack*, N.Y. TIMES (Sept. 6, 2018), https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html.

6. Rod Rosenstein, Deputy Attorney Gen., Remarks at the 2017 North American International Cyber Summit (Oct. 30, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-2017-north-american-international.

the sparse existing literature about ransomware and related cyber threats posed to corporate boards and management.

I. HISTORY OF RANSOMWARE

> *[T]he frequency and impact of cyber-attacks on our Nation's private sector and Government networks have increased dramatically in the past decade and are expected to continue to grow. We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Within the FBI, we are focused on the most dangerous malicious cyber activity: High-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as other technically sophisticated attacks.*[7]
>
> –Christopher A. Wray,
> Director of the Federal
> Bureau of Investigation

On October 30, 2017, Deputy Attorney General Rod Rosenstein stated, "On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. That is a 300% increase over the approximately 1,000 attacks per day in 2015."[8] The Federal Bureau of Investigation defines ransomware as:

> a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid. Ransomware is typically installed when a user clicks on a malicious link, opens a file in an e-mail that installs the malware, or through drive-by downloads (which do not require user-initiation) from a compromised Web site.[9]

---

7. *World-Wide Threats: Keeping America Secure in a New Age of Terror: Hearing Before the H. Comm. on Homeland Sec.*, 115th Cong. 29 (2017) (prepared statement of Christopher Wray, Dir., Fed. Bureau of Investigation).

8. Rosenstein, *supra* note 6.

9. FED. BUREAU OF INVESTIGATION, FBI PUBLIC SERVICE ANNOUNCEMENT, ALERT NO. I-091516-PSA: RANSOMWARE VICTIMS URGED TO REPORT INFECTIONS TO FEDERAL LAW ENFORCEMENT 1 (Sept. 15, 2016), https://www.ic3.gov/media/2016/160915.aspx.

The FBI states, "Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, [and] large businesses . . . are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them."[10] The U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) warns, "Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation."[11] Consider that "[t]he inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation."[12] The FBI warns, "in a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code."[13] Alternatively, "the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software."[14] In addition:

> On[c]e the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the

---

10. *What We Investigate: Cyber Crime*, FBI.GOV, https://www.fbi.gov/investigate/cyber (last visited Aug. 24, 2018).

11. NCCIC, ALERT (TA17-132A): INDICATORS ASSOCIATED WITH WANNACRY RANSOMWARE 5 (May 12, 2017), https://www.us-cert.gov/ncas/alerts/TA17-132A.

12. *What We Investigate*, *supra* note 10.

13. *Id.*

14. *Id.*

> ransom, usually with bitcoins because of the anonymity this virtual currency provides.[15]

According to estimates given by the US Department of Justice (DOJ), "ransomware infects more than 100,000 computers a day around the world."[16] As we will see during the next few pages, a review of the development chronology of ransomware malware reveals a pattern of growing complexity and technical sophistication. As Deputy Attorney General Rosenstein reported in 2017:

> A few years ago, ransomware attacks were unsophisticated and haphazard attempts by novice hackers to gain a few hundred dollars, mostly from individual users who happened to be affected. Today, the attacks are concerted efforts by sophisticated individuals, criminal enterprises, or nation-states that can target a range of home users, businesses, networks, or critical infrastructure with laser-like precision to cause widespread damage.[17]

Accordingly, we will now look at a brief history of ransomware by examining the following sample of malware exploits: the AIDS or PC Cyborg-Trojan, Police ransomware, Cryptoblocker, Nymain, and the Kelihos Botnet. Attacks directed at hospitals (employing the Locky exploit) and the WannaCry virus will be covered in more detail in Parts II and III. Petya and NotPetya attacks will be discussed in Part IV.

A. The AIDS or PC Cyborg-Trojan

Known as AIDS or the PC Cyborg Trojan, one of the first examples of a ransomware malware exploit dates back to 1989. This malware targeted healthcare institutions and providers and was provided to victims on a floppy disc, disguised as information about the AIDS health crisis.[18] Following installation, after the PC had been rebooted

---

15. *Id.*; *see also* Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. 1 (2019) (describing blockchain technology and its use as the foundation for virtual currencies), https://ssrn.com/abstract=3324660.

16. *See* Rosenstein, *supra* note 6.

17. *Id.*

18. *See* Danny Palmer, *What Is Ransomware? Everything You Need to Know About One of the Biggest Menaces on the Web*, ZDNET (Aug. 22, 2018), https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/; Kaveh Waddell, *The Computer Virus That Haunted Early AIDS*

ninety times, "it encrypted the machine and the files on it and demanded the user 'renew their license' with 'PC Cyborg Corporation' by sending $189 or $378 to a post office box in Panama."[19] A depiction of the ransom message appearing on the display screen of an infected computer is reproduced as Exhibit 1.

Exhibit 1
AIDS/PC Cyborg-Trojan Screen Message[20]

Dear Customer:
It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:
– a renewal software package with easy-to-follow, complete instructions;
– an automatic, self-installing diskette that anyone can apply in minutes.
Important Reference numbers: A5599796-2695577-
The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.
Press ENTER to continue

B. Ransomware

Cybercrime such as ransomware blossomed with the advent of the Internet. When floppy disk installations became replaced with Internet downloads by billions of users worldwide, a new criminal enterprise was born.

Researchers, ATLANTIC (May 10, 2016), https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

19. Palmer, *supra* note 18.

20. *Id.*

Technology journalist Danny Palmer documents the success of a criminal scheme known as Police ransomware, "which tried to extort victims by claiming to be associated with law enforcement. It locked the screen with a ransom note warning the user they'd committed illegal online activity, which could get them sent to jail."[21] The scheme was structured such that "if the victim paid a fine, the 'police' would let the infringement slide and restore access to the computer by handing over the decryption key. Of course, this wasn't anything to do with law enforcement—it was criminals exploiting innocent people."[22] Fast-forward, and we have a number of examples of ransomware technical advancement reflecting over a decade of Internet maturity.

Illustrating how many of these cases can take years to travel through the court system, the DOJ announced the following regarding the August 13, 2018 sentencing of Raymond Odigie Uadiale, of Maple Valley, Washington:

> The indictment charged Uadiale with one count of conspiracy to commit money laundering and one count of substantive money laundering. As part of the plea agreement, the government dismissed the substantive count. In addition to his prison sentence, Uadiale was also sentenced to three years of supervised release.
>
> According to the factual proffer filed in connection with the plea agreement, Uadiale helped to "cash out" the payments of victims whose computers were infected with Reveton, a type of ransomware that displayed a splash screen on the victim's computer with the logo of a law enforcement organization. The splash screen would include a message falsely telling the victim that the law enforcement organization had found illegal material on the infected computer and required the payment of a "fine" to regain access to the computer and its data. The ransomware directed the victim to purchase a GreenDot MoneyPak and enter the account number into a form on the splash screen. Using prepaid debit cards, Uadiale transformed the MoneyPak funds into cash, kept a portion for himself, and sent a portion back to Reveton's distributor, who resided in the United Kingdom.
>
> . . .

---

21. *Id.*
22. *Id.*

> According to court documents, Uadiale used the digital currency platform Liberty Reserve to transfer approximately [seventy] percent of the ransomware proceeds back to the ransomware distributor. Between October 2012 and March 27, 2013, while he was a graduate student at Florida International University, Uadiale sent approximately $93,640 in Liberty Reserve dollars to his co-conspirator as part of their scheme. Public records show that Uadiale was hired by Microsoft as a network engineer after the conspiracy charged in the indictment ended.[23]

C. Cryptolocker

On June 2, 2014, the DOJ "announced a multi-national effort to disrupt the Gameover Zeus Botnet—a global network of infected victim computers used by cyber criminals to steal millions of dollars from businesses and consumers . . . ."[24] The DOJ reported, "U.S. and foreign law enforcement officials worked together to seize computer servers central to the malicious software or 'malware' known as Cryptolocker, a form of 'ransomware' that encrypts the files on victims' computers until they pay a ransom."[25] In Pittsburgh, a federal grand jury unsealed a 14-count indictment naming a Russian individual "as a leader of a tightly knit gang of cyber criminals based in Russia and Ukraine that is responsible for the development and operation of both the Gameover Zeus and Cryptolocker schemes. An investigation . . . identified the Gameover Zeus network as a common distribution mechanism for Cryptolocker."[26] By way of methodology, "[u]nsolicited e-mails containing an infected file purporting to be a voicemail or shipping confirmation are also widely used to distribute Cryptolocker. When opened, those attachments infect victims' computers."[27]

---

23. Press Release, U.S. Dep't of Justice, Washington State Man Sentenced to Prison for Role in Connection with Riveton Ransomware (Aug. 13, 2018), https://www.justice.gov/opa/pr/washington-state-man-sentenced-prison-role-connection-reveton-ransomware.

24. Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

25. *Id.*

26. *Id.*

27. *Id.*

The DOJ has provided the following description of Cryptolocker:

> [T]he malware known as Cryptolocker (sometimes written as "CryptoLocker"), which began appearing about September 2013 . . . [is] a highly sophisticated malware that uses cryptographic key pairs to encrypt the computer files of its victims. Victims are forced to pay hundreds of dollars and often as much as $700 or more to receive the key necessary to unlock their files. If the victim does not pay the ransom, it is impossible to recover their files.
>
> Security researchers estimate that, as of April 2014, Cryptolocker had infected more than 234,000 computers, with approximately half of those in the United States. One estimate indicates that more than $27 million in ransom payments were made in just the first two months since Cryptolocker emerged.
>
> The law enforcement actions against Cryptolocker are the result of an ongoing criminal investigation by the FBI's Washington Field Office, in coordination with law enforcement counterparts from Canada, Germany, Luxembourg, the Netherlands, United Kingdom and Ukraine.
>
> Companies such as Dell SecureWorks and Deloitte Cyber Risk Services also assisted in the operation against Cryptolocker, as did Carnegie Mellon University and the Georgia Institute of Technology (Georgia Tech). The joint effort aided the FBI in identifying and seizing computer servers acting as command and control hubs for the Cryptolocker malware.[28]

D. Nymain

On December 5, 2016, the DOJ "announced a multinational operation involving arrests and searches in four countries to dismantle a complex and sophisticated network of computer servers known as 'Avalanche.' The Avalanche network allegedly hosted more than two dozen of the world's most pernicious types of malicious software and several money laundering campaigns."[29] The DOJ stated, "The types of malware and money mule schemes operating

---

28. *Id.*

29. Press Release, U.S. Dep't of Justice, Avalanche Network Dismantled in International Cyber Operation (Dec. 5, 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

over the Avalanche network varied. Ransomware such as Nymain, for example, encrypted victims' computer files until the victim paid a ransom (typically in a form of electronic currency) to the cybercriminal."[30] As we will see demonstrated in numerous instances, a request for payment to be made in Bitcoin or other virtual currency is a common denominator of ransomware schemes.[31] Relevant to our ransomware specific inquiry, the DOJ stated in its December 5, 2016 announcement:

> The Avalanche network, which has been operating since at least 2010, was estimated to serve clients operating as many as 500,000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of dollars worldwide, although exact calculations are difficult due to the high number of malware families present on the network.
>
> Several victims of Avalanche-based malware attacks are located in the Western District of Pennsylvania. A local governmental office was the victim of a Nymain malware attack in which computer files were encrypted until the victims paid a Bitcoin ransom in exchange for decrypting the files.[32]

E. Kelihos Botnet

On April 10, 2017, the DOJ announced substantial actions taken to combat the results from the Kelihos Botnet, a worldwide threat that had successfully infected tens of thousands of computers by that time.[33] The DOJ's press release stated (in part):

> The Justice Department today announced an extensive effort to disrupt and dismantle the Kelihos botnet—a global network of tens of thousands of infected computers under the control of a cybercriminal that was used to facilitate malicious

---

30. *Id.*

31. *See* Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICHMOND J.L. & TECH. 13, 9, 89–90 (2014), http://www.ssrn.com/abstract=2393537.

32. Press Release, Avalanche Network, *supra* note 29.

33. Press Release, U.S. Dep't of Justice, Justice Department Announces Actions to Dismantle Kelihos Botnet (Apr. 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

activities including harvesting login credentials, distributing hundreds of millions of spam e-mails, and *installing ransomware* and other malicious software.

