Journal of International Business and Law

Volume 22 | Issue 1 Article 6

12-1-2023

To Ban Ransomeware Payments or Not to Ban Ransomware Payments: The Problems Drafting Legislation in Reponse to Ransomware

Sean O'Connell

TO BAN RANSOMWARE PAYMENTS, OR NOT TO BAN RANSOMWARE PAYMENTS: THE PROBLEMS OF DRAFTING LEGISLATION IN RESPONSE TO RANSOMWARE.

By: Sean O'Connell

I. INTRODUCTION

A. Ransomware attacks

i. A Broad History of Ransomware

Ransomware is malware that encrypts a victim's data, which is then used by hackers as leverage to request payment to unlock the encrypted data in exchange to not leak the stolen data.[1] The usual victims of ransomware attacks are entities with cyber insurance policies or entities with access to massive amounts of sensitive consumer data.[2] The average ransom demand for these cyberattacks is between fifty to seventy million dollars. However, these demands are usually negotiated and the costs of these attacks are often mitigated by cyber insurance policies that cover some or all the expense.[3] The estimated average payment of a ransomware attack is between ten and fifteen million dollars.[4]

ii. The Economic Impact of Ransomware Attacks

A ransomware attack shut-down information technology ("IT") systems, causing disruption to Ireland's public health service in May 2021.[5] Approximately one-third of

[1] *See* Kartikay Mehrotra, *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, BLOOMBERG (May 20, 2021), https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack; *see also* John G. Browning, *The Battle Against Ransomware*, DMAGAZINE (Dec. 11, 2019), https://www.dmagazine.com/publications/d-ceo/2019/december/the-battle-against-ransomware/.

[2] *See* Mehrota, *supra* note 1; *see also* Browning, *supra* note 1.

[3] *See* Mehrota, *supra* note 1; *see also* James Coker, *Average Ransomware Demands Surge by 518% in 2021*, INFOSECURITY-MAGAZINE (Aug. 9, 2021), https://www.infosecurity-magazine.com/news/ransomware-demands-surge-2021/.

[4] *See* Mehrota, *supra* note 1; *see also* Scott Ikeda, *'Cyber Insurance Gap' Growing as 80% Of Business Coverage Below Median Ransomware Payment Demand*, CPO MAGAZINE (Sept. 7, 2022), https://www.cpomagazine.com/cyber-security/cyber-insurance-gap-growing-as-80-of-business-coverage-below-median-ransomware-payment-demand/.

[5] *See* Gerrit De Vynck,, *The Anatomy of a Ransomware Attack*, THE WASHINGTON POST (Jul. 9, 2021), https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/; *see also* Catherine Stupp, *Irish Healthcare Service Shuts Down IT Systems After Ransomware Attack*, WSJ (May 14, 2021), https://www.wsj.com/articles/irish-healthcare-service-shuts-down-it-systems-after-ransomware-attack-11620998875.

American companies have cyber insurance.[6] However, it is increasingly harder to get cyber insurance as cyberattacks surge.[7] In October 2020, the University of Vermont Health Network was afflicted with a ransomware resulting in delayed chemotherapy and mammogram appointments for the hospitals in its network.[8] Cyberattacks on hospitals are dangerous as shut-down computer systems prevent access to patient scans, prevent physicians from accessing necessary tools to provide care, and creates backlogs in operating systems.[9] As hospitals are already strained from the Coronavirus pandemic, a ransomware attack could be quite devastating to the healthcare industry.[10]

Part I of this Note will address the history of ransomware attacks by describing how cryptocurrencies enabled the possibility of ransomware attacks and detailing the impacts of historically significant ransomware attacks. Part II will describe the current problems with prosecuting ransomware perpetrators. Part III will focus on the problems caused by the current state of affairs regarding ransomware payments (i.e. companies paying ransoms which facilitates this ransomware business model). Part IV focuses on measures taken to improve cyber security in response to ransomware and other cyber breaches. Part IV concludes by proposing amendments to a ransomware bill to respond to a potential ransomware attack more effectively. The goal of this Note is to urge the development of an established incident response plan and reporting procedures in anticipation of suspected ransomware attacks, despite the difficulties involved with preventing the payment of these attacks.

II. BACKGROUND/ HISTORY

A. Cryptocurrency's Role in Ransomware Attacks

i. Cryptocurrencies Impact on Ransomware Attacks

In the United States, ransomware payments are not prohibited, as this administration is sympathetic to ensuring the business continuity of ransomware victims.[11] However, the federal government is considering an outright prohibition of ransomware payments.[12] After the Colonial Pipeline hearings, Senator Gary Peters proposed draft legislation that would mandate

---

[6] *See* De Vynck, *supra* note 5; *see also* Howard Solomon, *Many North American Firms Have No Cyber Insurance Coverage: Survey*, IT WORLD CANADA (Aug. 10, 2022), https://www.itworldcanada.com/article/many-north-american-firms-have-no-cyber-insurance-coverage-survey/497173.

[7] *See* De Vynck, *supra* note 5; *see also* Solomon, *supra* note 6.

[8] *See* Nicole Wetsman, *The Pandemic Revealed the Health Risks of Hospital Ransomware Attacks*, THE VERGE (Aug. 19, 2021), https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks; *see also* Ellen Barry and Nicole Periroth, *Patients of a Vermont Hospital are Left 'in the Dark' After a Cyberattack*, The New York Times (Nov. 26, 2020), https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

[9] *See* Wetsman, *supra* note 8; *see also* Barry, *supra* note 8.

[10] *See* Wetsman, *supra* note 8; *see also* Barry, *supra* note 8.

[11] *See* Brock Dahl and Boris Feldman, *Ransomware Threat and Cybersecurity Regulation: What's Next?*, BLOOMBERG LAW (Jun. 25, 2021), https://news.bloomberglaw.com/privacy-and-data-security/ransomware-threat-and-cybersecurity-regulation-whats-next; *see also* Aamir Lakhani, *Ransomware Payments: What Should You Do?*, FORTINET (May 31, 2022), https://www.fortinet.com/blog/industry-trends/paying-ransomware.

[12] *See* Dahl & Feldman, *supra* note 11; *see also* Jane Blaney & Jason Weiss, *Federal Legislation Considers Banning Ransom Payments to Hackers*, JD SUPRA (Jun. 17, 2021), https://www.jdsupra.com/legalnews/federal-legislation-considers-banning-5827069/.

information sharing when a company endures a cyberattack.[13] Companies can prepare for a cyber incident by ensuring that their information technology staff develop robust backup systems and continuity plans.[14] Public companies in the United States should prepare for more robust disclosures regarding their cybersecurity risk governance frameworks to government entities.[15] These companies should also consider the federal government's response to using cryptocurrencies in ransomware attacks.

In 2008, an anonymous individual, or individuals, referred to as Satoshi Nakamoto ("Nakamoto") released a scientific white paper on the internet that originated the concept of cryptocurrency, leading to the creation of Bitcoin.[16] In this scientific white paper, Nakamoto envisioned a peer-to-peer electronic cash system enabling parties to send cash directly to each other without involving a financial institution.[17] Nakamoto claimed that the reliance on financial institutions as a trusted third-party to process electronic payments was problematic due to the "inherent weakness of the trust based model."[18] For example, completely non-reversible transactions are not possible, as financial institutions need to mediate disputes; mediation costs lead to an increase in transaction costs, limiting the minimum transaction size.[19] Nakamoto proposed an electronic payment system based on cryptographic proof, instead of a trust-based model.[20] Nakamoto claimed that this proposed electronic payment system would eliminate the reliance on financial institutions for processing electronic payments while protecting sellers from fraud.[21] Additionally, Nakamoto believed that buyers could be protected by implementing "routine escrow mechanisms."[22] The peer-to-peer transactional system envisioned by Nakamoto, sought to eliminate the need for a trusted third-party in an electronic payment transaction.[23] However, the United States Securities and Exchange Commission's ("SEC") regulation of cryptocurrencies, while not initially imagined in Nakamoto's model, will help mitigate the risk of ransomware attacks that are enabled by the use of cryptocurrencies.[24]

---

[13] *See* Dahl & Feldman, *supra* note 11; *see also* Blaney & Weiss, *supra* note 12.

[14] *See* Dahl & Feldman, *supra* note 11; *see also* Jim Boehm, et al., *Ransomware Prevention: How Organizations Can Fight Back*, MCKINSEY & CO. (Feb. 14, 2022), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/ransomware-prevention-how-organizations-can-fight-back.

[15] *See* Dahl & Feldman, *supra* note 11; Press Release, Securities & Exchange Commission, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Mar. 9, 2022).

[16] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (Jan. 3, 2022), https://bitcoin.org/bitcoin.pdf; Jamie Redman, *Walk Like Nakamoto: 7 Anonymous Personalities in the Crypto Space*, BITCOIN.COM (Nov. 13, 2019), https://news.bitcoin.com/walk-like-nakamoto-7-anonymous-personalities-in-the-crypto-space/.

[17] *See* Nakamoto, *supra* note 16.

[18] *See id.*

[19] *See id.*

[20] *See id.*

[21] *See* Nakamoto, *supra* note 16; Valentijn v/den Hout, *Satoshi Nakamoto's Bitcoin Whitepaper: A thorough and straightforward walk-through*, FREECODECAMP (Sept. 12, 2018), https://www.freecodecamp.org/news/satoshi-nakamotos-bitcoin-whitepaper-a-walk-through-3e9e1dee71ce/.

[22] *See* Nakamoto, *supra* note 16.

[23] *See* Nakamoto, *supra* note 16; *see also* Hout, *supra* note 21.

