August 17, 2020

Ransomware – The Legal Impacts

By Thomas J. Shaw, Esq., DPO Services, Ireland

Share this:

Ransomware attacks are seemingly popping up everywhere these days. Lawyers and law firms are a prized target for threat actors, due to the significant amount of sensitive information they hold from and about their clients. Ransomware incident response firm Coveware states that “Small and medium sized professional service firms such as law firms, IT managed service providers and CPA firms continued to be the largest industry subset targeted by ransomware in Q1 2020.”[1] Ransomware attacks have recently hit law firms large and small.[2]

Healthcare Targets

Besides law firms, ransomware is also frequently directed at healthcare providers. According to one estimate,[3] the increase in ransomware attacks on healthcare entities from Q4 2018 to Q4 2019 was 350 percent! Another report[4] showed that in Q1 and Q2 2020, 41 hospitals and other healthcare providers were successfully attacked by ransomware.

Ransomware attacks can create legal issues and expenses in addition to the actual attack itself. For instance, after a SamSam ransomware attack on the servers of a healthcare software provider blocked access to its electronic health record (EHR) and e-prescribing services, it was sued[5] by a customer who needed these records for its HITECH meaningful use incentive payments. Similarly, after a dental practice was attacked with ransomware, it was sued[6] in tort and contract. The plaintiffs alleged injuries of “(1) an increased risk of their identities being stolen in the future; (2) the costs to mitigate that risk (namely, monitoring their credit); (3) overpayment for dental services, on the theory that an unspecified portion of their payment was for securing their data, which [the dental practice] allegedly failed to do; and (4) the diminishment of the value of their PII [personally identifiable information] by virtue of the possibility that it was exposed by the ransomware attack.”[7] Using the typical analysis in data breach cases after the Supreme Court’s *Spokeo* decision,[8] the court ruled that the alleged injuries were not sufficiently concrete, particularized, and imminent, so there was no Article III standing to sue.

Law Firm Targets

Law firms which have been targeted include Grubman, Shire, Meiselas and Sacks, a firm which handles many big-name clients in the entertainment field. It announced in May 2020 that its confidential files had been downloaded and its backups deleted/encrypted by hackers. These threat actors demanded $42 million in ransom not to publicly disclose this information and to provide the decryption keys. Small Rhode Island firm Moses Afonso Ryan was hit with a ransomware attack[9] that encrypted its files and had to make two ransom payments to get a working decryption tool from the threat actors. The cost of $25,000 ransom was dwarfed by the firm’s estimated $700,000 loss in business revenue during the three-month period it took for the firm to fully recover from the ransomware attack. Law firm service providers are also being targeted, as the April 2020 *Genetech v. Amgen* trial had to be delayed because the defendant's e-discovery firm, Epiq Systems, was hit with a ransomware attack.[10]

In March 2020, Hiscox Insurance Company sued its law firm Warden Grier after the law firm was breached in a ransomware attack and paid the ransom without disclosure to those affected. The insurance company and its insured customers were not directly notified of the 2016 breach, only finding out in 2018 inadvertently when an employee found some of the company's materials being offered on the dark web. The insurance company's suit[11] asserted claims of negligence, breach of fiduciary duty, and breach of the attorney-client contract, based upon failing to have appropriate safeguards to protect the personal information of Hiscox and its clients, not performing an adequate forensic investigation, and for failing to notify Hiscox and its clients after the breach. Damages of more than $1.5 million were claimed for the costs of running an investigation and for notifying and protecting the company's customers.

How Ransomware Works

Threat actors gain access to a system, often through spearphishing, an attack targeted at an employee to get the employee to click on an email attachment or weblink, launching a virus that allows the attackers inside the corporate system. Then, a second program encrypts or downloads the corporate files within the security perimeter of the organization. A message is next displayed with instructions on how to send a certain amount of cryptocurrency, such as Bitcoin, to a designated blockchain address while spelling out the consequences for not doing so. The message usually claims that the decryption key will be provided upon payment or the downloaded files will be deleted. Threat actors know that their ransom may be the smaller amount as weighed in the balance, since organizations have to think about the costs of lost business revenue, damage to systems and files, reputational injury, costs of external forensic and legal expertise, and the costs of breach notification and resolution.

