LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy, Security & Cybercrime Practice April 26, 2017 | Number 2126

Ransomware Attacks: When Is Notification Required?

Ransomware is not only a growing security threat but a potentially thorny notification issue.

Ransomware is one of the most prevalent cybersecurity threats afflicting businesses today. When an attack hits, a victim company must confront the difficult question whether to pay the ransom demanded in order to regain access to the company's files and restore business operations. But there is an additional question the company may face: *does the incident need to be disclosed?* The answer may not be straightforward. When sensitive data has been encrypted by ransomware, has it been "accessed" or "acquired" by an unauthorized actor as those terms are used in relevant breach notification statutes? What risks are there that the attacker will use the information in a way that harms the individuals whose data is affected? This *Client Alert* discusses these questions as well as other legal and technical issues a company should consider in addressing notification in the wake of a ransomware attack.

What Is Ransomware?

Ransomware is a type of malicious software designed to block access to a computer system — typically by encrypting the data on it — until a sum of money is paid to the attacker. Because ransomware allows hackers to easily monetize their attacks, it has quickly become the malware of choice for many cybercriminals. According to the FBI, ransomware attacks tripled in 2016, with an average of 4,000 attacks occurring per day.[1] The attacks are generally cheap to execute and highly lucrative: ransomware payments are estimated to generate more than US$1 billion in annual revenue for the online underworld.[2]

There are hundreds of known ransomware variants in circulation today, many of which can be purchased online in the form of exploit kits or crimeware-as-a-service packages, available on hacker forums or other websites that cater to cybercriminals. Attackers frequently infect their victims through phishing emails or other social engineering techniques. Following the infection, the victim is presented with a screen indicating that the data on the infected system has been encrypted and that, in order to obtain the decryption key, a ransom must be paid — in the form of Bitcoins or other anonymous cryptocurrency — within a certain time period. Otherwise, the decryption key will be destroyed and the files will be rendered permanently inaccessible.

Ransomware has rapidly increased in sophistication in recent years, evolving into a formidable threat for businesses and consumers alike. Newer ransomware variants use strong encryption algorithms that cannot be broken by law enforcement or security firms. Additionally, many variants do not simply target individual endpoints. Instead, after establishing a beachhead on a particular device, they search out other resources on the network to encrypt, such as share drives and backup servers. In this way, ransomware attackers can cripple significant portions of a company's operations and demand significant ransoms as a result — generally ranging from several to tens of thousands of dollars,[3] but, in some reported cases, reaching amounts far higher.[4]

Whereas most other forms of cybercrime involve some type of *theft* — *e.g.*, pilfering data that can be sold on the black market — ransomware is a modern form of *shakedown* in which the victim pays the criminal directly simply to get access to the data back. Thus, in a basic ransomware attack, the attackers merely encrypt — rather than remove or "exfiltrate" — data stored on the victim's system. However, ransomware is evolving in this regard also as some ransomware strains now come packaged with other types of malware designed to steal data, not just render it unusable. For example, "RAA" and "Betabot" are both recent forms of malware that combine a ransomware payload with a data-stealing Trojan designed to steal login credentials. The attackers use the stolen credentials to hack into and infect other victims, or they simply sell the credentials to other hackers. As another example, "doxware" describes an emerging type of ransomware attack in which the attackers not only encrypt the victim's data, but threaten to post the data publicly online, thereby exerting additional leverage on the victim to pay the ransom. As these trends reflect, cybercriminals are increasingly likely to use ransomware as only one part of a broader toolkit in order to maximize their potential means of extracting profit from their hacking activity.

HHS Guidance on Ransomware Attack Notification

When are companies required to disclose a ransomware attack? To date, the only regulator to have issued explicit guidance on the subject is the US Department of Health and Human Services (HHS).