[24] *See* J. Scott Colesanti, *Sorry, They Were on Mute: The SEC's "Token Proposal 2.0" As Blueprint for Regulatory Response To Cryptocurrency*, Corp. & Bus. L.J., (Jan. 3, 2022) at 46; Caroline A. Crenshaw,

People may believe that anonymity in two-party transactions should be prioritized and that the field of cryptocurrency should not be regulated.[25] However, these individuals must realize that cryptocurrency transactions are not as anonymous as most people imagine.[26]

Cryptocurrencies are utilized to purchase items from underground marketplaces.[27] However, because of their traceability, cryptocurrencies are poor candidates for illegal activity.[28] For example, in 2015, two United States federal agents, Carl M. Force and Shaun Bridges, from the Drug Enforcement Agency ("DEA") and the United States Secret Service, sought to enrich themselves while performing an undercover investigation of the Silk Road drug marketplace.[29] While undercover, the agents were likely under the assumption that Bitcoin was anonymous and untraceable when they allegedly stole, bribed, blackmailed, and laundered proceeds, eventually getting charged with money laundering and wire fraud.[30] On July 1, 2015, Force pled guilty to money laundering with predicates of wire fraud and theft of government property, obstruction of justice, and extortion.[31] On August 31, 2015, Bridges confessed that he stole over $800,000 of Bitcoin while on the case and pleaded guilty to money laundering and obstruction of justice.[32] The case of Carl M. Force and Shaun Bridges exemplifies how Bitcoin can be utilized to disrupt illegal activities through the tracking of transactions.[33]

Many cyber criminals prefer to utilize cryptocurrencies, such as Bitcoin, as they believe it enables them to conduct illicit business without disclosing personal information such as their names or locations.[34] However, cryptocurrencies may not actually be as difficult to

Statement on DeFi Risks, Regulations, and Opportunities, U.S. SECURITIES AND EXCHANGE COMMISSION (Nov. 9, 2021), https://www.sec.gov/news/statement/crenshaw-defi-20211109.

[25] *See* Colesanti, *supra* note 24; *see also* Crenshaw, *supra* note 24.

[26] *See* Antony Lewis, THE BASICS OF BITCOINS AND BLOCKCHAINS (2018); Julian Dossett, *Are Cryptocurrency Transactions Actually Anonymous?*, CNET (Jun. 27, 2022) https://www.cnet.com/personal-finance/crypto/are-cryptocurrency-transactions-actually-anonymous/#:~:text=Are%20bitcoin%20transactions%20anonymous%3F,ransom%20payment%20from%20the%20attackers.

[27] *See* Lewis, *supra* note 26; *see also* Dossett, *supra* note 26.

[28] *See* Lewis, *supra* note 26; *see also* Dossett, *supra* note 26.

[29] *See* Lewis, *supra* note 26; *see also* Nate Raymond, *Ex-agent in Silk Road probe gets more prison time for bitcoin theft*, REUTERS (Nov. 7, 2017) https://www.reuters.com/article/us-usa-cyber-silkroad/ex-agent-in-silk-road-probe-gets-more-prison-time-for-bitcoin-theft-idUSKBN1D804H.

[30] *See* Nate Raymond, *Ex-agent in Silk Road probe gets more prison time for bitcoin theft*, REUTERS (Nov. 7, 2017) https://www.reuters.com/article/us-usa-cyber-silkroad/ex-agent-in-silk-road-probe-gets-more-prison-time-for-bitcoin-theft-idUSKBN1D804H.

[31] *See id.*

[32] *See id.*

[33] *See id.*

[34] *See* Katie Benner et al., *Pipeline Investigation Upends Idea That Bitcoin Is Untraceable*, N.Y TIMES (June 9, 2021), https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html; *see also* Tom Sadon, *5 Reasons Why Criminals & Terrorists Turn to Cryptocurrencies*, COGNYTE (Nov. 1, 2021) https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/; *see also* Tom Sadon, *5 Reasons Why Criminals & Terrorists Turn to Cryptocurrencies*, COGNYTE (Nov. 1, 2021) https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/ (stating one of the primary reasons that criminals use cryptocurrency is due to the anonymity in transactions since crypto addresses are made up of random sets of characters and there is no link between these addresses and their owners, allowing makers of transactions to remain anonymous).

track as cyber criminals believe.[35] For example, federal officials were able to recover the majority of the Bitcoin ransom paid in the Colonial Pipeline ransomware attack.[36] Bitcoin can be created, moved, and stored outside the purview of any government or financial institution, however, Bitcoin is still traceable as each payment is recorded in a fixed ledger, which is referred to as "the blockchain."[37] According to cryptocurrency experts, all that was necessary for law enforcement to track the Bitcoin in the Colonial Pipeline attack was to connect the criminals to a "digital wallet."[38] To do so, law enforcement probably focused on a "public key" or "private key."[39] A public key is a string of numbers and letters, which Bitcoin holders utilize for transactions with others; the private key is used to keep a digital wallet secure.[40] With a public key, authorities are able to track down a user's transaction history, and with a private key, authorities are able to seize assets.[41] Private keys of ransomware attackers are far more difficult for authorities to acquire and it still remains unclear how federal agents were able to acquire DarkSide's private key during the Colonial Pipeline cyber incident.[42] The Federal Bureau of Investigation ("FBI") has worked with several companies specializing in tracking cryptocurrencies across digital accounts.[43] Start-ups such as TRM Labs, Elliptic, and Chainalysis have thrived as law enforcement agencies and financial institutions are trying to keep pace with financial crime.[44] These startups use technology that trace blockchains and look

[35] *See* Benner, et. al., *supra* note 34; *see also* Sean Michael Kerner, *Colonial Pipeline Hack Explained: Everything You Need to Know*, WHATIS.COM (Apr. 26, 2022), https://www.techtarget.com/whatis/feature /Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[36] *See* Benner, et. al., *supra* note 34; *see also* Kerner, *supra* note 35 (stating the Department of Justice recuperated 63.7 Bitcoin ransom paid from the Colonial Pipeline attackers, equivalent to about $2.3 million dollars).

[37] *See* Benner, et. al., *supra* note 34; *see also* Rakesh Sharma, *What Does the Bitcoin Blockchain Record?*, INVESTOPEDIA (Sept. 23, 2021) https://www.investopedia.com/ask/answers/063015/what-does-block-chain-record-bitcoin-exchange-transaction.asp ("The Bitcoin blockchain is essentially an enormous, shared, encrypted list of all addresses that hold Bitcoin balances. Because this list is shared, it is referred to as a digital distributed ledger technology (DLT). Every new block represents the latest update to account balances").

[38] *See* Benner, et. al., *supra* note 34; *see also* John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCIENCE.ORG (Mar. 9, 2016), https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin?cookieSet=1 ("If you catch people using something like Silk Road, you've uncovered their whole criminal history...It's like discovering their books" says Sarah Meiklejohn, a computer scientist at University College in London).

[39] *See* Benner, et. al., *supra* note 34; *see also* Katrina A. Hausfeld et al., *U.S. Department of Justice, Aided by Cryptocurrency Exchanges, Seizes Over U.S. $3.6 Billion In Stolen Bitcoin*, DLA PIPER (Feb. 15, 2022), https://www.dlapiper.com/en/us/insights/publications/2022/02/us-department-of-justice-aided-by-cryptocurrency-exchanges/.

[40] *See* Benner, et. al., *supra* note 34. *see generally* Cryptopedia Staff, *What Are Public and Private Keys?* GEMINI (June 28, 2022), https://www.gemini.com/cryptopedia/public-private-keys-cryptography.

[41] *See* Benner, et. al., *supra* note 34. *see generally* Cryptopedia Staff, *What Are Public and Private Keys?* GEMINI (June 28, 2022), https://www.gemini.com/cryptopedia/public-private-keys-cryptography.

[42] *See* Benner, et. al., *supra* note 34; *see also* Vanessa Romo, *How a New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back*, NPR (June 8, 2021, 2:08 AM), https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac.

[43] *See* Benner, et. al., *supra* note 34; *see also* Benjamin Pimentel, *How Blockchain Analytics Caught Washington's Attention*, PROTOCOL (Mar. 16, 2022), https://www.protocol.com/fintech/blockchain-analytics-russia-ukraine-sanctions (stating that cryptocurrency became a key focus of law enforcement agencies as money laundering and various other crimes were found to be linked to crypto).

[44] *See* Benner, et. al., *supra* note 34; *see also* Pimentel, *supra* note 43.

for patterns that indicate illegal activity.[45] The recovery of the majority of Bitcoin ransom in the Colonial Pipeline attack was considered a win among cryptocurrency enthusiasts because it legitimized the digital currency.[46] Ransomware attacks have put unregulated crypto exchanges under strict scrutiny.[47] Most people access Bitcoin through a central intermediary such as a crypto exchange.[48] The United States has anti-money laundering and identity verification laws requiring these crypto exchanges to identify who their customers are in order to create a link between identity and account; customers of these crypto exchanges must upload government identification when they sign up.[49]

In response to the Colonial Pipeline attack, several financial leaders proposed a ban on cryptocurrency.[50] There are several things hackers can do to make their Bitcoin accounts more secure, making it difficult for authorities to seize these assets.[51] For instance, some cryptocurrency holders will go to great efforts to store their private keys away from anything on the internet (this is referred to as a "cold wallet").[52] Other cryptocurrency holders will memorize the string of numbers and letters or will write them down on paper.[53] Cryptocurrency transactions are more transparent than most other forms of value transfer, like cash.[54] Last February, the United States Department of Justice stated that it had warrants to seize approximately $2 million in cryptocurrencies that North Korean cyber criminals had stolen and stored in accounts during two different cryptocurrency exchanges.[55]

---

[45] *See* Benner, et. al., *supra* note 34; *see also* Rachel Wolfson, *Tracing Illegal Activity Through the Bitcoin Blockchain to Combat Cryptocurrency – Related Crimes*, FORBES (Nov. 26, 2018, 12:00 PM), https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/?sh=1b0a151a33a9 (discussing clustering, a process in which companies against cryptocurrency related crimes closely monitoring blockchain activity can identify accounts that are of the same Bitcoin wallet and entity).

[46] *See* Benner, et. al., *supra* note 34*; see generally* Gideon Pell, *Colonial Pipeline as a Case Study On Cryptocurrency Risks*, FORBES (Jul. 1, 2021, 4:34 PM), https://www.forbes.com/sites/gideonpell/2021/07/01/colonial-pipeline-as-a-case-study-on-cryptocurrency-risks/?sh=3a236a9c4d54.