Two of the more popular ransomware toolkits used by threat actors are Sodinokibi, which encrypts file systems to make them unusable by the targeted organization and Maze, which not only encrypts files on the target system but exfiltrates information in documents and emails to further squeeze the targeted organization to pay. These tools change over time but for Q1 2020, Coveware identified[12] the most popular programs and their preferred attack vectors as the following three: Sodinokibi attacking the targeted systems through either software vulnerability or remote desktop protocol compromise, Ryuk using email phishing, and Phobos employing remote desktop protocol compromise.

For 2019, the FBI's Internet Crime Complaint Center (IC3) unit reported[13] more than 2, 000 cases of ransomware, with adjusted losses of nearly $9 million but considered that artificially low, as it did not include costs such as remediation, lost business, or time spent, and many victims did not report their losses while others reported elsewhere. Other sources claim ransomware losses in the billions. These attacks have led to several ransomware issues being litigated. These include victimized companies asking their insurance company to pay or refund ransom payments, to reimburse computer damages suffered, or to freeze paid cryptocurrency ransoms. The following cases address the legal issues in both the United States and the European Union (EU).

U.S. Caselaw: When Are Ransomware Expenses Covered by Insurance?

There is no guarantee that the threat actor will follow through on its commitment to provide the keys or delete the files, so victims are often unsure whether they should pay the ransom. In a ransomware case[14] before the district court in Maryland, the plaintiff had suffered a ransomware attack in late 2016. When the company paid the ransom, the threat actor did not provide the decryption key but instead demanded a second payment. The company decided instead to replace the affected software and add more protective software, which slowed the system down considerably.

Security experts believed that the malware was still on the existing equipment. This left the options open to the company to be either replacing all of the software and reinstalling it on the existing hardware or buying a new server. The business owner insurance policy covered direct physical loss or damage to covered property, which included software, data, and media. When the company claimed the cost of the new systems to the insurance company, its claim was refused.

The insured initiated the claim to be able to purchase new hardware and software that did not include the malware and was not slowed down by the protective measures plus the lost data. The insurance company's argument in denying the claim was that because the insured's loss was data, it was not a direct physical loss. The court disagreed and ruled that the insured could recover for "(1) the loss of data and software in its computer system, or (2) the loss of functionality to the computer system itself,"[15] as these were covered under the policy' wording.

In a ransomware case[16] before the state court of appeals in Indiana, the insurance company defendant asserted that it did not have to cover losses due to a ransomware attack. The insurance policy stated that the insurance company would "pay for loss of or damages to "money," "securities" and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the "premises" or "banking premise" to a person or place outside the premises.

The insured made a claim under its insurance coverage for the payment in Bitcoin it made to the threat actor to decrypt its servers and workstations. The insurance company claimed that the ransomware attack was more like theft than fraud. The trial court agreed, saying "Unlike the fraudster, a hacker, like the burglar or car thief is forthright in his scheme. The hacker deprived G&G Oil of use of its computer system and extracted bitcoin from the Plaintiff as ransom. While devious, tortious and criminal, fraudulent it was not."[17] The court also ruled that the ransom payment did not result from the use of a computer. The court of appeals agreed with these points and affirmed.

EU Caselaw: Tracking Anonymous Threat Actors

In a ransomware case[18] before a United Kingdom (UK) court, a UK insurer wanted to get back a ransom paid to the perpetrators on behalf of its cyber-crime policy customer, a Canadian insurance company. The lawsuit was brought by the unnamed insurance company against the threat actor (called "Persons Unknown Who Demanded Bitcoin on 10th and 11th October 2019"), the people who held the Bitcoin ransom payment (called "Persons Unknown who Own/Control Specified Bitcoin"), and the Bitcoin exchange that the payment was held with, Bitfinex.