In July 2016, in the face of mounting ransomware attacks against the healthcare sector, HHS issued informal guidance (the HHS Guidance) specifically addressing the notification obligations of healthcare providers and other businesses covered by the Health Information Portability and Accountability Act (HIPAA) in the event of a ransomware incident.[5] Under HIPAA, such covered entities are generally required to notify HHS in the event of any breach of unsecured protected health information (PHI). The HIPAA rules define a "breach" as the unauthorized "acquisition, access, use, or disclosure of PHI" that "compromises the security or privacy of the PHI."[6]

The HHS Guidance characterizes ransomware as "distinct from other malware," as "its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data ... until a ransom is paid."[7] The HHS Guidance notes that some variants of ransomware also exfiltrate data, or work together with other malware that does so.[8] Yet, perhaps surprisingly, HHS does not take the position that such exfiltration is necessary for a ransomware infection to qualify as a breach. Rather, the HHS Guidance states that any ransomware attack affecting PHI presumptively qualifies as a breach under HIPAA because the encryption of PHI resulting from the attack implies that the PHI has been "acquired" by attackers, in the sense that "unauthorized individuals have taken possession or control of the information."[9] On this view, the attacker's encryption of the data alone appears to qualify as an "acquisition" — even if the data is never viewed or stolen by the attacker.

Importantly, the HHS Guidance still adheres to the basic HIPAA multi-factor risk assessment for breach notification, which applies whenever a "breach" has occurred within the meaning of the HIPAA rules. Under that framework, if there is a "low probability" that the PHI affected by the breach has been "compromised," then the notification requirement does not apply. What the term "compromised" means in the context of a ransomware attack, however, is not entirely clear. The HHS Guidance suggests that a variety of factors could be relevant. One factor is "whether or not the malware may attempt to exfiltrate data" — *i.e.*, whether the malware results in the data being stolen, not merely inaccessible.[10] But the HHS Guidance indicates that other types of impacts must be considered as well. In particular, if "there is high risk of unavailability of the data" or "high risk to the integrity of the data" — *e.g.*, if the ransomware "deletes the original data and leaves only the data in encrypted form," and there is no ability to restore the data from a recent backup — these factors point toward "compromise" as well.[11] Overall, the HHS

Guidance seems to contemplate that any significant damage to the confidentiality, integrity or availability of PHI caused by a ransomware attack gives rise to a reporting obligation under HIPAA.

How Do State Breach Notification Requirements Compare?

In 2002, concerns over consumer privacy and data security on the internet led California lawmakers to enact a law requiring companies suffering a breach to inform any California residents whose personally identifiable information (PII) was exposed in the incident. Since California's law took effect in 2003, an additional 47 states have enacted similar breach notification laws. The main purpose of these laws is to protect individuals from identity theft or other forms of harm that could occur as a result of a data breach. Unlike HHS, the attorneys general and other authorities responsible for enforcing these notification requirements have not, so far, issued specific guidance addressing whether or how the requirements extend to ransomware attacks.

However, as with the HIPAA breach notification rule, the majority of state breach notification requirements are triggered when an unauthorized actor "accesses" and "acquires" PII stored on a company's network. Many of these laws also include provisions requiring a breach to be reported only if it poses a reasonable likelihood of harm to the customer. (In the same vein, some statutes also include a specific safe harbour provision making notification unnecessary if the stolen data was encrypted prior to the theft and thereby rendered unreadable to the attacker.)

None of the state breach notification statutes includes a definition of "acquisition," but the term is commonly understood to imply a "taking." It is certainly conceivable that state authorities could construe the term "acquisition" as broadly as the HHS Guidance and apply the term presumptively to any ransomware attack. But given that the core concern underlying state breach notification statutes is to protect consumers against identity theft or other tangible harms, it would seem natural to apply the term only where attackers actually "take" unencrypted PII from a computer system — in the sense of moving the data to the attackers' own servers, so that they may sell or use the stolen data themselves — rather than merely encrypting the data on the victimized system and rendering it unusable by the system owner. In the absence of any explicit guidance to the contrary by state authorities, application of the ordinary concepts of acquisition and likelihood of harm should mean that, where an attacker merely encrypts (locks up) data containing PII, and forensic analysis reliably indicates that the data has not been viewed, copied, or moved by the attacker, notification should not be required.[12]