[47] *See* Benner, et. al., *supra* note 34*; see generally* Alexandre Alper, *Biden Sanctions Cryptocurrency Exchange Over Ransomware Attacks*, REUTERS (Sept. 21, 2021, 12:23 PM), https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/.

[48] *See* Benner, et. al., *supra* note 34; *see also* Nathan Reiff, *What Are Centralized Cryptocurrency Exchanges?*, INVESTOPEDIA (Aug. 27, 2021), https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/ ("Centralized cryptocurrency exchanges are online platforms used to buy and sell cryptocurrencies.").

[49] *See* Benner, et. al., *supra* note 34; *see also Crypto KYC/AML in the U.S. and Around the Globe*, LIGHTICO, https://www.lightico.com/blog/crypto-kyc-aml-in-the-us-and-around-the-globe/ (last visited Oct. 10, 2022).

[50] *See* Nicole Perlroth, Erin Griffith & Katie Benner, *Pipeline Investigation Upends Idea That Bitcoin is Untraceable*, N.Y. TIMES (June 9, 2021), https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html; *see also* Ryan Ozawa, *Latest Draft on US Crypto Law Would Temporarily Ban Terra-Like Stablecoins*, DECRYPT (Sept. 20, 2022), https://decrypt.co/110208/stablecoin-law-ban-terra-luna.

[51] *See* Perlroth, Griffith, & Benner, *supra* note 50; s*ee also* Dalvin Brown, *Tracking stolen crypto is a booming business: How blockchain sleuths recover digital loot*, WASH. POST (Sept. 22, 2021).

[52] *See* Perlroth, Griffith, & Benner, *supra* note 50*; see also* Brown, *supra* note 51.

[53] *See* Perlroth, Griffith, & Benner, *supra* note 50; *see also* Brown, *supra* note 51.

[54] *See* Perlroth, Griffith, & Benner, *supra* note 50; *see also Crypto has always held the key to its future: transparency*, RACONTEUR, https://www.raconteur.net/sponsored/crypto-has-always-held-the-key-to-its-future-transparency/ (last visited Oct. 13, 2022, 3:28 PM).

[55] *See* Perlroth, Griffith, & Benner, *supra* note 50; *see also* Ellen Nakashima, *U.S. accuses three North Koreans of conspiring to steal more than $1.3 billion in cash and cryptocurrency*, WASH. POST (Feb. 17, 2021, 7:00 PM),

B. Wannacry and Notpetya

i. The Historical Impact of Ransomware Attacks.

"Wannacry" is a hacking group that created a ransomware attack occurring in 2017.[56] Wannacry encrypted over one hundred thousand computers in more than one hundred and fifty countries within a few hours.[57] In the United Kingdom, hospitals were offline due to malware and government systems while railway networks and private companies were disrupted.[58] The attack was caused by an unknown hacker group that was suspected to work with North Korea.[59] In a matter of hours, the ransomware attack caused billions of dollars in damages.[60] Marcus Hutchins, a malware reverse engineer and security researcher, found Wannacry's kill switch and halted the spread of the attack.[61] One month after the Wannacry attack, the world witnessed another ransomware attack, "NotPetya", a variant of Petya ransomware.[62] Petya ransomware began spreading internationally on June 27, 2017, targeting Windows servers, laptops, and PCs.[63] While Petya ransomware primarily targeted Ukraine in June 2017, its effects were felt throughout the globe.[64] Petya ransomware was discovered in March 2016.[65] The 2017 strain of Petya took down entities across the globe in a mere few hours.[66] These ransomware outbreaks were significant because of the scale of the damage.[67]

---

https://www.washingtonpost.com/national-security/north-korea-hackers-banks-theft/2021/02/17/3dccf0dc-7129-11eb-93be-c10813e358a2_story.html.

[56] *See* Zack Whittaker, *Two Years after WannaCry, a million computers remain at risk*, TECHCRUNCH (May 12, 2019, 5:37 PM), https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJ3VeC0rtTzP8MQcuTWG9ZMhVQxidEu9JPswSd4ruZZVj5YJvs5nF7eMLxLZx_1RT3PcAE2B2Qsqgvg-YfHeBUmvscKtQe69VCf8NcOECyPCFi6a6b95D_hTvORkFa6GdiuV5zKBL9n2ZADYGMnkRhkMwMRorVBJR99hh2OwmvSP; *see also* Linda Rosencrance, *WannaCry ransomware*, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware (last visited Oct. 13, 2022).

[57] *See* Whittaker, *supra* note 56; *see also* Rosencrance, *supra* note 56.

[58] *See* Whittaker, *supra* note 56; *see also* Rosencrance, *supra* note 56.

[59] *See* Whittaker, *supra* note 56; *see also* Rosencrance, *supra* note 56.

[60] *See* Whittaker, *supra* note 56; *see also* Rosencrance, *supra* note 56.

[61] *See* Whittaker, *supra* note 56; *see also* Rosencrance, *supra* note 56.

[62] *See* Whittaker, *supra* note 56; *see also* Rosencrance, *supra* note 56.

[63] *See What Is Petya and NotPetya Ransomware?*, MCAFEE, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html (last visited Sept. 12, 2021); *see generally* Olivia Solon & Alex Hern, *'Petya' ransomware attack: what is it and how can it be stopped?*, THE GUARDIAN (June 28, 2017), https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how.

[64] *See What Is Petya and NotPetya Ransomware?*, *supra* note 63; *see generally* Solon & Hern, *supra* note 63.

[65] *See What Is Petya and NotPetya Ransomware?*, *supra* note 63; *see generally* Solon & Hern, *supra* note 63.

[66] *See What Is Petya and NotPetya Ransomware?*, *supra* note 63; *see also* Gonzalo Torres, *2017 Petya Ransomware Outbreak — Your Quick Safety Guide*, AVG, https://www.avg.com/en/signal/petya-ransomware-what-you-need-to-know (Last Updated July 26, 2022).

[67] *See What Is Petya and NotPetya Ransomware?*, *supra* note 63; *see also* Torres, *supra* note 66.

C. Solarwinds' cyber attack

i.Impact of a Recent Ransomware Attack

The IT company, Solarwinds, sustained a supply chain attack in early 2020.[68] As a result of this cyberattack, the United States government was prepared to impose sanctions on approximately one dozen Russian intelligence officials.[69] The attack occurred when hackers broke into Solarwind's systems and inputted malicious code into the company's software.[70]

Starting in March of 2020, SolarWinds sent out software updates to their customers that, unbeknownst to SolarWinds, contained a hacked code.[71] This code created access to the customer's information technology systems which hackers used to install more malware to aid them in spying on companies and organizations.[72] SolarWinds informed the SEC that around 18,000 of its customers installed updates that exposed them to hackers.[73] Various United States agencies, including the Pentagon, the Department of State, the Department of Homeland Security, the Department of Energy, the National Nuclear[74] Security Administration, and the Treasury, were attacked.[75] Additionally, private companies like Microsoft, Cisco, Intel, and Deloitte were impacted by the SolarWinds cyberattack.[76]

Since the hack was undetected for several months, security experts believe that some victims may never realize if they were a victim to the SolarWinds cyberattack.[77] Cybersecurity experts also believe that the attack was caused by Russia's Foreign Intelligence Service.[78] This hack may result in broad changes to the cybersecurity industry as companies are now seeking

---

[68] *See* Isabella Jibilian & Katie Canales, *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal*, BUSINESS INSIDER (Apr. 15, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12; *see also Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them*, BEYOND IDENTITY (Oct. 28, 2021), https://www.beyondidentity.com/blog/software-supply-chain-attack-methods-behind-solarwinds-kaseya-and-notpetya.

[69] *See* Jibilian & Canales, *supra* note 68; *see also* Joseph Menn & Christopher Bing, *Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes*, REUTERS (Oct. 8, 2021, 6:42 AM), https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/.

[70] *See* Jibilian & Canales, *supra* note 68; *see also Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them*, *supra* note 68.

[71] *Id.; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them*, BEYOND IDENTITY BLOG (Oct. 28, 2021), https://www.beyondidentity.com/blog/software-supply-chain-attack-methods-behind-solarwinds-kaseya-and-notpetya.

[72] Jibilian & Canales, *supra* note 68; *see also* Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[73] Jibilian & Canales, *supra* note 68; *see also* Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[74] Jibilian & Canales, *supra* note 68; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[75] *See generally* Jibilian & Canales, *supra* note 68; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[76] *See generally* Jibilian & Canales, *supra* note 68; *see generally* Monika Evstatieva, *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*, NPR (Apr. 16, 2021, 10:05 AM), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[77] Jibilian & Canales, *supra* note 68; *see generally* Evstatieva, *supra* note 76.

[78] Jibilian & Canales, *supra* note 68; *see generally* Evstatieva, *supra* note 76.

new methods to become more cyber resilient.[79] Companies have started to adopt a safety measure in which the company assumes they have already been breached instead of reacting to cyber attacks after they occur.[80] Additionally, the United States may restructure its cybersecurity efforts by making the cyber commands independent of the National Security Agency.[81] The SolarWinds attack may also generate a strengthened relationship between the cybersecurity industry and the United States government as the private sector assists federal officials to combat nation-state cyber attacks.[82]

Starting in March of 2020, SolarWinds sent out software updates to their customers that, unbeknownst to SolarWinds, contained a hacked code.[83] This code created access to the customer's information technology systems which hackers used to install more malware to aid them in spying on companies and organizations.[84] SolarWinds informed the SEC that around 18,000 of its customers installed updates that exposed them to hackers.[85] Various United States agencies including the Pentagon, the Department of State, the Department of Homeland Security, the Department of Energy, the National Nuclear[86] Security Administration, and the Treasury were attacked.[87] Additionally, private companies like Microsoft, Cisco, Intel, and Deloitte were impacted by the SolarWinds cyberattack.[88] Since the hack was undetected for several months, security experts believe that some victims may never realize whether they were a victim to the SolarWinds cyber attack.[89]

If the ransomware hackers are situated in a different country, which is usually the case, the United States officials must pursue international cooperation and diplomacy resulting

---

[79] Jibilian & Canales, *supra* note 68; Saheed Oladimeji & Sean Michael Kerner, *SolarWinds hack explained: Everything you need to know*, TECHTARGET (Jun. 29, 2022), https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-toknow#:~:text=The%20SolarWinds%20supply%20chain%20attack,private%20systems%20around%20the%20world

[80] Jibilian & Canales, *supra* note 68; *see also* Lolita Baldor, *U.S. to Create the Independent U.S. Cyber Command, Split Off From NSA*, PBS (Jul. 17, 2017, 11:01 AM), https://www.pbs.org/newshour/politics/u-s-create-independent-u-s-cyber-command-split-off-nsa.