The threat actor had encrypted the Canadian company's files and then left the following message behind: "Hello [insured customer] your network was hacked and encrypted. No free decryption software is available on the web. Email us at [...] to get the ransom amount. Keep our contact safe. Disclosure can lead to impossibility of decryption. Please use your company name as the email subject."[19]

The negotiations got the amount of the ransom down to $950,000 (USD) in Bitcoin and an agreement to decrypt several files to show the threat actor had the decryption key. Then the threat actor sent the following message: "The Bitcoin address for the payment[...] When sending the payment check the USD/BTC exchange rate on bitrex.com we have to receive no less than USD 950K in Bitcoins. It takes around 40-60 minutes to get enough confirmations form[sic] the blockchain in order to validate the payment. Upon receipt we send you the tool."[20]

The threat actors delivered the decryption tool after the payment in Bitcoin was confirmed. It took the company about three business weeks to decrypt 20 servers and 1,000 desktop computers. Because 96 of the 109.25 Bitcoins paid were able to be tracked (the others were exchanged to fiat currency), the operator of the exchange was linked to the address used on the blockchain and the court believed that the operator would be required by Know Your Customer AML rules[21] to know the identity of the holder (the second defendant).

The court decided to hold the initial hearing in private, as it did not wish to tip off the threat actor that the court knew where the Bitcoins were and allow the threat actor to disperse the Bitcoins, to avoid revenge cyberattacks and copycat attacks, and to avoid revealing details of the covered customers' systems and vulnerabilities. It also had to decide how to treat Bitcoins, to be able to issue an injunction against them, finally deciding they were property, as they met the four-prong test of "being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence."[22]

The court granted an interim injunction placing a constructive trust over the Bitcoins. Given the unknown locations of the first two defendants, the court allowed for alternative service via email. The injunction also required the cryptocurrency exchange to identify the anonymous first and second defendants to allow for the return or restitution of the ransom paid.

How to Prepare and Respond

The National Institute for Standards and Technology (NIST) has published a guide for detecting and responding to ransomware[23]with a detailed technical approach. The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security advocates the following[24] preventative measures:

- Implement an awareness and training program.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind.
- Disable macro scripts from office files transmitted via email.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations (e.g. temp folders).
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.
- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure the backup (so it cannot be deleted or encrypted).

The Health Insurance Portability and Accountability Act (HIPAA)

The Department of Health and Human Services (HHS) also previously issued a fact sheet on Ransomware.[25] This stated that there were, on average, 4,000 daily ransomware attacks in 2016. It described the HIPAA Security Rule as a minimum floor, noting specific security practices that would assist in preventing ransomware, such as:

- "implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;
- training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
- implementing access controls to limit access to ePHI to only those persons or software programs requiring access."

As the presence of ransomware on the systems of a covered entity (such as a healthcare provider) or business associate (such as a law firm handling PHI on behalf of a covered entity) is considered to be a security incident under HIPAA's Security Rule, appropriate security incident response procedures in responding to a ransomware attach include:

- "detect and conduct an initial analysis of the ransomware;
- contain the impact and propagation of the ransomware;
- eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and
- conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents."

Whether the presence of ransomware is a breach can be analyzed as follows:

> "A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."
>
> When electronic PHI (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.
>
> Unless the covered entity or business associate can demonstrate that there is a "low probability that the PHI has been compromised," based on the factors set forth in HIPAA's Breach Notification Rule, a breach of PHI is presumed to have occurred."