However, given the continuing evolution of the ransomware threat and its increasing deployment in combination with other malicious payloads, companies dealing with a ransomware attack cannot readily assume that the damage is limited to the encryption of data. Careful investigation is needed, by qualified forensic experts, to determine the full scope of the attacker's activity. At a minimum, it is important to identify the specific strain of malware used in the attack, in order to determine its full range of capabilities — including whether it includes any credential stealers, keyloggers, exfiltration tools or other features designed to facilitate data theft. Further, the attacker's footsteps need to be carefully retraced to determine how the company's network was penetrated and whether the attacker engaged in any malicious activity other than deploying ransomware. Companies should be careful not to rush to judgment about the attacker's motives and methods. And, of course, to the extent that the attackers themselves assert that they have stolen data in addition to encrypting it — as with doxware attackers who threaten to publicly post the victim's data if the ransom is not paid — attention to these issues becomes all the more urgent.

In the event that the company's investigation indicates that the attackers could have viewed or stolen PII as a result of the incident, state breach notifications may very well apply. Just as in any other data breach

scenario, the company must carefully analyze each potentially applicable state requirement to determine if its specific terms reach the particular facts and circumstances of the incident.

Conclusion

Ransomware has proven to be a highly effective form of cyberattack, allowing criminals to quickly monetize an intrusion into a corporate network. As this form of cybercrime continues to grow and diversify, regulatory expectations for companies to disclose such attacks may expand as well. In the event that a business suffers a ransomware attack, it is important to consider potentially relevant notification obligations and how they might apply to the incident. That analysis, in turn, requires a close examination of the digital facts and a thorough understanding of the potential effects of the attack on customer information or other sensitive data.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Serrin Turner
serrin.turner@lw.com
+1.212.906.1330
New York

Marissa R. Boynton
marissa.boynton@lw.com
+1.202.637.3307
Washington, D.C.

You Might Also Be Interested In

US Magistrate Judge Upholds Search Warrants for Google Data Stored Overseas, "Shards" and All

Keeping Your Company's Data Safe This Tax Season

European Commission Proposes ePrivacy Regulation

NYSDFS Revises Cybersecurity Rules to Accommodate Industry Concerns

---

Endnotes

[1] U.S. GOVERNMENT INTERAGENCY GUIDANCE DOCUMENT, *HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE* (2016), *available at* https://www.justice.gov/criminal-ccips/file/872771/download.

[2] David Fitzpatrick & Drew Griffin, *Cyber-Extortion Losses Skyrocket, Says FBI*, CNN.COM (Apr. 15, 2016, 2:20 PM), *available at* http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/.

[3] IBM X-Force Research, *Ransomware: How Consumers and Businesses Value Their Data* (Dec. 14, 2016), *available at* https://blog.knowbe4.com/ibm-study-70-percent-of-businesses-attacked-pay-ransomware, at 13 (reporting that over half of surveyed businesses victimized by ransomware paid over $10,000 in ransom, while 20 percent paid more than $40,000).

[4] Darlene Storm, *Hollywood Hospital Hit with Ransomware: Hackers Demand $3.6 Million as Ransom,* COMPUTERWORLD (Feb. 15, 2016), *available at* http://www.computerworld.com/article/3032310/security/hollywood-hospital-hit-with-ransomware-hackers-demand-3-6-million-as-ransom.html.

[5] HEALTH AND HUMAN SERVICES, *FACT SHEET: RANSOMWARE AND HIPAA* (2016), *available at* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (HHS Guidance).

[6] 45 C.F.R. § 164.402 (2013).

[7] HHS Guidance at 1.

[8] *Id.*

[9] *Id.* at 5-6.

[10] *Id.* at 6.

[11] *Id.* at 6-7.

[12] Obligations aside, there may be circumstances where a company wishes to *voluntarily* disclose such an incident to state authorities and consumers, particularly where the incident may become public knowledge in any event — due, for example, to the possibility of media leaks or the application of independent notification requirements, such as SEC disclosure requirements for public companies, if the ransomware attack qualifies as a material event.