[81] Jibilian & Canales, *supra* note 68; *see generally* Evstatieva, *supra* note 76.

[82] *See* Rishi Iyengar, *Why it's so Difficult to Bring Ransomware Attackers to Justice*, CNN BUSINESS, (July 8, 2021), https://www.cnn.com/2021/07/08/tech/ransomware-attacks-prosecution-extradition/index.html; U.S. Dep't of Justice, *Comprehensive Cyber Review* 38 (2022).

[83] *Id.; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them*, BEYOND IDENTITY BLOG (Oct. 28, 2021), https://www.beyondidentity.com/blog/software-supply-chain-attack-methods-behind-solarwinds-kaseya-and-notpetya.

[84] Jibilian & Canales, *supra* note 68; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[85] Jibilian & Canales, *supra* note 68; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[86] Jibilian & Canales, *supra* note 68; Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[87] *See gennerally* Jibilian & Canales, *supra* note 68; *see also* Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them, *supra* note 71.

[88] *See generally* Jibilian & Canales, *supra* note 68; *see generally* Monika Evstatieva, *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*, NPR (Apr. 16, 2021, 10:05 AM), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[89] Jibilian & Canales, *supra* note 68; *see generally* Evstatieva, *supra* note 76.

in inefficiency and complication in the prosecution process.[90] Further, some countries are allegedly utilizing access to cyber criminals as a diplomatic bargaining chip.[91]

After a hacking group or attackers are located and prosecuted overseas, with the assistance of Interpol and Europol, the next obstacle is bringing these individuals back to the United States. While the United States has extradition treaties with more than one hundred countries, there are also dozens, such as Russia and China, with which it does not.[92] Often, United States authorities will wait patiently until the hackers travel to a country with an extradition treaty.[93] On the other hand, these extraditions can often take several years, which leaves United States authorities with little control over the process or timeline.[94] Taking on these criminal gangs requires cooperation of other countries, as it takes an immense amount of time to map them out and understand their motivations.[95]

III. LEGAL ISSUE

A. Rethinking The Efficiency of An Outright Ban on Paying Ransomware

i. AXA's approach to ransomware payments in France

On May 6, 2021, the global insurance company AXA stated that it will no longer write cyber insurance policies in France that reimburse customers for extortion payments made during a ransomware attack.[96] AXA refused to reimburse ransom payments as a reaction to concerns from French justice and cybersecurity officials about the destructive consequences of ransomware.[97] France lost around $5.5 billion in damages related to ransomware in 2020.[98] Ransomware attacks in France target businesses, hospitals, schools, and local governments.[99] While the suspension only applies to France, many adovcates that believe an outright ban on reimbursing ransomware payments is the most effective solution for responding to ransomware attacks.[100] Cyber hackers that utilize ransomware only provide keys to decode encrypted data

[90] *See* Iyengar, *supra* note 82; *see also Comprehensive Cyber Review*, *supra* note 82, at 29.

[91] *See* Iyengar, *supra* note 82; *see also Comprehensive Cyber Review*, *supra* note 82, at 35.

[92] *See* Iyengar, *supra* note 82; *see also Comprehensive Cyber Review*, *supra* note 82, at 24.

[93] *See* Iyengar, *supra* note 82; *see generally Comprehensive Cyber Review*, *supra* note 82 at 31, 34.

[94] *See* Iyengar, *supra* note 82; *see generally Comprehensive Cyber Review*, *supra* note 82 at 31, 34.

[95] *See* Iyengar, *supra* note 82; *see generally Comprehensive Cyber Review*, *supra* note 82 at 31, 34.

[96] *See* Frank Bajak, *Insurer AXA to Stop Paying for Ransomware payments in France*, Insurance Journal, (May 9, 2021) https://www.insurancejournal.com/news/international/2021/05/09/613255.htm.; *see also* Frank Bajak, *Insurer AXA halts ransomware crime reimbursement in France*, ABC NEWS (May 6, 2021), https://abcnews.go.com/Technology/wireStory/insurer-axa-halts-ransomware-crime-reimbursement-france-77540351.

[97] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (ABC), *supra* note 96.

[98] *See* Bajak (Insurer), *supra* note 96; *see also* Frank Bajak, *Insurer AXA halts ransomware crime reimbursement in France*, AP NEWS (May 6, 2022), https://apnews.com/article/europe-france-technology-business-caabb132033ef2aaee9f58902f3e8fba.

[99] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[100] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

to their victims when they are paid.[101] As a result of the increase of ransomware attacks, the cyber insurance industry has been criticized for reimbursing these extortion payments.[102]

Sometimes, facilitating ransomware payments may be the only way for an impacted business to avoid bankruptcy.[103] Usually, ransomware criminals study their targets ahead of time to learn if the victim carries insurance coverage for ransomware attacks.[104] Furthermore, cyber hackers may even know their victim's cyber insurance policy payment ceiling.[105] While an outright ban of reimbursing ransomware payments has not been the approach taken in the United States, there may be violations of the Office of Foreign Assets Control ("OFAC") regulations when a ransomware payment is facilitated to illegal entities.[106] Additionally, ransomware is worrisome as the illegal ransomware industry is only fueled when people continue to pay ransoms.[107]

IV. PROPOSED SOLUTION

A. Regulations by the SEC

Investment advisers and companies must comply with several cybersecurity regulations and rules if they register with the SEC.[108] Regulation S-P requires registered broker-dealers, investment companies, and investment advisors to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[109] Subpart C of Regulation S-ID regards identity theft red flags.[110] Investment Company Act ("ICA") Rule 38-1 requires SEC-registered investment companies to adopt compliance procedures and practices to avoid violating the Federal Securities law.[111] Additionally, the Investment Advisers Act ("IAA") Rule 206(4)-7 lays out the compliance procedures and practices required for an investment adviser to follow if they are registered or required under section 204 of the Investment Advisers Act of 1940.[112] Further, in an adopting release for ICA Rule 38-1 and IAA Rule 206(4)-7, the SEC has provided

---

[101] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[102] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[103] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[104] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[105] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[106] *See* Bajak (Insurer), *supra* note 96; *see also Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, DEPARTMENT OF THE TREASURY (Oct. 1, 2020) ("Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial"), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[107] *See* Bajak (Insurer), *supra* note 96; *see also* Bajak (AP), *supra* note 98.

[108] *See generally Cybersecurity*, U.S. SECURITIES AND EXCHANGE COMMISSION, https://www.sec.gov/spotlight/cybersecurity-old (last visited, Oct. 16, 2022).

[109] *Final Rule: Compliance Programs of Investment Companies and Investment Advisors*, U.S. SECURITIES AND EXCHANGE COMMISSION, https://www.sec.gov/rules/final/ia-2204.htm (last visited, Oct. 16, 2022).

[110] 17 CFR Part 248 Subpart C.

[111] *Final Rule: Compliance Programs of Investment Companies and Investment Advisors*, *supra* note 109.

[112] *See id.*

additional information regarding issues that the policies of funds and advisors should consider, including cyber security.[113] The SEC also released several guidance letters regarding cybersecurity protocols.[114] The SEC released a commission statement and guidance regarding public company cybersecurity disclosures on February 26, 2018.[115] This statement serves as interpretive guidance to help public companies prepare disclosures about cybersecurity risks and incidents.[116] In this release, the SEC addressed two topics regarding the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity.[117] There may be an obligation for registered entities of the SEC to disclose cybersecurity risks and incidents, even though the SEC disclosure requirements do not specifically refer to cybersecurity risks or incidents.[118] For instance, companies must file periodic reports, comply with the Securities and Exchange Act obligations, and maintain the accuracy of shelf registration statements regarding the costs and other consequences of cybersecurity incidents.[119]

B. 23 CRR-NY I 500 – New York's Cybersecurity Regulation

i. Advice to New York State Regulated Cyber Insurers

On February 4, 2021, the New York State Department of Financial Services ("DFS") issued a Cyber Insurance Risk Framework outlining practices for New York regulated property/casualty insurers ("regulated insurers") regarding the management of cyber insurance risk.[120] DFS has advised regulated insurers by offering cyber insurance protection, including adopting strategies directed and approved by its board or some other governing entity for measuring cyber insurance risk.[121] DFS suggested several practices to regulated insurers to improve their risk strategy, including managing and eliminating exposure to "silent" cyber risk.[122] "Silent" cyber risk refers to the obligation of an insurer to cover loss from a cyber event under a policy that does not explicitly address cyber events.[123] DFS further advised insurers that they should evaluate systemic risk including, but not limited to, the effect of catastrophic cyber events on third party service providers.[124] Further, regulated insurers were advised to rigorously

---

[113] *See id.*

[114] *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, U.S. SECURITIES AND EXCHANGE COMMISSION, https://www.sec.gov/rules/interp/2018/33-10459.pdf (Feb. 26, 2018.

[115] *See id.*

[116] *See id.*

[117] *See id.* at 6.

[118] *See id.* at 5.

[119] *See id.* at 8-9.