. . .

"The operation announced today targeted an ongoing international scheme that was distributing hundreds of millions of fraudulent e-mails per year, intercepting the credentials to online and financial accounts belonging to thousands of Americans, and spreading ransomware throughout our networks. The ability of botnets like Kelihos to be weaponized quickly for vast and varied types of harms is a dangerous and deep threat to all Americans, driving at the core of how we communicate, network, earn a living, and live our everyday lives," said Acting Assistant Attorney General [Kenneth A.] Blanco [of the Justice Department's Criminal Division]. . . .

. . .

Kelihos malware targeted computers running the Microsoft Windows operating system. Infected computers became part of a network of compromised computers known as a botnet and were controlled remotely through a decentralized command and control system. According to the civil complaint, Peter Yuryevich Levashov allegedly operated the Kelihos botnet since approximately 2010. The Kelihos malware harvested user credentials by searching infected computers for usernames and passwords and by intercepting network traffic. Levashov allegedly used the information gained from this credential harvesting operation to further his illegal spamming operation which he advertised on various online criminal forums. . . . *Kelihos was also responsible for directly installing additional malware onto victims' computers, including ransomware* and malware that intercepts users' bank account passwords.

As with other botnets, Kelihos is designed to operate automatically and undetected on victims' computers, with the malicious code secretly sending requests for instructions to the botnet operator. In order to liberate the victim computers from the botnet, the United States obtained civil and criminal court orders in the District of Alaska. These orders authorized measures to neutralize the Kelihos botnet . . . .[34]

---

34. *Id.* (emphasis added).

On September 12, 2018, Peter Yuryevich Levashov, also known by many aliases, age "38, of St. Petersburg, Russia, pleaded guilty . . . to offenses stemming from his operation of the Kelihos botnet, which he used to facilitate malicious activities including . . . installing ransomware and other malicious software."[35] The Department of Justice reported:

> Since the late 1990s until his arrest in April 2017, Levashov controlled and operated multiple botnets, including the Storm, Waledac and Kelihos botnets, to harvest personal information and means of identification (including email addresses, usernames and logins, and passwords) from infected computers. To further the scheme, Levashov disseminated spam and distributed other malware, such as banking Trojans and ransomware, and advertised the Kelihos botnet spam and malware services to others for purchase in order to enrich himself. Over the course of his criminal career, Levashov participated in and moderated various online criminal forums on which stolen identities and credit cards, malware and other criminal tools of cybercrime were traded and sold.

F. Adultery Blackmail Scam

On July 23, 2018, the Jacksonville Division of the Federal Bureau of Investigation (FBI) in Florida issued a press release "warning residents of central Florida and beyond of an emerging scam that can target a variety of individuals. FBI Ocala ha[d recently] received numerous reports of the 'blackmail scam' . . . ."[36] The FBI Jacksonville Division further warned, "The scam usually begins when a scammer sends an anonymous letter claiming to have uncovered evidence that the recipient of the letter has committed acts of adultery. The scammer threatens to reveal the information to the recipient's spouse, family and friends, and demands payment in exchange for secrecy."[37]

---

35. Press Release, U.S. Dep't of Justice, Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses (Sept. 12, 2018), https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime.

36. Press Release, FBI Jacksonville, FBI Jacksonville Warns of Blackmail Scam (July 23, 2018), https://www.fbi.gov/contact-us/field-offices/jacksonville/news/press-releases/fbi-jacksonville-warns-of-blackmail-scam.

37. *Id.*

Bitcoin had very often been the required form of payment.[38] The Federal Trade Commission (FTC) provided the following example of this new scam message primarily directed at men, "I know about the secret you are keeping from your wife and everyone else. You can ignore this letter, or pay me a $8,600 confidentiality fee in Bitcoin."'[39] The FTC's warning mentions that the scam message would "also explain[] how to use bitcoin to make the payment."[40]

As technology evolved and the mass digitization of information followed, cybercrime, too, evolved—rapidly. As this Part described, the weaponization of malware like ransomware has flourished, taking on many forms. And its impact on users, ranging from those in government, the private sector, and beyond, is undeniable. Having expounded upon the history of ransomware and touching on its impact in this Part, the next Part discusses ransomware in the health care context.

II. HOSPITALS AS RANSOMWARE TARGETS

> *Whether you work for local law enforcement, a utility provider, a hospital, or a small or large company, you need to protect your critical infrastructure against cyber infiltration. The threat that cybercriminals pose to public entities and private businesses is substantial. A single intrusion could mean economic loss, bankruptcy, and in some cases, loss of human life.*[41]
>
> –Rod Rosenstein,
> Deputy Attorney General

As Professor Deborah R. Farringer observes, "[w]hile hackers and data breaches are not new in the healthcare context, ransomware attacks are unique in the way they have a direct and immediate impact on the actual provision of care to patients and present a very

---

38. *Id.*; *see also* Trautman, *supra* note 31.

39. Press Release, Fed. Trade Comm'n, How to Avoid a Bitcoin Blackmail Scam (Aug. 21, 2018) (emphasis omitted), https://www.consumer.ftc.gov/blog/2018/08/how-avoid-bitcoin-blackmail-scam.

40. *Id.*; *accord* Press Release, NCCIC, FTC Issues Alert on Bitcoin Blackmail Scams (Aug. 22, 2018), https://www.us-cert.gov/ncas/current-activity/2018/08/22/FTC-Issues-Alert-Bitcoin-Blackmail-Scams.

41. Rosenstein, *supra* note 6.

real threat to patient safety."[42] In her excellent law review article she writes, "[s]adly, the potential devastation that could be caused when hospitals and health systems lose access to their EHRs [Electronic Health Records] and computer systems is exactly what makes these types of attacks so attractive to potential hackers."[43] Because of the critical importance of hospitals and other parts of the healthcare system, we will briefly review several of these attacks.

A. MedStar Health

On March 28, 2016, MedStar Health, a non-profit hospital system operating in Washington, D.C., Virginia, and Maryland, received pop-up messages reading: "You have [ten] days to send us the Bitcoin . . . [.] [A]fter [ten] days we will remove your private key and it's impossible to recover your files."[44] A MedStar employee provided *The Washington Post* with a copy of the ransom note image, "which demanded that the $5 billion health-care provider pay [forty-five] bitcoins—equivalent to about $19,000—in exchange for the digital key that would release the data."[45] While the FBI investigated, the ransomware cyberattack "forced MedStar's [ten] hospitals and more than 250 outpatient centers to shut down their computers and email."[46] *The Washington Post* reports learning from a nurse at the MedStar Washington Hospital Center that "[w]ithout access to email and computer systems, the medical staff fell back on seldom-used paper records that had to be faxed or hand delivered. But this nurse and another told The Post that the paper charts are far less comprehensive than those kept in digital form."[47] Many of the medical professionals had no experience with paper charts, which were "missing vital pieces of patient information: complete medical histories, every drug prescribed, allergies to medicine and treatment plans."[48]

---

42. *See* Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE U. L. REV. 937, 940 (2017) (footnotes omitted), https://ssrn.com/abstract=2995095.

43. *Id.* (footnote omitted).

44. *Id.* at 937–38.

45. John Woodrow Cox, *MedStar Health Turns Away Patients After Likely Ransomware Cyberattack*, WASH. POST (Mar. 29, 2016), https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html.

46. *Id.*

47. *Id.*

48. *Id.*

B. Hollywood Presbyterian Medical Center

On February 5, 2016, hackers successfully employed malware to infect the computer systems at Hollywood Presbyterian Medical Center, "preventing hospital staff from being able to communicate from those devices," according to CEO Allen Stefanek.[49] The hackers demanded and Hollywood Presbyterian paid the equivalent of approximately $17,000, denominated in forty bitcoin.[50] Stefanek stated, "The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key . . . . . In the best interest of restoring normal operations, we did this."[51] *The Los Angeles Times* reported learning from law enforcement sources that "the hospital paid the ransom before reaching out to law enforcement for assistance."[52] The hospital was able to regain access to its data within a few days, employing the help of technology experts. In the interim, it resorted to "pen and paper for its record-keeping."[53]

C. Others in 2016

In addition to the two ransomware attacks listed above, Beckers Hospital Review reported twelve additional ransomware attacks during 2016 alone:

1. Titus Regional Medical Center (Mount Pleasant, TX),
2. Lukas Hospital (Germany),
3. Klinikum Arnsberg Hospital (Germany),
4. Los Angeles County Health Department (Los Angeles, CA),
5. The Ottawa Hospital (Canada),
6. Methodist Hospital (Henderson, KY),
7. DeKalb Health (Auburn, IN),
8. Kansas Heart Hospital (Wichita, KS),
9. Professional Dermatology Care (Reston, VA),

---

49. Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*

10. Keck Medicine (Los Angeles, CA),
11. Marin General Healthcare District (Greenbrae, CA), and
12. Rainbow Children's Clinic (Grand Prairie, TX).[54]

D. Locky Exploit

Technology journalist Danny Palmer reports that "[p]erhaps the most notorious form of ransomware is Locky."[55] As the malware responsible for the hospital ransoms, "Locky remained successful because those behind it regularly update the code to avoid detection."[56] Those responsible for Locky "even update[d] it with new functionality, including the ability to make ransom demands in [thirty] languages, so criminals c[ould] more easily target victims around the world. Locky became so successful, it rose to become [among the] most prevalent forms of malware in its own right."[57]

E. Others

The ransomware attacks on hospitals continue. Deputy Attorney General Rod Rosenstein reported that during mid-2017, "Michigan's Caro Community Hospital and its related facilities lost access for approximately two weeks to computers, phones, patient records, and e-mail services because of a ransomware attack. Fortunately, no medical devices were directly affected."[58] But, as Deputy Attorney General Rosenstein warned, "imagine how much more serious the attack could have been. Many types of machines critical to emergency treatment are computers. MRI machines and ventilators may run software and be connected to networks. A targeted and widespread attack on medical service providers could endanger lives."[59]

According to the cybersecurity firm Symantec, a hacking group called SamSam has been responsible for many of the cyber attacks and ransom demands targeting healthcare organizations.[60] In late

---

54. *12 Healthcare Ransomware Attacks of 2016,* BECKER'S HOSP. REV. (Dec. 29, 2016), https://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html.

55. Palmer, *supra* note 18.

56. *Id.*

57. *Id.*

58. *See* Rosenstein, *supra* note 6.

59. *Id.*

60. *SamSam: Targeted Ransomware Attacks Continue,* SYMANTEC (Oct. 20, 2018), https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks (referring to SamSam as "highly active"); *see also* Olivia Beavers, *Security Firm: Hacking Group SamSam Primarily Targeting U.S. Organizations with*

2018, Symantec reported that fifty-six of the sixty-seven organizations targeted by SamSam that year were located in the U.S.[61] Why has SamSam been so attracted to healthcare organizations? Symantec posits that "[t]he attackers may believe that healthcare organizations are easier to infect. Or they may believe that these organizations are more likely to pay the ransom."[62]

Professor Farringer argues that "while stricter and more current federal regulations are necessary, the most expedient way to protect against immediate attacks will be an industry-driven response demanding industry-wide security standards from EHR [electronic health records] companies above and beyond HIPPA standards."[63] These enhanced standards are necessary, Professor Farringer contends, because:

> Hospitals and health systems appear uniquely vulnerable to ransomware attacks as a result of various factors, including (1) the fractured movement toward electronic medical records and (2) the Department of Health and Human Services' lack of emphasis on enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act with respect to security of electronic data.[64]

Ransomware Attacks, HILL (Oct. 30, 2018), https://thehill.com/policy/cybersecurity/413860-security-firm-hacking-group-samsam-primarily-targeting-us-organizations.

61. *SamSam: Targeted Ransomware Attacks Continue*, *supra* note 63 ("A small number of attacks were logged in Portugal, France, Australia, Ireland, and Israel.").