Conclusion

While the legal issues pertaining to ransomware will continue to evolve, companies will need to closely examine their cyber insurance coverage. They will also need to implement and maintain technical and organizational measures. These include having sufficient and distributed backups, strong and omnipresent use of encryption, tested incident response and business continuity plans, rigorous vulnerability management and network penetration testing, segmentation of the network, awareness training for all employees, a tested cyber response plan, ongoing network and threat monitoring, strict access control policies, locked-down network and remote protocols, avoidance of possible entry points like macro scripts, application whitelisting instead of blacklisting, and leadership commitment to cyber security.

[1] Coveware, Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020, https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[2] ABA Journal, Hacking group publishes 'full dump' of law firm's data; another responds to cybersecurity incident (Feb. 12, 2020).

[3] Corvus, Security Report- Health Care - Hospitals, Providers and more (March 2020).

[4] Emsisoft, State of Ransomware in the US: Report and Statistics for Q1 and Q2 2020 (July 2020).

[5] *Surfside Non-Surgical Orthopedics P.A. v. Allscripts Healthcare Solutions Inc.,* No. 18 C 566. (N.D. Ill. June 4, 2019).

[6] *Blahous v. Sarrell Regional Dental Center for Public Health, Inc.,* No. 2:19-cv-798 (M.D. Ala. July 16, 2020).

[7] *Id.*

[8] *Spokeo, Inc. v. Robins*, No. 13-1339 (136 S.Ct. 1540, May 16, 2016).

[9] *Moses Afonso Ryan Ltd. v. Sentinel Insurance Co.*, No. PC-2017-1280 (R.I. Sup. Ct. Apr. 21, 2017).

[10] *Genetech, Inc. v. Amgen, Inc.*, No. 17-1407, Consol, 18-924 (D. Del. Mar. 6, 2020).

[11] *Hiscox Insurance Co. Inc. and Hiscox Syndicates Ltd. vs. Warden Grier, LLP*, No. 4:20-cv-00237 (W.D. Mo. Mar. 27, 2020).

[12] *See supra* n.1.

[13] FBI Internet Crime Complaint Center, 2019 Internet Crime Report (Feb. 2020).

[14] *National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Co.,* No. 1:18-cv-02138 (D. Md. Jan. 23, 2020).

[15] *Id.*

[16] *G&G Oil Co. of Indiana v. Continental Western Insurance Co.*, No. 19A-PL-1498 (Ind. Ct. App. Mar. 31, 2020).

[17] *Id.*

[18] *AA v Persons Unknown who Demanded Bitcoin on 10th and 11th October 2019, Persons Unknown who Own/Control Specified Bitcoin, FINEX trading as Bitfinex, and BFXWW Inc. trading as Bitfinex*, No. 3556 (EWHC (Comm) 13 Dec. 2019).

[19] *Id.*

[20] *Id.*

[21] *See* https://corpgov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/.

[22] *Id.*

[23] NIST, SP 1800-26, Detecting and Responding to Ransomware and Other Destructive Events (draft) (Jan. 2020).

[24] CISA, How to Protect Your Networks from Ransomware (2019).

[25] HHS, Fact Sheet: Ransomware and HIPAA (2016).

About the Author

Thomas J. Shaw, Esq. is an EU-based American lawyer, CPA, CIPP/E, CIPP/US, CRISC, ECM^{M}, CISM, ERM^{P}, CISA, CGEIT and CCSK, who runs DPO Services, and is the author of a dozen legal books, including: U.S. & EU Information and Internet Law - Second Edition (2020); U.S. & EU Emerging and Emerged Technologies Law - Second Edition (2020); Cloud Computing for Lawyers and Executives - A Global Approach, Second Edition (2019); DPO Handbook – Data Protection Officers under the GDPR, Second Edition (2018); Revolutionary War Law and Lawyers – Issues, Cases, and Characters (2019); World War I Law and Lawyers – Issues, Cases, and Characters (2014); and World War II Law and Lawyers – Issues, Cases, and Characters (2013). He can be reached at thomas@tshawlaw.com.

ABA American Bar Association | /content/aba-cms-dotorg/en/groups/health_law/publications/health_lawyer_home/2020-august/ran-the