[120] *See generally* Press Release, Dept. of Financial Services, Superintendent Lacewell Announces DFS Issues Cybersecurity Insurance Risk Framework (Feb. 4, 2021) https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202102041; *see also* Letter from DFS to Chief Executive Officers of Regulated Entities (Feb. 4, 2021) https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

[121] *See id.*

[122] *See id.*

[123] *See id.*

[124] *See Letter from DFS to Chief Executive Officers of Regulated Entities*, *NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (Dec. 18, 2020), https://www.dfs.ny.gov/reports_and_publications/press_releases/*

measure insured risk through the utilization of a data-driven approach, in order to evaluate potential vulnerabilities in the insureds' cybersecurity system(s).[125] Additionally, DFS recommended regulated insurers to educate insureds and insurance producers about the necessity of cybersecurity measures, as well as the benefits and limitations of cyber insurance.[126] It was recommended that regulated insurers should also obtain expertise in cybersecurity through strategic hiring and recruiting practices. [127] Moreover, DFS advised regulated insurers to notify law enforcement whenever a cyberattack occurs. [128]

C. DFS's Cyber Insurance Risk Framework

DFS's cybersecurity regulation, "Part 500 Cybersecurity Requirements for Financial Companies" ("Part 500"), is a regulation that ensures New York regulated entities are as cyber resilient as possible, in order to protect New York consumers.[129] Regulations such as Part 500 allow regulated entities to ensure they are providing adequate cybersecurity programs.[130]

On October 22, 2021, DFS released a letter to all DFS-regulated entities regarding the adoption of an affiliate's cybersecurity program.[131] This letter clarifies Part 500 by requiring DFS-regulated entities to form risk-based cybersecurity programs to protect their information systems as well as the nonpublic information maintained on them.[132] A "Covered Entity" is defined under the cybersecurity regulation as "any [p]erson operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law."[133] An information system is defined under the Cybersecurity Regulation as "a discrete set of electronic information resources

---

pr202102041; *see also* Press Release, Dept. of Financial Services, Superintendent Lacewell Announces DFS Issues Cybersecurity Insurance Risk Framework (Feb. 4, 2021), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202102041.

[125] *See Letter from DFS to Chief Executive Officers of Regulated Entities*, *supra* note 124; *see also* Press Release, *supra* note 124.

[126] *See Letter from DFS to Chief Executive Officers of Regulated Entities*, *supra* note 124; *see also* Press Release, *supra* note 124.

[127] *See Letter from DFS to Chief Executive Officers of Regulated Entities*, *supra* note 124. *See also* Press Release, *supra* note 124.

[128] *See Letter from DFS to Chief Executive Officers of Regulated Entities*, *supra* note 124; *see also* Press Release, *supra* note 124.

[129] *See* Part 500 Cybersecurity Requirements for Financial Services Companies, 23 CRR-NY (Oct. 30, 2020); *see also See Golden Data Law*, *New York Cybersecurity Requirements for Financial Services Companies (NY-CRFSC)*, (June 7, 2019) https://medium.com/golden-data/new-york-cybersecurity-requirements-for-financial-services-companies-nydfs-28e057a12476.

[130] *See* Part 500 Cybersecurity Requirements for Financial Services Companies, *supra* note 129; *see also Golden Data Law*, *supra* note 129.

[131] *See* Letter from DFS to DFS-regulated entities (Oct. 22, 2021); *see also* Buchanan & Simeone, *DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, JD SUPRA: DATA SEC. L. BLOG (Nov. 10, 2021), https://www.jdsupra.com/legalnews/dfs-issues-new-guidance-regarding-3462868/.

[132] *See Letter from DFS to Chief Executive Officers of Regulated Entities*, *supra* note 124; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[133] *See* 23 NYCRR § 500.1(e).

organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."[134] An "affiliate" is defined under the regulation as "any person that controls, is controlled by or is under common control with another person."[135] "Control" is defined as "the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise."[136]

It is essential that companies have robust cybersecurity programs as cyber risk has increased tremendously since 2017.[137] According to DFS, 23 NYCRR §500.2(c) allows, "Covered Entities to adopt 'the relevant and applicable provisions' of the cybersecurity program of an affiliate provided that such provisions satisfy the requirements of the cybersecurity regulation.."[138] Some Covered Entities are affiliates of other companies – parents, subsidiaries, etc. – and usually share information about cybersecurity resources with those affiliates. For example, adoption can occur when a DFS-licensed subsidiary uses a shared service provided by a parent corporation. Covered Entities must make available to DFS, on request, all documentation and information relevant to their cybersecurity programs.[139] This includes any documentation or information pertinent to cybersecurity programs adopted from an affiliate.[140] In order to guarantee that DFS is able to access all pertinent documentation and information, Covered Entities should make sure that its agreements between affiliates provides for DFS access.[141] At minimum, DFS must have access to documentation regarding the affiliate's cybersecurity policies and procedures, risk assessments, penetration testing and vulnerability assessment results, and third-party audits regarding the adopted portions of the cybersecurity program of the affiliate.[142] Covered Entities are required to provide documentation from the affiliate sufficient to convey that the portions of the cybersecurity program adopted by the covered entity are in compliance with the cybersecurity regulation.[143] Covered Entities are permitted to adopt the cybersecurity program of an affiliate.[144] A DFS examination of the Covered Entity may include a review of the adopted portions of the

[134] *See Id.*

[135] *See* 23 NYCRR § 500.1(a).

[136] *See Id.*

[137] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[138] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[139] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[140] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[141] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[142] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[143] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[144] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

cybersecurity program of that affiliate.[145] Further, the Covered Entity is responsible for providing DFS with documentation and information sufficient to allow DFS to determine whether the Covered Entity is in compliance with the cybersecurity regulation.[146]

D. Actions Taken to Improve Cyber Resiliency Around the Worlds

The International Monetary Fund ("IMF") and the Monetary Authority of Singapore ("MAS") released a paper in February of 2020 which offered various analytical approaches to assessing and monitoring cyber risk in the financial sector of Singapore.[147] These analytical approaches include various modes of cyber stress testing.[148] A "cybersecurity stress test" is used to evaluate the cybersecurity resiliency of financial institutions.[149] Cybersecurity stress tests are often utilized to determine the adequacy of capital and liquidity buffers to determine the effect of cyberattacks.[150] A cybersecurity stress test involves an industry-wide exercise of a hypothetical cyber incident to test financial institutions.[151]

MAS performed an industry-wide stress test ("IWST") in 2016 that involved a cyber scenario where an international crime syndicate launched simultaneous hacking attacks on financial institutions in Asia, including Singapore.[152] "The cyberattack resulted in a loss of entire customer databases and a 24-hour system downtime for the bank's client-facing operational systems."[153] The 2016 IWST results conveyed less of an impact on the banks than what was estimated.[154] Direct life and general insurers were asked to quantify the hypothetical losses in this scenario and "the 2016 cyber stress test results suggested that insurers were not materially affected by the scenario."[155] MAS collaborated with the IMF to conduct another cybersecurity stress test in 2019 to measure cyber risk in Singapore.[156] The 2019 cybersecurity stress test allowed the Singapore banks to identify the direst cyber scenarios for financial buffers and profits through the use of the cyber risk assessment matrix ("cyber RAM").[157] The cyber RAM is an analytical device that contains rows that index downside scenarios, and columns that convey the likelihood and severity of each scenario.[158] "The scenarios for the 2019

---

[145] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[146] *See* Letter from DFS, *supra* note 131; *see also DFS Issues New Guidance Regarding Cybersecurity Regulation and the Adoption of an Affiliate's Cybersecurity Program*, *supra* note 131.

[147] *See* Joseph Goh et al., *Cyber Risk Surveillance: A Case Study of Singapore* 1, 2 (Int'l Monetary Fund, Working Paper 20,28).

[148] *See id.*

[149] *See id.* at 11.

[150] *See id.* at 10.

[151] *See id.* at 18.

[152] *See id.*

[153] *See id.*

[154] *See id.*

[155] *See id.*

[156] *See id.* at 19.

[157] *See id.*

[158] *See* Goh, *supra* note 147; *see generally* Ethan Bresnahan, *Using Risk Assessment Matrix to Report to Executive Management,* CYBER RISK SAINT, https://www.cybersaint.io/blog/risk-management-matrix-reporting (last visited Oct. 14, 2022).

Singapore Bank cybersecurity stress test were separated into different categories: theft, disruption, and damage." [159] As part of the 2019 IWST, Singapore insurers were asked to measure their exposure to affirmative and silent cyber risk coverage under their policies.[160] The insurers that participated in the 2019 IWST expected the claims from affirmative and silent cyber risk coverage to be mitigated by reinsurance.[161] These insurers reported $600 million worth of exposure for affirmative cyber coverage and $3.4 million for silent cyber coverage.[162] Some of the participating insurers were able to incorporate risk mitigation actions to address the issue of silent cyber coverage.[163]

E. How Else Is the Threat of Ransomware Being Addressed in the United States?

The SEC established the Division of Enforcement's Cyber Unit ("Cyber Unit") in September 2017.[164] The Cyber Unit primarily focuses on violations relating to digital assets, cryptocurrencies, cybersecurity controls at regulated entities, issuer disclosures of cybersecurity incidents and risks, trading as a result of hacked nonpublic information, and cyber related manipulations.[165] On July 10, 2020, the Office of Compliance Inspections and Examinations ("OCIE") released a "Cybersecurity Ransomware Alert" to inform registrants, and those who participate in the financial services market, of the increasing sophistication of ransomware attacks on SEC registrants.[166] This alert warned that one or more cyber criminals had "orchestrated phishing and other campaigns designed to penetrate financial institution networks to, among other objectives, access internal resources and deploy ransomware."[167] In response to these ransomware attacks, OCIE advised registrants to monitor cybersecurity alerts; published by the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency ("CISA") lays out this advice [168] Additionally, OCIE advised registrants to share any relevant information relating to ransomware attacks with third-party service providers.[169] OCIE released another alert on September 15, 2020, regarding how recent cyber attacks resulted from "credential stuffing."[170] Credential stuffing is a form of cyberattack that

---

[159] *See* Goh, *supra* note 147.