62. *Id.*

63. Farringer, *supra* note 43 at 941.

64. *Id.* (citing Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 300gg (2010), 1320d (2010); 29 U.S.C. §§ 1181 (2011), 1182 (2008), 1183 (1996); Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§300jj–jj-51 (2016), §§ 17901–903 (2009); Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 226-79 (2009)).

III. THE WANNACRY RANSOMWARE VIRUS

> *Pyongyang has previously conducted cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014—and remains capable of launching disruptive or destructive cyber attacks to support its political objectives. Pyongyang also poses a cyber threat to US allies. South Korean officials have suggested that North Korea was probably responsible for the compromise and disclosure of data in 2014 from a South Korean nuclear plant.*[65]
>
> —Daniel R. Coats,
> Director of National
> Intelligence

On May 12, 2017, reports surfaced about a virulent new strain of ransomware originating in India, Hong Kong, and the Philippines.[66] The U.S. Department of Homeland Security's NCCIC reported, "According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as [twenty-seven] different languages."[67] Known as WannaCry, Wanna Decryptor, or WCry,[68] this ransomware is, most fundamentally, a specific type of malicious software that "locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in [the anonymous digital cryptocurrency] Bitcoin."[69] This "digital extortion racket is not new—it's been around since about 2005," but it has recently seen a resurgence due to refined methods: "attackers have greatly improved on the scheme with the development of ransom cryptware, which encrypts your files using a private key that only the attacker possesses, instead of simply locking your keyboard or

---

65. *Open Hearing on Worldwide Threats Before the S. Select Comm. on Intelligence*, 115th Cong. 17 (2017) (prepared statement of Daniel R. Coats, Director of National Intelligence).

66. *See* Bill Brenner, *WannaCry: The Ransomware Worm That Didn't Arrive on a Phishing Hook*, NAKED SECURITY (May 17, 2017), https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/.

67. NCCIC, *supra* note 11.

68. *See id.*

69. Kim Zetter, *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*, WIRED (May 14, 2017), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.

computer."[70] The WannaCry ransomware employs this refined technique.[71]

This Part first examines WannaCry's origins—how an exploitation of Microsoft Windows developed by the U.S. National Security Agency was responsible for the attack's wide scale infection. Second, we discuss the virus's method of action and relate the impacts it had across the globe. Finally, we address who authorities and experts believe perpetrated the attack: the same North Korean hacking group that was responsible for the 2014 breach of Sony Pictures.

A. WannaCry's U.S. NSA Origins

In August 2016, a group known only as the "Shadow Brokers" began releasing and auctioning off a set of cyber weapons belonging to the U.S. National Security Agency's ("NSA") highly secretive Office of Tailored Access Operations ("TAO").[72] The Shadow Brokers began by announcing a putative auction of digital weapons they claimed had been stolen from the "Equations Group," a highly advanced hacking group that many commentators believe is synonymous with NSA's TAO.[73]

The Shadow Brokers released a number of leaks throughout the second half 2016, including digital tools for exploiting firewalls and network infrastructure engineered by companies that include Cisco, Juniper, Fortinet, and Huawei, a Chinese company.[74] Simultaneously, the group provided a cache of encrypted files, and it claimed they would provide the password to this cache to the winner of a Bitcoin auction.[75] This fundraising auction effort was ultimately

---

70. *Id.*

71. *See, e.g.*, Palmer, *supra* note 18.

72. *See* David E. Sanger, *'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?* N.Y. TIMES (Aug. 16, 2016), https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html.

73. *See* Scott Shane, Nicole Perloth & David E. Sanger, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. TIMES (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

74. Lorenzo Franceschi-Bicchierai, *NSA Targeted Chinese Firewall Maker Huawei, Leaked Documents Suggest*, MOTHERBOARD, (Aug. 24, 2016, 9:00 AM), https://motherboard.vice.com/en_us/article/nsa-huawei-firewalls-shadow-brokers-leak.

75. Joseph Cox, *They're Back: The Shadow Brokers Release More Alleged Exploits*, MOTHERBOARD (Apr. 8, 2017, 11:33 AM), https://motherboard.vice.com/en_us/article/theyre-back-the-shadow-brokers-release-more-alleged-exploits.

not successful,[76] so on April 8, 2017, the Shadow Brokers publicly released the password to this encrypted cache of files.[77]

Then, on April 14, 2017, the group released another set of tools developed by the U.S. NSA. Among this April 14 cache was a Microsoft Windows zero-day exploit known as ETERNALBLUE.[78] A zero-day exploit is "software vulnerabilit[y] for which no patch or fix has been publicly released."[79] Microsoft actually issued a patch for the ETERNALBLUE exploit a month before it was leaked,[80] which has fueled speculation that Microsoft had been tipped off about the existence of the vulnerability, presumably by its original engineer—the NSA.[81]

B. WannaCry's Method of Operation and Global Impacts

A technical and highly detailed discussion of WannaCry's format, signatures, and method of operation exceeds the scope of this Article.[82] However, in broad terms, enterprise server access was gained via "exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP,

---

76. Janus Kopfstein, *'Shadow Brokers' Whine That Nobody Is Buying Their Hacked NSA Files*, MOTHERBOARD (Oct. 1, 2016, 4:00 PM), https://motherboard.vice.com/en_us/article/shadow-brokers-whine-that-nobody-is-buying-their-hacked-nsa-files.

77. *See* Cox, *supra* note 76.

78. Dan Goodin, *NSA-leaking Shadow Brokers Just Dumped Its Most Damaging Release Yet*, ARS TECHNICA (Apr. 14, 2017, 1:27 PM), https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.

79. LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS: THE LIFE AND TIMES OF ZERO-DAY VULNERABILITIES AND THEIR EXPLOITS ix (2017), http://www.rand.org/pubs/research_reports/RR1751.html.

80. Phillip Misner, *Protecting Customers and Evaluating Risk*, MICROSOFT SECURITY RESPONSE CTR. (Apr. 14, 2017), https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/ (listing the "EternalBlue" vulnerability as having been patched by MS17-010 on Mar. 14, 2017).

81. *See* Richard Lawler, *Microsoft Says It Already Patched 'Shadow Brokers' NSA Leaks*, ENGADGET (Apr. 15, 2017), https://www.engadget.com/2017/04/15/microsoft-says-it-already-patched-several-shadow-brokers-nsa-l/ ("Because 'The Shadow Brokers' listed what tools they had in January, it seemed like the NSA had to know this release could happen."); Scott Shane, *Malware Case Is Major Blow for the N.S.A.*, N.Y. TIMES, May 16, 2017, at A1.

82. *See, e.g.*, Raj Samani & Christiaan Beek, *An Analysis of the WannaCry Ransomware Outbreak*, MCAFEE (May 12, 2017), https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/; Zammis Clark, *The Worm That Spreads WanaCrypt0r*, MALWAREBYTES, https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/ (last updated May 13, 2017).

Windows 8, and Windows Server 2003 operating systems on May 13, 2017."[83] Worldwide victims of the WannaCry exploit included: the U.K.'s National Health Service[84]; U.S. FedEx, Spain's Telefónica, Russian telecommunications giant MegaFon[85]; Russian Interior Ministry and Romanian carmaker Dacia[86]; and a disproportionate negative effect on China due to bootleg software.[87] However, it did not take long for intelligence officials and security experts to agree that North Korea was responsible for using the NSA's ENTERNALBLUE exploit to engineer the WannaCry virus.[88]

C. WannaCry and North Korea

Former U.S. Director of National Intelligence (DNI) James R. Clapper reports, "on November 24 [2014], a hacker group calling itself the Guardians of Peace published a tranche of personal emails and embarrassing information about the executives at Sony Pictures."[89] Then, these hackers, "continued to post emails and documents and even yet-to-be-released Sony movies, and they then tried to sabotage Sony Pictures' IT operating systems. They threatened to do more damage if Sony didn't cancel the release of *The Interview*."[90] The assessment of DNI Clapper and other U.S. cyber specialists is "that the Sony hacks had originated in North Korea, and that, to do what they'd accomplished, the North Koreans had been on Sony Pictures' systems for weeks, even months."[91] As Trautman has described elsewhere:

> During the 2014 December holiday season Americans were confronted with yet another reported cyber attack. This time, state actor North Korea is alleged to have committed a major cyber attack on the data systems of Sony Corporation in

---

83. *See* NCCIC, *supra* note 11.

84. Steven Erlanger et al., *Britain's Health Service, Targeted in Cyberattack, Ignored Warnings for Months*, N.Y. TIMES, May 13, 2017, at A9.

85. Nicole Perlroth & David E. Sanger, *Hackers Use Tool Taken from N.S.A. in Global Attack*, N.Y. TIMES, May 13, 2017, at A1, A9.

86. Mark Scott & Nick Wingfield, *Clock Ticking, Security Experts Scramble to Defuse Cyberattack*, N.Y. TIMES, May 14, 2017, at A15.

87. Paul Mozur, *Addiction to Pirated Software Leaves China Vulnerable to Malware Assaults*, N.Y. TIMES, May 16, 2017, at A8.

88. *See* Perlroth & Sanger, *supra* note 86.

89. JAMES R. CLAPPER, FACTS AND FEARS: HARD TRUTHS FROM A LIFE IN INTELLIGENCE 283 (2018).

90. *Id.*

91. *Id.*

> retaliation for a proposed Christmas day-release of the Hollywood motion picture spoofing a fictitious plan to assonate the leader of North Korea. The attack traced to North Korea was soon followed by threats of attacks on those theaters scheduled for the film's release on Christmas day 2014. As a result, Sony Pictures Entertainment cancelled the planned release to theaters and the film became available on Netflix.
>
> In his June 9, 2011 confirmation hearing for the post of secretary of defense before the Senate Armed Services Committee[,] Central Intelligence Agency Director Leon Panetta observed, "'the next Pearl Harbor that we confront could very well be a cyberattack that cripples' America's electrical grid and its security and financial systems." Here, the 2014 cyber attack of Sony Pictures Entertainment was a breach of corporate communications, strategy and entertainment assets, including motion picture films.
>
> By 2017, ransomware has gained significant use by criminals as a tool to extort payments from businesses, governments, and individuals. After infecting the victim's computer with ransomware, a payment often by Bitcoin is required, before the victim's computer is returned to a functional condition. *The Interview* is not the only motion picture to receive extortion demands. A major cyberattack during May 2017 is attributed to North Korean actors, approximately two and a half years following the December 2014 attack on SONY Pictures Entertainment. The attack on SONY is not at all among the largest breaches either in terms of number of individuals impacted or the cost to the shareholders of SONY. What sets the SONY attack apart from others is that this is one of the first attributed to a nation state actor that aims at a U.S. corporation, SONY Pictures Entertainment.[92]

On September 6, 2018, the DOJ announced the unsealing of a complaint, "charging Park Jin Hyok . . . , a North Korean citizen, for his involvement in a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money

---

92. *See* Lawrence J. Trautman, The SONY Data Hack: Implications for World Order (Feb. 18, 2018) (unpublished manuscript) (on file with author).

and other resources."[93] In a press release, the DOJ described the complaint's allegations and further commented:

> The complaint alleges that Park was a member of a government-sponsored hacking team known to the private sector as the "Lazarus Group," and worked for a North Korean government front company . . . to support the DPRK government's malicious cyber actions.
>
> The Conspiracy's malicious activities include the creation of the malware used in the 2017 WannaCry 2.0 global ransomware attack; the 2016 theft of $81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment . . . ; and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities.
>
> . . .
>
> . . . [FBI Director Christopher Wray stated,] "We stand with our partners to name the North Korean government as the force behind this destructive global cyber campaign. This group's actions are particularly egregious as they targeted public and private industries worldwide—stealing millions of dollars, threatening to suppress free speech, and crippling hospital systems. We'll continue to identify and illuminate those responsible for malicious cyberattacks and intrusions, no matter who or where they are."
>
> . . .
>
> *About the Defendant Park and Chosun Expo Joint Venture*
>
> According to the allegations contained in the criminal complaint, which was filed on June 8, 2018 in Los Angeles federal court, and posted today: Park Jin Hyok, was a computer programmer who worked for over a decade for Chosun Expo Joint Venture . . . . Chosun Expo Joint Venture had offices in China and the DPRK, and is affiliated with Lab 110, a component of DPRK military intelligence. In addition to the programming done by Park and his group for paying