[160] *See* Goh, *supra* note 147; *see generally Cyber Risk Toolkit*, AMERICAN ACADEMY OF ACTUARIES 37 (August 2021) (last updated June 2022).

[161] *See* Goh, *supra* note 147; *see generally* AMERICAN ACADEMY OF ACTUARIES, *supra* note 160.

[162] *See* Goh, *supra* note 147; U.S. GOV'T. ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET (2021).

[163] *See* Goh, *supra* note 147.

[164] *See Press Release: SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors*, U.S. SEC. AND EXCH. COMM'N (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176.

[165] *See id.*

[166] *See Cybersecurity: Ransomware Alert*, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS (U.S. SEC. AND EXCH. COMM'N) (July 10, 2020), https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf [hereinafter OCIE].

[167] *See id.*

[168] *See id.*

[169] *See id.*

[170] *See generally Cybersecurity: Safeguarding Client Accounts Against Credential Compromise*, U.S. SEC. AND EXCH. COMM'N (last modified Sept. 18, 2020), https://www.sec.gov/ocie/announcement/risk-alert-credential-compromise.

utilizes compromised client login credentials; this form of attack could potentially result in loss of customer assets and unauthorized disclosure of sensitive personal information.[171]

The CISA launched a resource page to help individuals and organizations improve their resilience to cybersecurity in response to the increasing frequency and sophistication of ransomware attacks.[172] This website provides various resources to help businesses and individuals prevent ransomware attacks, one of which being a guide of best practices to avoid a ransomware attack.[173]

While paying ransomware has not been banned in the United States, there are still some severe legal risks that must be considered before a ransomware payment is facilitated.[174] Some victims who have paid ransomware demands were targeted again by cyber hackers.[175] Additionally, paying a ransom does not guarantee that a company will be able to regain access to the encrypted data, as several victims of ransomware attacks report not receiving a decryption key after facilitating a ransomware payment.[176] Further, some victims that facilitated a ransomware payment were not provided the decryption key after paying the demanded amount.[177]

In addition to the risks previously mentioned, paying ransomware could unintentionally encourage the ransomware business model.[178] For these reasons, United States governmental entities advise potential victims to adopt cyber resiliency measures to prevent ransomware attacks, arguably the best defense to these cyber incidents.[179] Implementing a cybersecurity awareness and training program so that employees are educated about the threat of ransomware, such as configuring firewalls to prevent access to malicious IP addresses, setting anti-virus and anti-malware programs, and conducting regular scans automatically, are preventive measures that United States governmental entities suggest companies take to ensure cyber resiliency.[180] Additionally, the government advises that United States corporations regularly backup their data, conduct annual penetration testing and vulnerability assessments,

---

[171] *See id.*

[172] *See Ransomware 101: General Information*, CISA, https://www.cisa.gov/stopransomware/general-information (last visited Oct. 4, 2021); *see also* MULTI-STATE INFO. SHARING & ANALYSIS CENTER, RANSOMWARE GUIDE 2 (Cybersecurity & Infrastructure Security Agency, Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

[173] *See* CISA, *supra* note 172; *see also* MULTI-STATE INFO. SHARING & ANALYSIS CENTER, RANSOMWARE GUIDE, *supra* note 172.

[174] *See Ransomware What It Is and What To Do About It*, INCIJTF, https://us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf (last visited Oct. 4, 2021); *see also* Sandra Gittlen, *The Complete Guide to Ransomware*, TECHTARGET (Oct. 13, 2021), https://www.techtarget.com/searchsecurity/Guide-to-preventing-phishing-and-ransomware.

[175] *See* INCIJTF, *supra* note 174; s*ee also* Gittlen, *supra* note 174 (explaining the range and frequency of ransomware attacks).

[176] *See* INCIJTF, *supra* note 174; s*ee also* Gittlen, *supra* note 174 (describing what ransomware attackers tell their victims).

[177] *See* INCIJTF, *supra* note 174; *see also* Gittlen, *supra* note 174 (explaining what is defined as "double extortion").

[178] *See* INCIJTF, *supra* note 174; *see also* Gittlen, *supra* note 174.

[179] *See* INCIJTF, *supra* note 174; *see also* Gittlen, *supra* note 174.

[180] INCIJTF, *supra* note 174; Gittlen, *supra* note 174.

and to secure their backups to avoid disruption to business continuity.[181] When a company is infected by ransomware malware, the United States government advises isolating the infected computer as soon as possible, isolating affected devices that have not yet been completely corrupted, contacting law enforcement (such as the FBI or U.S. Secret Service) immediately and changing online account passwords after removing ransomware from the network.[182]

Ransomware is increasing and has multiple variants.[183] Some of these variants encrypt the contents of shared or networked drives, externally attached storage media devices, and cloud storage services that are mapped to infected computers.[184] The top five ransomware variants that are targeting the United States are CryptoWall, CTB-Locker, TeslaCrypt, MSIL/Samas, and Locky.[185]

On June 30, 2021, DFS issued new guidance identifying cybersecurity controls that significantly reduce the risk of a ransomware attack.[186] DFS examined ransomware attacks reported by its regulated entities and observed a similar pattern of hackers, including entering a victim's network, obtaining administrator privileges, using these privileges to deploy ransomware, avoid security controls, steal data, and disable backup data.[187] DFS advised its regulated entities to adopt the following measures to prepare for a ransomware attack: (1) train employees in cybersecurity awareness; (2) implement a vulnerability and Patch Management program; (3) use multi-factor authentication ("MFA") and strong passwords; (4) employ privilege access management; (5) use monitoring and response to anticipate intruders; (6) separate and test backups; (7) and have a ransomware specific incident response plan.[188] As a result of ransomware, loss ratios on cyber insurance went from an average of forty-two percent during 2015-2019 to seventy-three percent in 2020.[189] The recent increase in ransomware attacks is a result of the continuous payments made by ransomware victims.[190] For this reason, the FBI and other state governmental entities advise against paying ransoms.[191]

---

[181] *See* INCIJTF, *supra* note 174; *see generally* Gittlen, *supra* note 174 (asserting that companies can protect against ransomware attacks by continuing to strengthen their levels of protection).

[182] *See* INCIJTF, *supra* note 174; *see also* Gittlen, *supra* note 174.

[183] *See* INCIJTF, *supra* note 174; *see also* Gittlen, *supra* note 175 (laying out the various forms and strains of ransomware).

[184] *See* INCIJTF, *supra* note 174; *see generally* Gittlen, *supra* note 175 (explaining what many forms of ransomware set out to do).

[185] *See* INCIJTF, *supra* note 174; *see also* Gittlen, *supra* note 175 (naming popular variants of ransomware).

[186] *See* Press Release, N.Y. Dept. of Fin. Serv., Superintendent Lacewell Announces DFS Issues New Guidance on Ransomware Prevention (June 30, 2021) (on file with author); *see also* Letter from N.Y. Dept. of Fin. Serv. to All N.Y. State Regulated Entities (June 30, 2021) (on file with author).

[187] *See id*; *see also* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186.

[188] *See id*; *see also* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186.

[189] Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also US Cyber Insurance Payouts Increase Amid Rising Claims, Premium Hikes*, FITCH RATINGS (May 6, 2022, 10:56AM EST) https://www.fitchratings.com/research/insurance/us-cyber-insurance-payouts-increase-amid-rising-claims-premium-hikes-06-05-2022.

[190] Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* Press Release, U.S. DEPARTMENT OF TREASURY TAKES ROBUST ACTIONS TO COUNTER RANSOMWARE (September 21, 2022).

[191] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* U.S. DEPARTMENT OF TREASURY TAKES ROBUST ACTIONS TO COUNTER RANSOMWARE *supra* note 190.

Paying ransoms help fund future cyber attacks and may also risk a violation of OFAC sanctions.[192] In some cases of ransomware attacks, even when victims paid, companies were still unable to regain access to their data or their data was leaked by the hackers anyway.[193] Despite the increasing frequency of ransomware attacks, hackers are repeatedly using the same techniques.[194] Throughout the period of January 2020 through May 2021, DFS regulated companies reported seventy-four ransomware attacks and seventeen companies paid a ransom.[195] These ransomware attacks followed a similar pattern where hackers gained entry to their victims' network through one of three techniques: (i) phishing; (ii) exploiting unpatched vulnerabilities; or (iii) exploiting poorly secured Remote Desktop Protocols ("RDP").[196] DFS advises its regulated entities to prevent ransomware by implementing email filtering and anti-phishing training, vulnerability/patch management, MFA, disabling RDP access, managing passwords as well as privileged access, and having a way to monitor their systems for intruders.[197] In order to prepare for a cyber incident, DFS advises its entities to test and segregate backups and to have an Incident Response plan.[198]

F. Ransomware Exceptions

i. When facilitating Ransomware payments are absolutely necessary.

This Note argues that facilitating ransomware attacks should be discouraged by governmental entities, federal and state regulators, insurers, and reinsurers without policies that completely ban these payments. There are certain circumstances where paying ransomware is

[192] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* Press Release, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (September 21, 2022).

[193] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* Press Release, OVER HALF OF RANSOMWARE VICTIMS PAY THE RANSOM, BUT ONLY A QUARTER SEE THEIR FULL DATA RETURNED (March 30, 2021).

[194] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* DFS, SUPERINTENDENT LACEWELL ANNOUNCES DFS ISSUES NEW GUIDANCE ON RANSOMWARE PREVENTION *supra* note 186.

[195] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* Memorandum, New York State Department of Financial Services Issues New Guidance on Preventing Ransomware Attacks (July 2, 2022), https://www.sullcrom.com/files/upload/sc-publication-DFS-issues-new-guidance-on-minimizing-ransomware-risks.pdf.

[196] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* DFS, SUPERINTENDENT LACEWELL ANNOUNCES DFS ISSUES NEW GUIDANCE ON RANSOMWARE PREVENTION *supra* note 186.

[197] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also* DFS, SUPERINTENDENT LACEWELL ANNOUNCES DFS ISSUES NEW GUIDANCE ON RANSOMWARE PREVENTION *supra* note 186.

[198] *See* Letter from Dept. of Fin. Serv. to All N.Y. State Regulated Entities, *supra* note 186; *see also Cybersecurity Incident & Vulnerability Response Playbooks*, Cybersecurity and Infrastructure Security Agency (Nov. 2021) https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

the most practical solution.[199] When a disruption in business operations occur because of a ransomware attack, it occasionally results in a loss of life or risk thereof in of loss of life.[200]

One clear example of a such disruption is within the healthcare industry.[201] In May 2021, information technology ("IT") systems for hospitals in Ireland were victims of ransomware attacks.[202] Irish Foreign Minister Simon Coveney described the incident as a "very serious attack," and Irish Minister Of State, Ossian Smyth referred to it as "possibly the most significant cybercrime attack on the Irish State."[203] Emergency services were still operating in the country, however, were abnormally busy as a result of the IT outage.[204] This ransomware attack resulted in many radiology appointments being cancelled and also caused delays in COVID-19 test result reporting.[205] Further, pediatric services, maternity services, and outpatient appointments in certain hospitals were also impacted by this cyberattack.[206] There were also delays in issuing death, birth, and marriage certificates.[207] Ireland's Health Minister, Stephen Donnelly, revealed that payment down payment systems impacted 146,000 people who work in the healthcare industry.[208] The hackers behind this ransomware attack demanded $20 million to restore the system and began leaking private information about the impacted patients online.[209]

Around the same time, New Zealand faced a similar cybersecurity attack that completely shut down the country's healthcare IT services.[210] Hospitals in Waikato, Thames,

---

[199] *See* Jonathan Greig, *Healthcare Organizations in Ireland, New Zealand and Canada Facing Intrusions and Ransomware Attacks*, ZDNET (May 20, 2021), https://www.zdnet.com/article/healthcare-organizations-in-ireland-new-zealand-and-canada-facing-intrusions-and-ransomware-attacks/; *see generally* Jareth, *To pay or not to pay ransomware: A cost-benefit analysis of paying ransom*, EMSISOFT (Aug. 20, 2019), https://blog.emsisoft.com/en/33686/to-pay-or-not-to-pay-ransomware-a-cost-benefit-analysis-of-paying-the-ransom/.

[200] *See* Greig *supra* note 199; *see also* Melissa D. Berry, *Ransomware attacks against healthcare organizations nearly doubled in 2021, report says*, THOMSON REUTERS (July 5, 2022), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ransomware-attacks-against-healthcare/.

[201] *See* Greig *supra* note 199; *see also* Anastassia Gliadkovskaya, *Ransomware attacks impact patient care, including increased mortality rates, report finds*, FIERCE HEALTHCARE (Sep. 24, 2021), https://www.fiercehealthcare.com/tech/ransomware-attacks-impact-patient-care-including-increased-mortality-rates-report-finds.

[202] *See* Greig *supra* note 199; *see also* Nicole Perlroth & Adam Satariano, *Irish Hospitals Are Latest to Be Hit by Ransomware Attacks*, NEW YORK TIMES (May 20, 2021), https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html.

[203] *See* Greig *supra* note 199.

[204] *See* Greig *supra* note 199; *see also* Perlroth & Satariano *supra* note 202.

[205] *See* Greig *supra* note 199; *see also* Perlroth & Satariano *supra* note 202.

[206] *See* Greig *supra* note 199; *see also* Rory Carroll, *Irish Hospitals Are Latest to Be Hit by Ransomware Attacks*, GUARDIAN (May 14, 2021), https://www.theguardian.com/world/2021/may/14/ransomware-attack-disrupts-irish-health-services.

[207] *See* Greig *supra* note 199; *see also* Jonathan Greig, *Conti ransomware attack on Irish healthcare system may cost over $100 million*, ZDNET (Feb. 24, 2022), https://www.zdnet.com/article/cost-of-conti-ransomware-attack-on-irish-healthcare-system-may-reach-over-100-million/.

[208] *See* Greig, *supra* note 199.

[209] *See* Greig, *supra* note 199; *see also* Joe Tidy, *Hackers bail out Irish health service for free*, BBC (May 21, 2021), https://www.bbc.com/news/world-europe-57197688.

[210] *See* Greig, *supra* note 199; *see also* Jamie Tarabay, *New Zealand Hospitals Under Prolonged IT Outrage From Ransom Hack*, BLOOMBERG (May 25, 2021), https://www.bloomberg.com/news/articles/2021-05-25/new-zealand-hospitals-under-prolonged-it-outage-from-ransom-hack#xj4y7vzkg.

Tokoroa, Te Kuiti and Taurunui were impacted by this attack.[211] As a result of the outage, landline phone services were disabled, and more than thirty elective surgeries were cancelled.[212]

These cyberattacks in Ireland and New Zealand demonstrate how damaging ransomware attacks can be.[213] When afflicted with ransomware attacks, sometimes the only practical choice is to pay the ransom to avoid putting lives in danger.[214] Ransomware gangs and other cybercriminals do not have much regard for human life or privacy and there exists an urgent need for a safety net to help businesses affected by unexpected ransomware attacks.[215]

G. The Sanction and Stop Ransomware Act of 2021 (S.2666)

i. How to Draft Legislation in Response to Ransomware Attacks

On August 5, 2021, Senator Marco Rubio introduced a bill to the Committee on Homeland Security, titled "Sanction and Stop Ransomware Act of 2021" ("the Act").[216] This bill suggests a strict 24-hour limit on reporting ransomware payments for businesses with more than 50 employees.[217] However, some have argued that the 24-hour reporting requirement is not a reasonable amount of time, and that the United States should instead implement the 72-hour data time frame issued by the European Union's General Data Protection Regulation, which is regarded as one of the most comprehensive global privacy laws.[218]

Additionally, a federal agency or covered entity that facilitates a ransomware payment must disclose information such as the method of payment, amount, and recipient.[219] Reporting will be done via a computer system that communicates with the CISA,[220] and failure to report a ransomware payment could result in being subpoenaed and referred to the United States Department of Justice.[221]

Further, there are other enforcement terms mentioned in this bill, such as barring federal government contractors from the Federal Contracting Schedule if they fail to comply, or financial penalties of up to 0.5 percent of the violator's gross annual revenue. Section 5(c)

---

[211] *See* Greig, *supra* note 199; *see also* Tarabay, *supra* note 210.

[212] *See* Greig, *supra* note 199; *see generally* Ben Leahy, *New Zealand's hospitals battle daily cyber attacks: Ministry of Health*, NZ HERALD (May 19, 2021), nzherald.co.nz/nz/new-zealands-hospitals-battle-daily-cyber-attacks-ministry-of-health/2FMFTJXIWJ3UQLXAULGQXOUHUE/.

[213] *See* Greig, *supra* note 199; *see generally* Jessica Davis, *Healthcare Ransom Outrages: Scripps, Ireland HSE, and NZ Hospitals*, HEALTH IT SECURITY (May 18, 2021), https://healthitsecurity.com/news/healthcare-ransomware-outages-scripps-ireland-hse-and-nz-hospitals.

[214] *See* Greig, *supra* note 199; *see also* Stacey Weiner, *The Growing Threat of Ransomware Attacks on Hospitals*, AAMC NEWS (Jul. 20, 2021), https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

[215] *See* Greig, *supra* note 199.

[216] *See* S.2666, 117th Cong. (2021); *see also* Brandon Robinson, *Senate Introduces Legislation Requiring 24-hour Ransomware Notification*, BALCH & BINGHAM LLP (Oct. 5, 2021), https://www.jdsupra.com/legalnews/senate-introduces-legislation-requiring-3965688/.

[217] *See* Robinson, *supra* note 216.

[218] *See id.*

[219] *See* S.2666, 117th Cong. (2021).

[220] *See* Robinson, *supra* note 216.

[221] *See id.*

of the Act describes the requirements of a submitting a report to the Director of National Intelligence and the Director of the Federal Bureau of Investigation to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence no later than 180 days after the enactment of the Act. The content of this report is required to describe the implications of the ransomware threat to United States national security.[222] Specifically, the required content of the report is described in Section 5(c)(2) and is to include the following:

> (A) Identification of individuals, groups, and entities who pose the most significant threat, including attribution to individual ransomware attacks whenever possible.
>
> (B) Locations from where individuals, groups, and entities conduct ransomware attacks.
>
> (C) The infrastructure, tactics, and techniques ransomware actors commonly use.
>
> (D) Any relationships between the individuals, groups, and entities that conduct ransomware attacks and their governments or countries of origin that could impede the ability to counter ransomware threats.
>
> (E) Intelligence gaps that have, or currently are, impeding the ability to counter ransomware threats.[223]

Section 2242 of the "Sanction and Stop Ransomware Act of 2021" regards the establishment of a ransomware operation reporting system ("the system").[224] This section of the bill requires the CISA to "establish ransomware operation reporting capabilities to facilitate the submission of timely, secure, and confidential ransomware notifications by [f]ederal agencies and covered entities to the Agency".[225] Further, this section describes a security assessment that the CISA must perform on the system at least once every two years.[226] Under Section 2242(c), the Director is required to do the following: "(1) assess the security of the System not less frequently than once every 2 years; and (2) as soon as is practicable after conducting an assessment under paragraph (1), make any necessary corrective measures to the system".[227]

The Sanction and Stop Ransomware Act of 2021 is a productive bill for addressing the need for established incident response plans and reporting procedures to prepare for

[222] *See* S.2666, 117th Cong. (2021).
[223] *See id.*
[224] *See id.*
[225] *See id.*
[226] *See id.*
[227] *See id.*

ransomware attacks.[228] In order to further this bill's purpose, this Note suggests these following preliminary amendments:

> 1. Regarding the information required to be disclosed when a federal agency or covered entity facilitates a ransomware payment, there should also be a requirement to provide a written explanation as to why the payment was facilitated (i.e. continuity of essential operations).[229] This will discourage paying ransoms for reckless reasons, and will help to distinguish those cases when facilitating a ransomware payment was absolutely necessary, for instance, the circumstances of the impacted hospitals in Ireland and New Zealand described in the previous section of this article.
>
> 2. Regarding the 24-hour limit controversy, the time limit should be extended only to 48 hours if it is to be extended at all. The concern that 24 hours is not a sufficient amount of time for covered entities to comply is justified.[230] However, time is of the essence when it comes to responding to ransomware attacks and other legislative proposals require a similar 24-hour reporting window.[231] To split the difference between the concern of overburdening covered entities and the concern of responding quickly to ransomware attacks, this article suggests to implement a 48-hour time window.[232] A 48-hour time window would better provide a sufficient amount of time to determine the nature, scope, and degree of a potential cyber breach while maintaining a sense of urgency when reporting ransomware payments.[233]

---

[228] *See* Robinson, *supra* note 216; *see also* Maggie, Miller, *Senators Introduce Bipartisan Bill to Sanction Nations Involved in Ransomware Attacks*, THEHILL (Aug. 5, 2021), https://thehill.com/policy/cybersecurity/566610-senators-introduce-legislation-to-sanction-nations-involved-in/.