93. Press Release, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions: North Korean Hacking Team Responsible for Global WannaCry 2.0 Ransomware, Destructive Cyberattack on Sony Pictures, Central Bank Cybertheft in Bangladesh, and Other Malicious Activities, Dep't of Justice (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

> clients around the world, the Conspiracy also engaged in malicious cyber activities. Security researchers that have independently investigated these activities referred to this hacking team as the "Lazarus Group." The Conspiracy's methods included spear-phishing campaigns, destructive malware attacks, exfiltration of data, theft of funds from bank accounts, ransomware extortion, and propagating "worm" viruses to create botnets.
>
> . . .
>
> *Creation of Wannacry 2.0*
>
> In May 2017, a ransomware attack known as WannaCry 2.0 infected hundreds of thousands of computers around the world, causing extensive damage, including significantly impacting the United Kingdom's National Health Service. The Conspiracy is connected to the development of WannaCry 2.0, as well as two prior versions of the ransomware, through similarities in form and function to other malware developed by the hackers, and by spreading versions of the ransomware through the same infrastructure used in other cyber-attacks.
>
> Park and his co-conspirators were linked to these attacks, intrusions, and other malicious cyber-enabled activities through a thorough investigation that identified and traced: email and social media accounts that connect to each other and were used to send spear-phishing messages; aliases, malware "collector accounts" used to store stolen credentials; common malware code libraries; proxy services used to mask locations; and North Korean, Chinese, and other IP addresses. Some of this malicious infrastructure was used across multiple instances of the malicious activities described herein. Taken together, these connections and signatures—revealed in charts attached to the criminal complaint—show that the attacks and intrusions were perpetrated by the same actors.[94]

More evidence continues to build regarding the ongoing involvement of North Korea in WannaCry exploits and progeny.[95] Exhibit 2 presents a sample of North Korean Government activity, known as HIDDEN COBRA.

---

94. *Id.*

95. *See* Perlroth, *supra* note 5.

Exhibit 2
North Korean Government Cyber Activity[96]

Date	Item	Comment
Oct. 2, 2018	Alert (TA18-275A)	HIDDEN COBRA FASTCash Campaign
Oct. 2, 2018	Malware Analysis Report (MAR-10201537)	HIDDEN COBRA FASTCash-Related Malware
Aug. 9, 2018	Malware Analysis Report (10135536-17)	North Korean Trojan: KEYMARBLE
June 14, 2018	Malware Analysis Report (10135536-12)	North Korean Trojan: TYPEFRAME
May 29, 2018	Alert (TA18-149A)	HIDDEN COBRA- Joanap Backdoor Trojan and Brambul Server Message Block Worm
May 29, 2018	Malware Analysis Report (MAR-10135536-3)	HIDDEN COBRA RAT/Worm
Mar. 28, 2018	Malware Analysis Report (MAR-10135536.11)	North Korean Trojan: SHARPKNOT-STIX file for MAR-10135536.11
Feb. 13, 2018	Malware Analysis Report (MAR-10135536-F)	North Korean Trojan: HARDRAIN-STIX file for MAR-10135536-F
Feb. 13, 2018	Malware Analysis Report (MAR-10135536-G)	North Korean Trojan: BADCALL-STIX file for MAR-10135536-G
Dec. 21, 2017	Malware Analysis Report (MAR-10135536)	North Korean Trojan: BANKSHOT-STIX file for MAR-10135536
Nov. 14, 2017	Alert (TA-318A)	HIDDEN COBRA-North Korean Remote Administration Tool: FALLCHILL
Nov. 14, 2017	Alert (TA17-318B)	HIDDEN COBRA-North Korean Trojan: Volgmer
Aug. 23, 2017	Malware Analysis Report (MAR-10132963)	An Delta Charlie Attack Malware – STIX file for MAR-10132963
June 13, 2017	Alert (TA17-164)	HIDDEN COBRA- North Korea's DDoS Botnet Infrastructure
May 12, 2017	Alert (TA17-132A)	Indicators Associated With WannaCry Ransomware

96. *See* Hidden Cobra—North Korean Malicious Cyber Activity, U.S.-CERT, U.S. DEPT. OF HOMELAND SEC., https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity (last visited Apr. 23, 2019).

D. WannaCry, Bitcoin, and Digital Currencies

Numerous scholars have discussed the fundamental role bitcoin plays in the success of criminal enterprises and recent ransomware.[97] While not "untraceable or completely anonymous,"[98] "[b]itcoin is currently the most popular cryptocoin . . . ."[99] But new cybercurrencies "claim to provide full anonymity and untraceability, and will probably be preferred in the future by cyber gangs to make law enforcement work in tracking the flux of money almost impossible."[100] In the case of the Cryptolocker ransomware exploit, Professors Hernandez-Castro, Cartwright, and Stepanova observe:

> Cryptolocker employed a number of different bitcoin addresses to request the victims to send the money to. There is speculation that it created a new one for each victim. . . . [O]nce the victim's bitcoins were transferred to that address, they were rapidly moved to others, and laundered using bitcoin mixers. At least 628 of these initial addresses are known. When further investigated, it was discovered that the bitcoin transfers very frequently visited a small number of addresses. For example, from this list of 628 at least 440 visited the address 174psvzt77NgEC373xSZWm9gYXqz4sTJjn. This single address received a total of 346,102.31357807 BTC, which is a significant amount of the total number of bitcoins in circulation (approx. [twelve] million) at the time of its last transaction in February 2014. The average value of this amount of bitcoins at that time was in excess of $207 [million].[101]

The mechanics of bitcoin transfer in the case of Cryptolocker ransomware involved payments received at the address requested

---

97. *See* Julio Hernandez-Castro et al., Economic Analysis of Ransomware (March 20, 2017), https://ssrn.com/abstract=2937641; Adam J. Sulkowski, Blockchain, Law, and Business Supply Chains: The Need for Governance and Legal Frameworks to Achieve Sustainability 1 (May 13, 2018) (unpublished manuscript), https://ssrn.com/abstract=3205452; Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L. Q. REP. 232, 234 (2016); Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041, 1050 (2017).

98. Hernandez-Castro, et al., *supra* note 98, at 3.

99. *Id.*

100. *Id.*

101. *Id.*

going "straight to accumulator addresses like those shown above. These accumulators, after receiving around 500 BTC, then sent the money to a chain of addresses [with] typically only 2 transactions each, the first one receiving the bitcoin and another one sending bitcoin to two or more addresses,"[102] further dividing the transaction amounts.

IV. PETYA AND NOTPETYA ATTACKS

> *Taken all together, cyber poses an incredibly complex set of threats, because criminals, and "hacktivist" collectives like Anonymous, are all thrown in together with aggressors like North Korea and Iran, and with the Russians and Chinese, who could do real damage if they are so inclined. Each of those actors has different capabilities and different objectives when they engage in Cyberspace, and all of them operate on the same Internet.*[103]
>
> —James R. Clapper,
> Former Director of National
> Intelligence

A. Petya Ransomware

Petya is a type of ransomware that propagates using an email attachment.[104] The first iteration appeared in March 2016 and arrived in victims' inboxes as a job applicant's resume with an executable file attached.[105] If a victim downloaded the file, the victim would be prompted by the Windows User Access Control warning that the executable file wants to make changes to the computer.[106] If a victim allowed the malware to make changes, the computer would reboot; upon rebooting, the victim's files would be encrypted and a ransom message would be displayed.[107]

---

102. *Id.*

103. CLAPPER, *supra* note 90, at 284–85 (citing James R. Clapper, Remarks at the International Conference on Cyber Security at Fordham University (Jan. 2015)).

104. Josh Fruhlinger, *Petya Ransomeware and NotPetya Malware: What You Need to Know Now*, CSO BLOG (Oct. 17, 2017, 2:59 AM), https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

105. *Id.*

106. *Id.*

107. *Id.*

In some ways, however, Petya is the next logical step in ransomware's evolution. For example, Petya's mode of encrypting a victim's files is more sophisticated than past strains of malware, and a later iteration of Petya bundled a second, alternative mechanism—called Mischa—to render victims' computers unusable.[108] All things considered, Petya is a fairly routine malware evolutionary step: it uses a more sophisticated technique to encrypt a victim's files but its reliance on unwitting users granting permissions limited the scope of its damage.

B. NotPetya Malware

In June 2017, a new and far more dangerous version of Petya wreaked international havoc. Many people initially believed it was merely a routine evolutionary step in Petya's development—a version of Petya that used the ETERNALBLUE exploit, rather than relying on users granting permissions.[109] But eventually researchers determined this new strain was fundamentally different from Petya, and it has been dubbed NotPetya.[110] NotPetya is the most costly and damaging cyberattack in history: The U.S. government estimated its damages in excess of $10 billion.[111]

While superficially resembling Petya, NotPetya differed in some significant and important ways. Perhaps most notably, NotPetya is not, technically, ransomware. While it does encrypt a victim's computer files, it does so irreversibly: Even if a victim paid the ransom, the files could not be recovered.[112]

Like WannaCry, NotPetya spreads using the ETERNALBLUE zero-day.[113] NotPetya, however, does not incorporate the fairly fundamental errors that stunted WannaCry's proliferation—namely, it omits the infamous WannaCry "kill switch," meaning that the only way to protect against NotPetya is to install the Windows patch.[114] The U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) observes that "if

---

108. *Id.*

109. *See, e.g.*, Lily Hay Newman, *A Scary New Ransomware Outbreak Uses WannaCry's Old Tricks*, WIRED (June 27, 2017, 12:09 PM), https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/.

110. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

111. *Id.*

112. *Id.*

113. *Id.*

114. Newman, *supra* note 110.

the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable,"[115] and provides the following technical details:

> NCCIC received a sample of the NotPetya malware variant and performed a detailed analysis. Based on the analysis, NotPetya encrypts the victim's files with a dynamically generated, 128-bit key and creates a unique ID of the victim. However, there is no evidence of a relationship between the encryption key and the victim's ID, which means it may not be possible for the attacker to decrypt the victim's files even if the ransom is paid. It behaves more like destructive malware rather than ransomware.
>
> NCCIC observed multiple methods used by NotPetya to propagate across a network. The first and—in most cases—most effective method, uses a modified version of the Mimikatz tool to steal the user's Windows credentials. The cyber threat actor can then use the stolen credentials, along with the native Windows Management Instrumentation Command Line (WMIC) tool or the Microsoft SysInternals utility, psexec.exe, to access other systems on the network. Another method for propagation uses the EternalBlue exploit tool to target unpatched systems running a vulnerable version of SMBv1. In this case, the malware attempts to identify other hosts on the network by checking the compromised system's IP physical address mapping table. Next, it scans for other systems that are vulnerable to the SMB exploit and installs the malicious payload. Refer to the malware report, MIFR-10130295, for more details on these methods.
>
> The analyzed sample of NotPetya encrypts the compromised system's files with a 128-bit Advanced Encryption Standard (AES) algorithm during runtime. The malware then writes a text file on the "C:\" drive that includes a static Bitcoin wallet location as well as unique personal installation key intended for the victim to use when making the ransom payment and the user's Bitcoin wallet ID. NotPetya modifies the master boot record (MBR) to enable encryption of the master file table (MFT) and the original MBR, and then reboots the system. Based on the encryption methods used, it appears unlikely that the files could be

115. Press Release, Alert (TA17-181A) Petya Ransomware (Feb. 15, 2018), https://www.us-cert.gov/ncas/alerts/TA17-181A.

> restored, even if the attacker received the victim's unique key and Bitcoin wallet ID.
>
> The delivery mechanism of NotPetya during the June 27, 2017, event was determined to be the Ukrainian tax accounting software, M.E.Doc. The cyber threat actors used a backdoor to compromise M.E. Doc's development environment as far back as April 14, 2017. This backdoor allowed the threat actor to run arbitrary commands, exfiltrate files, and download and execute arbitrary exploits on the affected system. Organizations should treat systems with M.E.Doc installed as suspicious, and should examine these systems for additional malicious activity.[116]

But NotPetya also has a mechanism for infecting computers that have been patched. This second mechanism is called Mimikatz, and Mimikatz is capable of pulling a Windows user's password out of a computer's RAM.[117] This becomes particularly dangerous in multi-computer networks: If a single machine has not installed the ETERNALBLUE patch, then NotPetya could use the Mimikatz to obtain administrator credentials and thus infect the entire network.[118] The French security researcher who first demonstrated Mimikatz, Benjamin Deply, explained: "You can infect computers that aren't patched, and then you can grab the passwords from those computers to infect other computers that *are* patched."[119]

The victims of NotPetya were widespread and included several sophisticated companies. The attack was initially focused on Ukraine, but the malware was so virulent that it spread far and wide, damaging "Ukrainian infrastructure like power companies, airports, public transit, and the central bank, as well as Danish shipping company Maersk, the Russian oil giant Rosnoft, and institutions in India, Spain, France, the United Kingdom," among others.[120] The shipping giant Maersk alone estimated that NotPetya cost the company between $250 million and $300 million.[121] There is universal consensus that the Russian government is responsible for using NotPetya to wage war on Ukraine.[122] But, in light of the fact NotPetya damaged Rosnoft, it seems that the malware was more successful

---

116. *Id.*
117. Greenberg, *supra* note 111.
118. *Id.*
119. *Id.*
120. Newman, *supra* note 110.
121. Greenberg, *supra* note 111.
122. *Id.*

than even its creators anticipated. NotPetya represents a startling escalation of nation-state cyberwar.

V. MUNICIPAL AND EDUCATIONAL RANSOMWARE ATTACKS

> *The concept is simple: Your computer gets infected with a virus that encrypts your files until you pay a ransom. It's extortion taken to its networked extreme. The criminals provide step-by-step instructions on how to pay, sometimes even offering a help line for victims unsure how to buy bitcoin. The price is designed to be cheap enough for people to pay instead of giving up: a few hundred dollars in many cases. Those who design these systems know their market, and it's a profitable one.*[123]
>
> —Bruce Schneier,
> Chief Technology Officer,
> IBM Resilient, fellow at
> Harvard's Berkman Center,
> and a board member of EFF

Municipalities, educational institutions, and other public institutions have also proven to be an attractive target for ransomware criminals. During 2017, reports of a $25,000 ransom demanded of the St. Louis Public Library and a $50,000 demand of Licking County, Ohio, surfaced: "Local governments are forced to spend money on frantic efforts to recover data, system upgrades, cybersecurity insurance and, in some cases, to pay their online extortionists if they can't restore files some other way."[124] This Part presents a few of the ample 2018 examples of ransomware attacks on such institutions.

---

123. Bruce Schneier, *The Future of Ransomware*, SCHNEIER ON SECURITY (May 23, 2017, 5:55 AM), https://www.schneier.com/blog/archives/2017/05/the_future_of_r.html.

124. *See* Jon Kamp & Scott Calvert, *Cyberattacks Target Local Governments*, WALL ST. J., June 25, 2018, at A4.

A. Atlanta

During mid-March 2018, the city of Atlanta received a ransom demand from hackers known as the SamSam group, requesting a payment of about $51,000 to be made in Bitcoin.[125] *The New York Times* characterizes the Atlanta attack as "one of the most sustained and consequential cyberattacks ever mounted against a major American city."[126] The digital extortion "laid bare once again the vulnerabilities of governments as they rely on computer networks for day-to-day operations."[127] While wastewater systems and the systems involving 911 emergency telephone calls were not impacted, "other arms of city government [were] scrambled for days. The Atlanta Municipal Court [was] unable to validate warrants. Police officers [were] writing reports by hand. The city . . . stopped taking employment applications."[128] Even after the desktop computers for roughly 8,000 Atlanta employees came "back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world's busiest airport still could not use the free Wi-Fi."[129]

It appears that victims of SamSam's attacks "more easily afford the $50,000 or so in ransom than the time and cost of restoring their locked data and compromised systems. In the past year, the group has taken to attacking hospitals, police departments and universities—targets with money but without the luxury of going off-line for days or weeks for restoration work."[130] So, what appears to be the cost to Atlanta? *The Wall Street Journal* reported that Atlanta Mayor Keisha Lance Bottoms, speaking in mid-2018 at a mayor's conference, "estimated that the city, which decided to rebuild its systems, was facing more than $20 million in costs, but she hoped insurance would cover much of that."[131]

---

125. *See* Alan Blinder & Nicole Perlroth, *Atlanta Hobbled by Major Cyberattack That Mayor Calls 'a Hostage Situation'*, N.Y. TIMES, Mar. 28, 2018, at A14.
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.*
130. *Id.*
131. *See* Kamp & Calvert, *supra* note 125.

B. Rockport, Maine

In addition to the Atlanta ransomware attack, other local governments attacked during 2018 include Leeds, Alabama and Rockport, Maine.[132] In the Rockport attack, "[a]n unknown hacker had sneaked malicious software onto the network and was demanding a payment of roughly $1,200 in bitcoin in return for codes to unlock the town's files"[133] and "offered tips on how to acquire cryptocurrency."[134] Rockport decided not to pay the ransom. Instead, two city employees "worked through the weekend and had town systems up and running again by the next week. Still, the hamlet of about 3,400 ultimately paid about $10,000 to cover the immediate restoration work, plus another $28,000 to $30,000 on security improvements."[135]

C. Schools and Others

Schools have also been the target of substantial ransomware threats and requests.[136] Examples of recent ransomware payments made by educational institutions include: in 2016, South Carolina's Horry County Schools (paying hackers nearly $10,000); in 2017, Los Angeles Valley College in California (paying a ransom of $28,000 in January) and Dorchester School District Two in South Carolina (paying $2,900 to hackers in July). Dorchester School District Two ultimately paid "a $5,000 deductible in an insurance claim, which covered the $2,900 ransom and just over $150,000 for legal fees, consulting costs and personnel costs to rebuild some databases destroyed in the hack."[137] Horry County's executive director of technology, Charles Hicks, stated that the County's "nearly $10,000 payment to hackers pales in comparison to each day it didn't have access to files and content created by 43,000 students and 4,000-plus faculty and staff."[138] Other examples of ransomware demands made on educational institutions far exceed the limited space available for this Article. In Part VI, our attention will shift to threats directed toward corporations.

---

132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. Tawnell D. Hobbs, *Hackers Target Schools*, WALL ST. J., Oct. 24, 2017, at A3.
137. *Id.*
138. *Id.*

VI. THREATS RANSOMWARE POSE TO CORPORATIONS

Cyber criminals know that a company's lifeblood is contained in its networks and the information flowing through those systems. The last few years have witnessed a significant increase in criminals using ransomware.[139]

–Rod Rosenstein,
Deputy Attorney General

Transnational organized crime syndicates have utilized extortion schemes for many years.[140] Joining longstanding illicit lines of business—such as the kidnapping of executives and piracy of vessels and their cargos in exchange for ransom payments—is the newly technologically-enabled extortion business model of computer ransomware.[141] This new technology vulnerability is now on the long list of crises that face corporate directors.[142]

The *Proofpoint Quarterly Threat Report* for the fourth quarter of 2017 states that "ransomware remained the top payload distributed by malicious messages[,] . . . account[ing] for 57% of all malicious volume."[143] Proofpoint provides the following commentary about ransom payment:

---

139. *See* Rosenstein, *supra* note 6.

140. *See* Morse & Ramsey, *supra* note 3, at 287.

141. *Id.*; *see also* David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability* 21 (Sept. 18, 2018) (unpublished manuscript), https://ssrn.com/abstract=3251479.

142. *See* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance,* 13 HASTINGS BUS. L. J. 275, 281–82 (2017); Lawrence J. Trautman & George P. Michaely, Jr., *The SEC & The Internet: Regulating the Web of Deceit,* 68 CONSUMER FIN. L. Q. REP. 262, 262 (2014), http://www.ssrn.com/abstract=1951148; Lawrence J. Trautman, *Who Qualifies As an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?,* 11 DEPAUL BUS. & COMM. L. J. 205, 232–33 (2013) (discussing the need for cybersecurity expertise represented on corporate boards); Lawrence J. Trautman et al., *Corporate Information Technology Governance Under Fire,* 8 J. STRAT. & INT'L STUD. 105, 105 (2013), https://ssrn.com/abstract=2346583; Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer,* 1 AM. U. BUS. L. REV. 337, 344 (2011) (cyber insurance is important in managing risk); Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75, 112–15 (2012) (discussing need for recruitment of corporate directors experienced in cybersecurity matters).

143. *See* PROOFPOINT, PROOFPOINT QUARTERLY THREAT REPORT Q4, at 4 (2017), https://www.proofpoint.com/us/resources/threat-reports/january-2018.

> For much of the last two years, attackers' ransoms have been denominated in Bitcoin values. The amount demanded is expressed as some number of bitcoins, whether a full integer or a fraction such as "0.5" or "0.15." Surging cryptocurrency values are a boon for holders of Bitcoin. But they are a challenge for anyone who tries to price their product or service in Bitcoin—threat actors included. In Q4, newer ransomware strains appeared to take this into account. Sigma ransomware first appeared in mid-November [2017] demanding a payment denominated in U.S. dollars. Denominating ransoms in a government issued currency—even if the actual payment is made in the form of Bitcoin—has two big benefits for an attacker. It allows the threat actors to maintain stability and still accept their payments anonymously, and in a currency that, for the moment, continues to appreciate quickly.[144]

Large corporations often have developed customized software over the years, while still operating on older operating systems. These mission critical applications often break due to programming conflicts between these legacy operating systems as updates are installed.[145] Bruce Schneier observes, "Many of the organizations hit by WannaCry had outdated systems for exactly these reasons. But as expensive and time-consuming as updating might be, the risks of not doing so are increasing."[146]

A. BYOD, IoT, and Vulnerability Escalation

Cyber threats to corporations have increased substantially due to the use of multiple electronic devices by each of their employees, often referred to as Bring Your Own Data (BYOD).[147] Use of personal laptops, smart phones, iPads, and any of the numerous other personal digital devices interconnecting with employees expose corporate data systems to the vulnerabilities resident on employee devices.

---

144. *Id.* at 6–7.

145. Bruce Schneier, *WannaCry Ransomware*, SCHNEIER ON SECURITY (May 19, 2017, 6:10 AM), https://www.schneier.com/blog/archives/2017/05/wannacry_ransom.html.

146. *Id.*

147. *See* Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761, 770 (2018).

As Bruce Schneier has observed:

> Everything is becoming a computer. Your microwave is a computer that makes things hot. Your refrigerator is a computer that keeps things cold. Your car and television, the traffic lights and signals in your city and our national power grid are all computers. This is the much-hyped Internet of Things (IoT). It's coming, and it's coming faster than you might think. And as these devices connect to the Internet, they become vulnerable to ransomware and other computer threats.[148]

B. Bribery, Corruption, FCPA, and the UK Bribery Act

Laws designed to prohibit bribery and corruption have existed for many years. Notable among these are the Foreign Corrupt Practices Act (FCPA)[149] in the United States, the U.K. Bribery Act,[150] and the OECD Convention on Combating Bribery.[151] International bribery and corruption schemes have also employed cyber tools to assist in the payment of funds conveyed for nefarious purposes. The anonymity of cryptocurrencies provides obvious benefits to those seeking to mask payments for such things as armaments, ransom, or bribes to officials of foreign governments.[152]

---

148. Schneier, *supra* note 124.

149. *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors*, 6 VA. L. & BUS. REV. 145, 146 (2011); Lawrence J. Trautman & Kara Altenbaumer-Price, *Foreign Corrupt Practices Act: An Update on Enforcement and SEC and DOJ Guidance*, 41 SEC. REG. L.J. 241, 244 (2013), http://ssrn.com/abstract=2293382.

150. *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *Lawyers, Guns, and Money: The Bribery Problem and U.K. Bribery Act*, 47 INT'L LAW. 481, 481 (2013).

151. *See generally* Lawrence J. Trautman & Joanna Kimbell, *Bribery and Corruption: The COSO Framework, FCPA, and U.K. Bribery Act*, 30 FLA. J. INT'L L. 481 (2019), http://ssrn.com/abstract=3239193.