[229] *See* Robinson, *supra* note 216; *see also* Micah J. Fincher, *24 Hours: Government Likely to Require Notice of Ransomware Payments from Banks, Other Key Businesses*, THE NATIONAL LAW REVIEW (Apr. 28, 2022), https://www.natlawreview.com/article/24-hours-government-likely-to-require-notice-ransomware-payments-banks-other-key.

[230] *See* Robinson, *supra* note 216; *see also* Scott Ikeda, *24, 48 or 72 Hours? New Bill Complicates Regulation of Ransomware Payments, Introduces Terms that Conflict with Existing Legislation Under Consideration*, CPO MAGAZINE (Oct. 12, 2021), https://www.cpomagazine.com/cyber-security/24-48-or-72-hours-new-bill-complicates-regulation-of-ransomware-payments-introduces-terms-that-conflict-with-existing-legislation-under-consideration.

[231] *See* Robinson, *supra* note 216 ("For instance, the Cyber Incident Notification Act, introduced by the Senate in July 2021, establishes a similar 24-hour reporting window for any business that supports a national security function"); *see also* Miller, *supra* note 228.

[232] *See* Robinson, *supra* note 216; *see also* Karen Lynch, *Laws Pending on Reporting and Paying Ransomware in 2022*, MIMECAST (Jan. 24, 2022), https://www.mimecast.com/blog/laws-pending-on-reporting-and-paying-ransomware-in-2022.

[233] *See* S.2666, 117th Cong. (2021); *see also* Dan Gunderman, *New Bill Would Require Ransom Disclosure Within 48 Hours*, Data Breach Today (Oct. 7, 2021), https://ransomware.databreachtoday.com/new-bill-would-require-ransom-disclosure-within-48-hours-a-17689.

3. Referring to the failure to report on potential ransomware payments risking subpoenas and a reference to the United States Department of Justice, the subpoenas should be replaced by fines as some agencies have suggested that imposing fines would be preferred in lieu of the subpoena power.[234]

4. With regards to Section 5(c)(2), there should be another item in the report that should include the following: "(F) Any relationships or trends between the cryptocurrencies utilized in ransomware attacks and the traceability of these cryptocurrencies." (emphasis added).[235] As previously mentioned in this Note, ransomware hackers like to utilize cryptocurrencies as they believe these forms of payment are not easily traceable; for the purposes of the report, this Note argues that it would be beneficial to know if particular cryptocurrencies were desired by ransomware hackers due to the perceived lack of traceability or difficulty in tracing a particular cryptocurrency.[236]

5. With reference to Section 2242(c)(1), it should be amended to read as follows, "[t]he Director shall (1) assess the security of the System *utilizing continuous monitoring or periodic penetration testing and vulnerability assessments. In lieu of effective continuous monitoring, the Director shall perform: (a) annual penetration testing of the System's information systems determined each given year based on relevant known risks in accordance with the security assessment; and (b) bi-annual vulnerability assessments such as any reviews of information systems that are reasonably formulated to mitigate publicly known cybersecurity vulnerabilities in the System's information systems based on the security assessment*." (emphasis added).[237] These proposed amendments clarify what the Director's responsibilities are when assessing the security of the System.[238] Further, this article suggests

[234] *See* S.2666, 117th Cong. (2021)*; see also* Robinson, *supra* note 216.

[235] *See* S.2666, 117th Cong. (2021)*; see also* Julia Magas, *Law Enforcement's Guide to Policing Crypto Cybercrimes*, Cointelegraph (Feb. 19, 2020) https://cointelegraph.com/news/the-law-enforcements-guide-to-policing-crypto-cybercrimes.

[236] *See* S.2666, 117th Cong. (2021)*; see also Ransomware: Paying Cyber Extortion Demands in Cryptocurrency*, Marsh McLennan (last visited Oct. 25, 2022) https://www.marsh.com/us/services/cyber-risk/insights/ransomware-paying-cyber-extortion-demands-in-cryptocurrency.html.

[237] *See* S.2666, 117th Cong. (2021); *see also* Kevin Patterson & Joseph D. Simon, *New York State Adopts Cybersecurity Regulation*, CULLEN AND DYKMAN LLP (Feb. 28, 2017) https://www.cullenllp.com/blog/new-york-state-adopts-cybersecurity-regulation/.

[238] *See* S.2666, 117th Cong. (2021); *see also* Alexander H. Southwell et al., *New York State Department of Financial Services Meaningfully Rachets Up Cyber Requirements with New Draft Amendments*, GIBSON, DUNN & CRUTCHER LLP (Aug. 8, 2022) https://www.gibsondunn.com/new-york-state-department-of-financial-services-meaningfully-rachets-up-cyber-requirements-with-new-draft-amendments/.

> defining "penetration tests" and "vulnerability assessments" in a similar fashion to NY DFS's definitions of those terms.[239]
>
> 6. There should be a definition for the term "multi-factor authentication" in the "Stop and Sanction Ransomware Act of 2021" bill such as "authentication through verification of at least two of the following types of authentication factors:
>
> (1) knowledge factors, such as a password;
>
> (2) possession factors, such as a token or text message on a mobile phone; or
>
> (3) inherence factors, such as a biometric characteristic."[240]
>
> 7. Likewise, "multi-factor authentication" should be a requirement under Section 2242.[241] Specifically, this article suggests the following language to implement multi-factor authentication in the System: "*(a) Upon review of its security assessment, the System shall use effective controls, including multi-factor authentication or risk-based authentication to ensure protection against unauthorized access to information systems. (b) Multi-factor authentication shall be used for any person accessing the System's internal networks from an external network, unless the Director has provided written approval regarding the use of reasonably equivalent or more secure access controls."* (emphasis added).[242]

These proposed amendments attempt to strengthen the beneficial "Sanction and Ransomware Act of 2021"[243] Whether this bill inevitably gets passed into law is irrelevant to its noble pursuit of an established incident response plans and reporting in response to potential breaches or ransomware attacks.[244] Legally banning ransomware payments may potentially have disastrous consequences, however, the "Sanction and Ransomware Act of 2021" provides

---

[239] *See* 23 CRR-NY 500 (defining "penetration tests" as "a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside the covered entity's information system"; further clarifying that "vulnerability assessments" include "any systematic scans or reviews of information systems reasonably designed to identify).

[240] *See id.*

[241] *See* S.2666, 117th Cong. (2021); *see also Key compliance and security considerations for US banking and capital markets*, MICROSOFT 365 (Sept. 22, 2022) https://learn.microsoft.com/en-us/microsoft-365/solutions/financial-services-secure-collaboration?view=o365-worldwide.

[242] *See* 23 CRR-NY 500 (imposing the responsibility on NY DFS covered entities to implement multi-factor authentication or risk-based authentication to secure non-public).

[243] *See* S.2666, 117th Cong. (2021); *see also Rubio, Feinstein Introduce the Sanction and Stop Ransomware Act*, MARCO RUBIO: U.S. SENATOR FOR FLORIDA (Aug. 5, 2021) https://www.rubio.senate.gov/public/index.cfm/2021/8/rubio-feinstein-introduce-the-sanction-and-stop-ransomware-act.

[244] *See* S.2666, 117th Cong. (2021); *see also* Mariarosaria Taddeo & Francesca Bosco, *We must treat cybersecurity as a public good. Here's why*, WORLD ECONOMIC FORUM (Aug. 22, 2019) https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/.

an example of legislation that can impose incident response plans and reporting standards to fight against the emerging threat of ransomware.[245]

V. CONCLUSION

There are many sufficient methods to prevent ransomware attacks.[246] Though an outright ban of ransomware payments may seem ideal, it may cause undesirable consequences.[247] In lieu of an outright ban, insurers and regulators can take measures to improve cybersecurity resilience in society.[248] National and State governments should look into tracking Bitcoin transactions when ransomware payments are facilitated to catch cyber criminals instead of legally preventing the ransomware payment from commencing in the first place. Additionally, there are several entities that should not endure business disruption as it puts lives at risk; thus, entities such as hospitals, police departments, and elderly homes, should be the only entities to complete ransomware payments as this may be the only way to avoid continuous business disruption.

---

[245] *See* S.2666, 117th Cong. (2021); *see also* Tarah Wheeler & Ciaran Martin, *Should ransomware payments be banned?*, BROOKINGS (Jul. 26, 2021) https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/.

[246] *See* Letter from DFS to New York State regulated entities, *supra* note 189; *see also Ransomware protection: How to keep your data safe in 2022*, KAPERSKY (last visited Oct. 13, 2022) https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware.

[247] *See* Bajak, *supra* note 96; *see also* Edward Segal, *Banning Ransomware Payments Could Create New Crisis Situations*, FORBES (June 8, 2021), https://www.forbes.com/sites/edwardsegal/2021/06/08/banning-ransomware-payments-could-create-new-crisis-situations/?sh=3b80504e2982.

[248] *See* Goh, *supra* note 147; U.S. GOV'T. ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET (2021).