152. *See* Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447, 467–68 (2018), https://ssrn.com/abstract=3182867; Lawrence J. Trautman, *How Law Operates in a Wired Global Society: Cyber and E-Commerce Risk*, PROCEEDS KOREA LEGIS. RES. INS. 21–22 (Sept. 28, 2017), https://ssrn.com/abstract=3033776; Adam J. Sulkowski, Blockchain, Law, and Business Supply Chains: The Need for Governance and Legal Frameworks to Achieve Sustainability 3 (unpublished manuscript), https://ssrn.com/abstract=3205452.

VII. GOVERNANCE AND THE ORMEROD-TRAUTMAN SECURITY MODEL

Undoubtedly, the decision to notify law enforcement of a cyber-attack and to cooperate fully in an investigation involves a certain risk-reward calculation weighing the anticipated benefits of a pro-active approach against potential legal, reputational, and other costs.[153]

–Rod Rosenstein,
Deputy Attorney General

This Part begins by discussing the legal duty of each corporate board member owes to the shareholders for the governance of the corporation, including the productive functioning of the board in protecting the corporation from cyberthreats like ransomware.

A. Legal Responsibilities and Duties of Directors

State granted charters create corporations; their governance is dictated by state law, with corporate directors responsible for managing the affairs of the corporation.[154] Delaware law provides that directors owe their corporation and shareholders fiduciary duties of care and loyalty.[155] The duty of loyalty stands for the proposition that

---

153. *See* Rosenstein, *supra* note 6.

154. DEL. CODE ANN. tit. 8, § 141(a) (1991) ("The business and affairs of a corporation organized under this chapter shall be managed by or under the direction of a board of directors, except as may be otherwise provided in this chapter or in its certificate of incorporation."). While more than half of all publicly owned United States corporations are chartered under the laws of the state of Delaware, corporate counsel and directors will want to closely examine the laws of relevant states when considering any particular matter. *See* Stephen M. Bainbridge, *Why a Board? Group Decisionmaking in Corporate Governance*, 55 VAND. L. REV. 1, 4 (2002); Ronald J. Gilson & Reinier Kraakman, *Delaware's Intermediate Standard for Defensive Tactics: Is There Substance to Proportionality Review?*, 44 BUS. LAW. 247, 248 (1989) ("Delaware corporate law . . . governs the largest proportion of the largest business transactions in history."); Lawrence J. Trautman, *Who Sits on Texas Corporate Boards? Texas Corporate Directors: Who They Are & What They Do*, 16 HOUS. BUS. & TAX L.J. 44, 86, 91–97 (2016) (describing the experience and demographics of corporate directors in Texas); Lawrence J. Trautman, *Corporate Boardroom Diversity: Why Are We Still Talking About This?*, 17 SCHOLAR 219, 242–48 (2015).

155. *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 322–23 (2011) (citing Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1985)); *see also* Stephen M. Bainbridge et al., *The Convergence of Good Faith and Oversight* 5–9 (UCLA Sch. of Law, Law-Econ. Research Paper No. 07-09), http://ssrn.com/abstract=1006097; Bernard S. Black, *The Core Fiduciary Duties of Outside Directors*, ASIA BUS. L. REV., July 2001, at 1, 3; Julian Velasco, *How Many*

directors "must act in good faith and must not allow his personal interests to prevail over the interests of the corporation."[156]

Even when Directors make mistakes, the business judgment rule often provides a safe harbor. Delaware courts have stated that the business judgment rule is a "presumption 'that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company.'"[157] Professor Stephen M. Bainbridge has observed that the business judgment rule "pervades every aspect of state corporate law."[158] A discussion by former SEC commissioners and seasoned legal experts contends that external events or pressures can cause a crisis; as such, cyber-attacks can seriously disrupt or harm

---

Fiduciary Duties Are There in Corporate Law?, 83 S. CAL. L. REV. 1231, 1268 (2010); *cf.* Eric J. Pan, *Rethinking the Board's Duty to Monitor: A Critical Assessment of the Delaware Doctrine*, 38 FLA. ST. U. L. REV. 209, 209 (2011) (assessing the duty to monitor). *But see* Bernard S. Black et al., *Outside Director Liability*, 58 STAN. L. REV. 1055, 1074–76 (2006); Stuart R. Cohn, *Demise of the Director's Duty of Care: Judicial Avoidance of Standards and Sanctions Through the Business Judgment Rule*, 62 TEX. L. REV. 591, 602–03 (1983); William T. Allen, *Modern Corporate Governance and the Erosion of the Business Judgment Rule in Delaware Corporate Law* 11–13 (CLPE Research Paper No. 06/2008), http://ssrn.com/abstract=1105591.

156. BYRON F. EGAN, HOW RECENT FIDUCIARY DUTY CASES AFFECT ADVICE TO DIRECTORS AND OFFICERS OF DELAWARE AND TEXAS CORPORATIONS 7 (Feb. 13, 2015) (citing Gearhart Indust., Inc. v. Smith Int'l, Inc., 741 F.2d 707, 719 (5th Cir. 1984)); *see also* Dalia Tsuk Mitchell, *Status Bound: The Twentieth Century Evolution of Director's Liability*, 5 N.Y.U. J.L. & BUS. 63, 119 (2009).

157. Dalia Tsuk Mitchell, *The Import of History to Corporate Law*, 59 ST. LOUIS U. L.J. 683, 690–91 (2015) (quoting Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984)); *see also* Sean J. Griffith, *Good Faith Business Judgment: A Theory of Rhetoric in Corporate Law Jurisprudence*, 55 DUKE L.J. 1, 11–12 (2005); Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139, 1148 (2013).

158. Stephen M. Bainbridge, *The Business Judgment Rule As Abstention Doctrine*, (UCLA Sch. of Law, Law and Econ. Research Paper No. 03-18), http://ssrn.com/abstract=429260. *See generally* Douglas M. Branson, *The Rule That Isn't a Rule—the Business Judgment Rule*, 36 VAL. U. L. REV. 631 (2002); Deborah A. DeMott, *Corporate Officers As Agents*, 74 WASH. & LEE L. REV. 847 (2017); Lisa M. Fairfax, *Spare the Rod, Spoil the Director? Revitalizing Directors' Fiduciary Duty Through Legal Liability*, 42 HOUS. L. REV. 393 (2005); Darian M. Ibrahim, *Individual or Collective Liability for Corporate Directors?*, 93 IOWA L. REV. 929 (2008); Lyman P.Q. Johnson, *Corporate Officers and the Business Judgment Rule*, 60 BUS. LAW. 439 (2005); Bernard S. Sharfman, *The Importance of the Business Judgment Rule*, 14 N.Y.U. J.L. & BUS. 27 (2017); Robert Sprague & Aaron J. Lyttle, *Shareholder Primacy and the Business Judgment Rule: Arguments for Expanded Corporate Democracy*, 16 STAN. J.L. BUS. & FIN. 1 (2011); John C. P. Goldberg, The Fiduciary Duty of Care (unpublished manuscript), https://ssrn.com/abstract=3182604.

a business.[159] In all cases of corporate crisis, "[w]hatever the cause, the Board is expected to act quickly and effectively to mitigate the damage to the company."[160] The foundation of corporate governance is constructed upon the key duties of corporate directors: the duty of care, the duty of loyalty, and the duty of good faith.

B. Duty of Care

A careful, diligent approach to the effective discharge of every director's duties and responsibilities is required to satisfy the legal concept of duty of care. Professors Lyman P.Q. Johnson and Mark Sides note:

> The duty of care specifies the manner in which directors must discharge their legal responsibilities . . . includ[ing] electing, evaluating, and compensating corporate officers; reviewing and approving corporate strategy, budgets, and capital expenditures; monitoring internal financial information systems and financial reporting obligations, and complying with legal requirements; making distributions to shareholders; approving transactions not in the ordinary course of business; [and] appointing members to committees and discharging committee assignments, including the important audit, compensation and nominating committees . . . .
>
> The duty of due care arises in both the discrete decision-making context *and in the oversight and monitoring areas.* In the decision-making setting—whether it involves directors making a routine business decision or responding to a high-stakes unsolicited bid for corporate control—the duty of care inquiry clearly focuses on a board's 'decision-making process.' Directors in that setting are under an obligation to obtain and act with due care on all material information reasonably available.[161]

---

159. Alan Beller et al., panelists, The Role of Corporate Directors in a Corporate Crisis, Denit Trust Challenges in Corporate Governance Series: George Washington University School of Law 32 (Oct. 21, 2013) (discussion materials available at http://business.gwu.edu/about-us/research/institute-for-corporate-responsibility/the-series-on-corporate-governance/#Q7).

160. *Id.*

161. Lyman P.Q. Johnson & Mark A. Sides, *Corporate Governance and the Sarbanes-Oxley Act: The Sarbanes-Oxley Act and Fiduciary Duties,* 30 WM. MITCHELL L. REV. 1149, 1197 (2004); *see also* William T. Allen et al., *Realigning the Standard of*

In the landmark 1985 corporate governance case *Smith v. Van Gorkom*,[162] the Delaware Supreme Court found that the experienced and sophisticated directors[163] of Trans Union Corporation were not entitled to the protection of the business judgment rule[164] and had breached their fiduciary duty to their shareholders "(1) by their failure to inform themselves of all information reasonably available to them and relevant to their decision to recommend the Pritzker merger; and

---

Review of Director Due Care with Delaware Public Policy: A Critique of Van Gorkom *and Its Progeny As a Standard of Review Problem*, 96 NW. U. L. REV. 449, 449–51 (2002). *See generally* Lucian A. Bebchuk et al., *Director Liability*, 31 DEL. J. CORP. L. 1011 (2006); Christopher M. Bruner, *The Fiduciary Enterprise of Corporate Law*, 74 WASH. & LEE L. REV. 791 (2017); Christopher M. Bruner, *Is the Corporate Director's Duty of Care a "Fiduciary" Duty? Does It Matter?*, 48 WAKE FOREST L. REV. 1027 (2013); Donald C. Langevoort, Internal Controls After Sarbanes-Oxley: Revisiting *Corporate Law*'s "Duty of Care as Responsibility for Systems" (unpublished manuscript), http://ssrn.com/abstract=808084.

162. 488 A.2d 858 (Del. 1985). Two decades after the Delaware Supreme Court's landmark decision, authors continue to discuss *Smith v. Van Gorokom* in corporate governance. *See* Lawrence A. Hamermesh, *Twenty Years after* Smith v. Van Gorkom*: An Essay on the Limits of Civil Liability of Corporate Directors and the Role of Shareholder Inspection Rights*, 45 WASHBURN L.J. 283, 283–84 (2006); Stephen J. Lubben & Alana J. Darnell, *Delaware's Duty of Care*, 31 DEL. J. CORP. L. 589, 590–91 (2006); Robert T. Miller, Smith v. Van Gorkom *and the* Kobayashi Maru*: The Place of the Trans Union Case in the Development of Delaware Corporate Law*, 9 WM. & MARY L. REV. 65, 70–71 (2017); Steven A. Ramirez, *The Chaos of* Smith, 45 WASHBURN L.J. 343, 343 (2006); Bernard S. Sharfman, *The Enduring Legacy of* Smith v. Van Gorkom, 33 DEL. J. CORP. L. 287, 288, 289–90 (2008); Bernard S. Sharfman, *Being Informed Does Matter: Fine Tuning Gross Negligence Twenty Plus Years after* Van Gorkom, 62 BUS. LAW. 135, 136, 138 (2006); Cheryl L. Wade, *What Independent Directors Should Expect from Inside Directors:* Smith v. Van Gorkom *As a Guide to Intra-Firm Governance*, 45 WASHBURN L.J. 367, 368 (2006). *See generally* Stephen M. Bainbridge, Smith v. Van Gorkom (UCLA Sch. of Law, Law-Econ. Research Paper No. 08-13), http://ssrn.com/abstract=1130972.

163. *See* Trautman & Altenbaumer-Price, *supra* note 156, at 323, 323 n.55 (citing PETER V. LETSOU, CASES AND MATERIALS ON CORPORATE MERGERS AND ACQUISITIONS 643 n.21(Erwin Chemerinsky et al. eds. 2006)) ("Trans Union's five 'inside' directors had backgrounds in law and accounting, 116 years of collective employment by the company and 68 years of combined experience on its Board. Trans Union's five 'outside' directors included four chief executives of major corporations and an economist who was a former dean of a major school of business and chancellor of a university. The 'outside' directors had 78 years of combined experience as chief executive officers of major corporations and 50 years of cumulative experience of Trans Union. Thus, defendants argue that the Board was eminently qualified to reach an informed judgment on the proposed 'sale' of Trans Union notwithstanding their lack of any advance notice on the proposal, the shortness of their deliberation, and their determination not to consult with their investment banker or to obtain a fairness opinion.").

164. *Van Gorkom*, 488 A.2d at 888.

(2) by their failure to disclose all material information such as a reasonable shareholder would consider important in deciding whether to approve the Pritzker offer."[165] Before the corporate takeover decision involving the Trans Union board, "courts had rarely found individual directors liable for breaching their duty of care absent accompanying disloyal acts."[166] With an analogy that seems to follow the clear and present danger logic of contemporary cybersecurity threat, the Business Roundtable says of the September 11, 2001 terrorist attacks:

> According to Judge Alvin Hellerstein, who administered the lawsuits resulting from the attacks, principles of 'duty of care' and 'foreseeable risk' were forever altered by the tragic attacks. For example, according to Judge Hellerstein: 'Defendants argue that the ground victims lost their lives and suffered injuries from an event that was not reasonably foreseeable, for terrorists had not previously used a hijacked airplane as a suicidal weapon to destroy buildings and murder thousands.' He continued, 'Defendants contend that because the events of September 11 were not within the reasonably foreseeable risks, any duty of care that they would owe to ground victims generally should not extend to the victims of September 11. According to the Court's decision, however, corporate leaders now also must adopt strategies to manage widespread infrastructure disruptions and crises resulting from previously unforeseeable terrorist attacks or nonmalicious infrastructure failures.[167]

---

165. PETER V. LETSOU, CASES AND MATERIALS ON CORPORATE MERGERS AND ACQUISITIONS 644 (Erwin Chemerinsky et al. eds. 2006).

166. Jacqueline M. Veneziani, *Causation and Injury in Corporate Control Transactions:* Cede & Co. v. Technicolor, Inc., 69 WASH. L. REV. 1167, 1167 & n.3 (1994) ("Before *Van Gorkom* was decided, one commentator had stated that '[t]he search for cases in which directors . . . have been held liable in derivative suits for negligence uncomplicated by self-dealing is a search for a very small number of needles in a very large haystack.'" (quoting Joseph W. Bishop, Jr., *Sitting Ducks and Decoy Ducks: New Trends in the Indemnification of Corporate Directors and Officers*, 77 YALE L.J. 1078, 1099 (1968)).

167. BUSINESS ROUNDTABLE, COMMITTED TO PROTECTING AMERICA: CEO GUIDE TO SECURITY CHALLENGES 81 (2005), http://www.cj.msu.edu/~outreach/wmd/ceo_guide.pdf.

C. Duty of Good Faith

A director must be able to demonstrate that she acted in "good faith" to effectively invoke the business judgment rule in defending against a claim for breach of fiduciary duty.[168] Professor Janet E. Kerr writes, "[b]ecause the duty of good faith has not been clearly defined nor fully developed, its definition and application are being driven by numerous forces."[169] Many factors "define what it means for a corporate director to act in good faith[,] . . . includ[ing] the judicial application of state corporate law, federal and state legislation, shareholder activism, . . . corporate governance ratings, and the expectations of the public in response to the media's treatment of current issues in corporate governance."[170] *Stockbridge v. Gemini Air Cargo, Inc.* stands for the proposition that "the board of directors of a Delaware corporation [is charged with] the legal responsibility to manage its business for the benefit of the corporation and its shareholders with 'due care, good faith, and loyalty.'"[171] According to Professor Kerr, "[r]ecognizing that directors have a fiduciary duty to manage a corporation with good faith in the best interests of all its shareholders and of the long-term health of the corporation, the court opined that whether directors have acted in good faith is a question of fact."[172] In addition:

> Whether the duty to act in good faith is merely a subset of the duties of care and loyalty, a duty separate and freestanding from the other two duties, or a duty similar to the duty of good

---

168. *See id.* at n.45; *see also* Christopher M. Bruner, *Good Faith, State of Mind, and the Outer Boundaries of Director Liability in Corporate Law*, 41 WAKE FOREST L. REV. 1131, 1137–38 (2006); Sean J. Griffith, *Good Faith Business Judgment: A Theory of Rhetoric in Corporate Law Jurisprudence*, 55 DUKE L.J. 1, 9–13, 15–16 (2005); Leo E. Strine, Jr. et al., *Loyalty's Core Demand: The Defining Role of Good Faith in Corporation Law*, 98 GEO. L.J. 629, 633 (2010); Hillary A. Sale, *Good Faith's Procedure and Substance*, In re Caremark International Inc., Derivative Litigation 8 (U. Iowa Legal Studies Research Paper No. 08-02), http://ssrn.com/abstract=1133570; *cf.* Melvin A. Eisenberg, *The Duty of Good Faith in Corporate Law*, 31 DEL. J. CORP. L. 1, 5 (2006).

169. Janet E. Kerr, *Developments in Corporate Governance: The Duty of Good Faith and Its Impact on Director Conduct*, 13 GEO. MASON L. REV. 1037, 1038 (2006).

170. *Id. See generally* Hillary A. Sale, *Delaware's Good Faith*, 89 CORNELL L. REV. 456 (2004).

171. Kerr, *supra* note 170, at 1045 (quoting Stockbridge v. Gemini Air Cargo, Inc., 611 S.E. 2d 600, 606 (Va. 2005)). For more information about the duty of loyalty, see Julian Velasco, *The Diminishing Duty of Loyalty*, 75 WASH. & LEE L. REV. 1035, 1038 (2018).

172. *See* Kerr *supra* note 170, at 1046 (citing *Stockbridge*, 611 S.E.2d at 605).

faith required in the contractual context, remains to be answered. Importantly, the duty of good faith could be held to encompass compliance with the expectations of the parties involved and conformity to the spirit of the fiduciary relationship. Finally, despite inconsistency and uncertainty, under the emerging definition of the duty of good faith, directors may be held personally liable for corporate misbehavior if their conduct evidences improper motive or ill will, a reckless disregard of known risks, a sustained failure to oversee management, or is so egregious that it is unexplainable on any other grounds other than bad faith.[173]

According to Delaware Chief Justice E. Norman Veasey,

[F]ailure to follow the minimum expectations of the evolving standards of director conduct, the . . . Sarbanes-Oxley, or the NYSE or NASDAQ Rules (when . . . approved by the SEC) might likewise raise a good faith issue. There is no definitive answer to that question, but counsel should advise the directors of that possible exposure and encourage the utmost good faith behavior.[174]

Consider:

[T]he evolving business and judicial expectations of director conduct over the years are part of the common law grist for the fiduciary duty mill. As Chancellor Allen stressed in *Caremark*, the kind of sustained inattention of directors exemplified by the failure to institute law compliance programs contemplated by the federal sentencing guidelines and expected of prudent businesses could be held to be a violation of fiduciary duty of good faith. That standard of conduct—good faith—is key to director conduct, and it must be considered when one looks at the directors' processes and motivations to be certain that they are honest and not disingenuous or reckless.[175]

---

173. *Id.* at 1051.

174. E. Norman Veasey, *Policy and Legal Overview of Best Corporate Governance Principles*, 56 SMU L. REV. 2135, 2141 (2003). *See generally* Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* OXFORD HANDBOOK OF FIDUCIARY LAW 12–14 (forthcoming 2019), https://ssrn.com/abstract=3197941.

175. Veasey, *supra* note 175, at 2141; *see also* Robert T. Miller, *Oversight Liability for Risk-Management Failures at Financial Firms*, 84 S. CAL. L. REV. 47, 81

D. Cyber Enterprise Risk Management

While a comprehensive discussion of cyber enterprise risk management far exceeds the scope of this Article, some useful resources are listed below.[176] Here, we pause to reflect upon the basic duties of loyalty and care imposed by law on corporate directors.

E. Ormerod-Trautman Profit Maximizing Model of Security

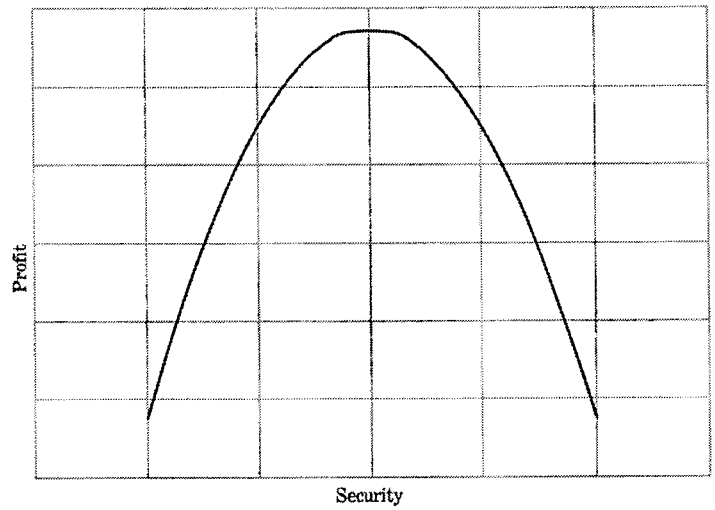
Professors Ormerod and Trautman present a way to think about the management of cybersecurity, *The Profit-Maximizing Model of Security*, in Exhibit 3.[177]

(2010); Christine Hurt, *The Duty to Manage Risk* 5–7 (U. of Ill. College of Law, Behavior and Social Science Paper No. LBSS14-09), http://ssrn.com/abstract=2308007.

176. *See generally* Michelle M. Harner, *Ignoring the Writing on the Wall: The Role of Enterprise Risk Management in the Economic Crisis*, 5 J. BUS. & TECH. L. 45 (2010) ("examin[ing] the different approaches to enterprise risk management . . . and how ERM contributed to the survival or failure of [] firms"); Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230 (2016); Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-commerce, Political and Regulatory Compliance Risks*, 10 WM. & MARY BUS. L. REV. 1 (2018) (answering "What are the major cyber risks perceived by those engaged in the universe of Internet businesses?"); Lawrence J. Trautman, *E-Commerce and Electronic Payment System Risks: Lessons from PayPal*, 16 U.C. DAVIS BUS. L.J. 261 (2016); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341 (2015); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works*, 5 J.L. & CYBER WARFARE 147 (2016); Lawrence J. Trautman & Janet Ford, *Nonprofit Governance: The Basics*, 52 AKRON L. REV. 1, 64–66 (forthcoming).

177. Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1290 (2017); Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. ___ (forthcoming 2019), https://ssrn.com/abstract=3340674.

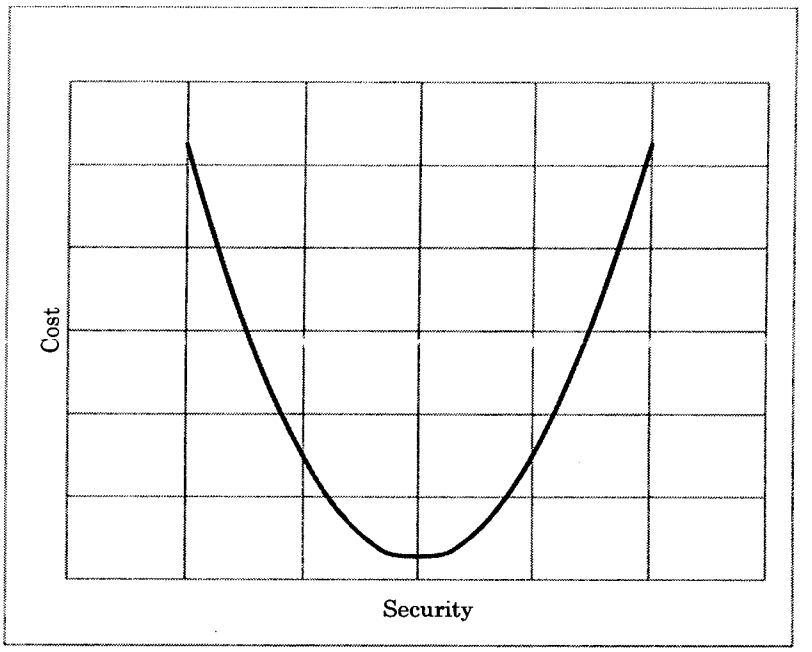
Exhibit 3
The Ormerod-Trautman Profit-Maximizing Model of Security[178]



Note that at the leftmost point on the curve, enterprise data security is so abysmal that few, if any, users trust the enterprise with their Personally Identifiable Information (PII), therefore rendering the profitability or efficiency of the enterprise's data security function a nullity. To paraphrase, zero security measures, as shown at the bottom left-hand side of the graph, result in zero users and, therefore, zero profitability (efficiency). But, as the enterprise security improves an increasing number of users trust the enterprise with their PII, and the risk of data breach and loss of users' PII decreases, both of which contribute to increased profitability (efficiency). At a point where the number of users is maximized, increased security measures (spending on cybersecurity) result in limiting the usability of the data/website and thus decrease profitability (efficiency). Thus, taken to an extreme, excessive security measures may theoretically drive usability to the point of futility, achieving no additional benefit from the next dollar spent on cybersecurity and decreasing utility of additional spend. For nonprofits, the Ormerod-Trautman Model can be rephrased to illustrate the "cost-minimizing" level of security, as shown in Exhibit 4.[179]

178. Trautman & Ormerod, *supra* note 178, at 1290.
179. Trautman & Ford, *supra* note 177, at 68.

Exhibit 4
Ormerod-Trautman Nonprofit Cost-Minimizing Model of Security



On the left, as Professor Ormerod explains, "[C]yber services are costly due to the threat of litigation and penalties; on the right, cyber services are costly because they are prohibitively difficult to use and cost money to generate/host. This re-conception allows nonprofits and governments to express security within the confines of a dollar amount."[180] "The critical takeaway is that little or no digital security may be just as damaging to an enterprise's financial health as implementing overly excessive security."[181]

> As this area of the law develops and matures in the coming years, courts, regulators, shareholders, and commentators will increasingly view the relationship between data security and enterprise efficiency as described in [Exhibits 3 and 4 herein]. Perhaps the most important implication of embracing the relationship depicted in the Ormerod-Trautman model is that there is a profit-maximization [or cost effective] amount of security. And, as this view of the relationship between security

180. *Id.*
181. *Id.*

and profitability is embraced, there can be little doubt that the various constituencies of stakeholders will increasingly expect corporate officers and directors to actively seek their company's profit-maximizing level of data security.[182]

VII. THE CURRENT CYBERSECURITY LEGAL FRAMEWORK

We cannot have a society in which some dictator someplace can start imposing censorship here in the United States. Because if somebody is able to intimidate folks out of releasing a satirical movie, imagine what they start doing when they see a documentary that they don't like, or news reports that they don't like. Or even worse, imagine if producers and distributors and others start engaging in self-censorship because they don't want to offend the sensibilities of somebody whose sensibilities probably need to be offended.[183]

–President Barak Obama

Emerging threats like WannaCry demonstrate in stark relief the risks to corporate directors and officers who are ill-prepared to confront digital threats. As detailed in this Part, a complicated patchwork of authorities makes compliance with applicable law a difficult and complex task. But corporate directors need not dismay: the law favors a comprehensive process-based approach to defending organizations, complex and simple alike, from cyber threats. As further detailed below, implementing a Written Information Security Process (WISP) is an approach we believe all organizations should be undertaking to ensure compliance with a dizzying variety of cybersecurity-related legal authorities.

A. Sources of Cybersecurity Legal Authority

There is no one, single comprehensive authority for cybersecurity-related legal duties.[184] Instead, organization obligations to implement data security systems are "set forth in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement

182. Trautman & Ormerod, *supra* note 178, at 1291.

183. President Barak Obama, Remarks by the President in Year-End Press Conference (Dec. 19, 2014) (transcript available at https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference).

184. *See* Trautman & Ormerod, *supra* note 178, at 1235.

actions, as well as common law duties, contractual commitments, and other expressed and implied obligations to provide 'reasonable' or 'appropriate' security for corporate data."[185]

There are many different types of statutes and regulations that have digital security components; these include privacy laws, data security laws, electronic transaction laws, corporate governance laws, unfair and deceptive business practice and consumer protection laws, and breach notification laws.[186]

Federal privacy statutes include: the Financial Services Modernization Act of 1999,[187] which governs financial information; Health Insurance Portability and Accountability Act of 1996,[188] which governs healthcare information; the Children's Online Privacy Protection Act,[189] which applies to anyone who collects personal information on the Internet from children; and the Privacy Act of 1974, which provides governmental record-keeping requirements.[190] Some federal regulations impose a duty to protect specific types of information, such as IRS Revenue Procedures requiring security measures to protect electronic tax records[191] and SEC regulations requiring the protection of corporate financial data.[192]

Many states have enacted data security statutes that impose "a general obligation on all companies to ensure the security of personal information."[193] California was the first state to enact this type of law, and it requires all businesses to "implement and maintain reasonable security procedures and practices" to protect California residents' personal information against "unauthorized access, destruction, use, modification, or disclosure."[194]

---

185. THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE 29 (2008).

186. *See* Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors 4–6 (Oct. 8, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323.

187. Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999 ("GLBA"), Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 and 15 U.S.C.).

188. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 and 42 U.S.C.).

189. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–02 (2012).

190. Privacy Act of 1974, 5 U.S.C. § 552(a) (2012).

191. *See* Rev. Proc. 97-22, 1997-1 C.B. 652; Rev. Proc. 98-25, 1998-11 I.R.B. 7.

192. *See* 17 C.F.R. §§ 240.17a-4, 248.30 (2015); 17 C.F.R. § 257.1(e)(3) (2011).

193. *See* Smedinghoff, *supra* note 187, at 5.

194. CAL. CIV. CODE § 1798.81.5(b) (West 2016).

There are electronic transaction laws that apply at both the federal[195] and state[196] levels. These laws are intended to maintain the fidelity, accuracy, and enforceability of electronic documents, and they also require data security for electronic record-keeping. Both federal and state law mandate companies secure electronic records that relate to online transactions, primarily through requirements concerning the data's accessibility, integrity, and accuracy.[197]

B. The Need to Implement a WISP Protocol

Of the authorities discussed above that impose a data security duty, most simply state that there is "an obligation to implement 'reasonable' or 'appropriate' security measures," but they "provide little or no guidance as to what is required for legal compliance."[198] While there is little question that the legal standard for what constitutes reasonable security is still emerging, much progress has been made in recent years.

Thomas J. Smedinghoff, a leading expert on this emerging cybersecurity standard, explains that the emerging digital security standard is particularized and case specific.[199] Unlike prior specific requirements, such as passwords or firewalls, the new corporate security obligation is fact-specific, requiring companies to go through a "process" and determine what security measures are most appropriate for the company's security needs.[200] The emerging legal standard follows suit by allowing companies to create their own specific security measures so long as the companies conduct ongoing reviews of their security mechanisms.[201] This repetitive review process includes detecting and evaluating risks, implementing specific security responses to those risks, verifying the effective implementation of those security responses, and updating the measures as needed in reaction to developing security concerns.[202]

---

195. *See* C.F.R. §§ 240.17a-4, 248.30; C.F.R. § 257.1(e)(3).

196. NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, UNIFORM ELECTRONIC TRANSACTIONS ACT § 7 (1999).

197. *See id.* § 12; *see also* 15 U.S.C. § 7001(d)–(e) (clarifying that statutory requirements to retain documents or to execute documents in writing are satisfied by electronic documents so long as the electronic versions are accurate and accessible).

198. *See* Smedinghoff, *supra* note 187, at 9.

199. *Id.* at 9–10.

200. *Id.* at 10.

201. *Id.*

202. *Id.*

Specifically, Mr. Smedinghoff's process-oriented approach to satisfying a "reasonable" or "appropriate" standard of care for a duty to provide security is composed of the following seven provisions[203]:

- "*Assign Responsibility*": A corporation should expressly designate one or more employees to be responsible for maintaining the data security program.
- "*Identify Information Assets*": A corporation should identify its information assets that require protection, which include both the data itself (i.e., records containing personal information) and the computing systems that store the personal information (e.g., servers, laptops, and portable devices).
- "*Conduct Risk Assessment*": A corporation should perform a risk assessment to identify both internal and external risks to its data security, and it should evaluate the effectiveness of the company's current practices for safeguarding and minimizing the risks identified.
- "*Select and Implement Responsive Security Controls*": A corporation should implement physical, administrative, and technical security controls it considers appropriate to minimize the risks it identified in its risk assessment.
- "*Monitor Effectiveness*": A corporation should *regularly* monitor, test, and reassess the security controls it has chosen to implement to ensure its security program is operating in a manner reasonably calculated to protect personal information. Relatedly, a corporation should regularly upgrade its security controls as necessary to limit emerging risks.
- "*Regularly Review the Security Program*": A corporation should review and adjust its data security program no less than once per year. A corporation should also perform security program reviews whenever there is a material change in business practices that could affect personal information or after any incident involving a breach of its data security.
- "*Address Third Party Issues*": A corporation should take all reasonable steps to verify that every third-party service provider that has access to the company's data assets and

203. *Id.*

> personal information has the capacity to protect that information.[204]

An ever-increasing number of authorities are expressly adopting this process-oriented approach to data security, which is referred to as a Written Information Security Program (WISP).[205] The FTC is the most important of the authorities that have adopted the WISP standard. According to the FTC, businesses in all industries should comply with the process-oriented approach to information security as it demonstrates the "best practice" for legal compliance.[206] The FTC has demonstrated this view by requiring any company resolving FTC complaints about failure to provide adequate information security through consent decrees to implement and comply with this process-oriented approach.[207] The FTC's adherence to the WISP standard is particularly important in light of the agency's post-2005 theory of liability that sanctions a duty to protect data.[208]

As a precautionary measure, the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) recommends the following basic hygiene for defending against ransomware:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.

---

204. *Id.*

205. *See id.* at 11; *see also, e.g.*, 201 HIPAA Security Standards, 45 C.F.R. § 164.308 (2018); 201 MASS. CODE REGS. § 17.03 (2017). *See generally* Bruce Radke & Michael J. Waters, *Selected State Laws Governing the Safeguarding and Disposing of Personal Information*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 487 (2015) (comparing different state WISP regulations).

206. *See* Smedinghoff, *supra* note 187, at 11("'[T]he FTC Safeguards Rule promulgated under the GLB Act serves as a good model' for satisfying the obligation to maintain reasonable and appropriate security." (citing *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Tech. & Homeland Sec. of the S. Comm. on the Judiciary*, 110th Cong. 93 (statement of Lydia Parnes, Dir., Bureau of Consumer Prot., FTC)).

207. *Id.*

208. *See, e.g.*, Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine*, 4 J.L. & CYBER WARFARE 109, 124, 127–28 (2014) (describing the duty to protect in the context of the responsibilities of company director to be informed and actively engaged in cybersecurity issues that arise in a company).

- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.
- Only download software—especially free software—from sites you know and trust.
- Enable automated patches for your operating system and Web browser."[209]

CONCLUSION

Businesses must confront information security risks in a systematic way. Global policymakers and corporate stakeholders increasingly expect complex institutions to implement process-based security solutions. This focus on process may, however, wane over time, as robust procedures give way to substantive rules.[210]

Ransomware poses particularly vexing problems. Given the rapid rate of technological change, our world increasingly becomes smaller and more interconnected. Global data systems interact with increasing frequency. Ransomware threatens institutions worldwide, but the risks for businesses are all the starker—potentially catastrophic. Business leaders are responsible for ensuring that their organizations have considered and addressed these threats.

---

209. *See* NCCIC, *supra* note 11.
210. *See, e.g.*, Ormerod, *supra* note 177.