Published on *The National Law Review* https://natlawreview.com

Twelve Things You Need to Know Now About Ransomware

Article By:

Ryan P. Blaney

Margaret A Dale

Bradley I. Ruskin

Nolan M. Goldberg

While most organizations are aware that ransomware attacks involve the use of malicious software that renders data inaccessible and systems inoperable, it is often unappreciated how the nature of these attacks, as compared to other cyber-attacks, might impact incident response and the risks faced by a victim. This client alert provides a framework for addressing the myriad issues that an organization must face in the aftermath of a ransomware attack.

1. What is ransomware?

Ransomware refers to a category of cyber-attack where encryption (or other similar mechanism) is used to render data inaccessible and cripple computer systems. The bad actor then offers to restore the data and systems in exchange for a ransom payment, made typically in cryptocurrency. Notably, however, these attacks vary widely in sophistication and scope, ranging from a simple intrusion into a single computer that are automatically triggered to larger and human guided intrusions into – and incapacitation of – an entire network.

2. Ransomware's "Triple Extortion"

A defining characteristic of a ransomware attack is the promise to restore systems and data if a ransom is paid. For example, in 2016 ransomware attacks of this type impacted a number of entities, including a hospital in Los Angeles that was well publicized by the media. More recently, however, bad actors are layering two additional types of extortion onto attacks. With more frequency, bad actors exfiltrate data during the early stages of a ransomware attack and then threaten to publish and publicize that data if the ransom is not paid, compounding the potential harm of the initial attack (a second layer of extortion in addition to rendering the data inaccessible). One of the earliest examples of this type of "double extortion" happened in 2019 against Allied Universal. The third type of extortion involves steps by such bad actors to mine the exfiltrated data to identify any confidences or other sensitive information belonging to third parties (customers, business partners, etc.) and then

attempt to extort them as well. For example, after stealing patient data from the Finnish psychotherapy clinic Vastaamo and demanding a ransom from the clinic, the bad actors also demanded smaller sums from each of the patients whose data was exfiltrated, under threat of publishing therapist session notes. Accordingly, ransomware attacks are associated with at least three different types of extortion.

3. The calling card

A victim of a ransomware attack often finds a text file or other message that directs the victim to a website where they can find out the amount of the demanded ransom and pay it. But it is often the case that a clock starts as soon as the victim accesses the site, threatening to increase the ransom progressively after certain periods of time. Accordingly, even though an organization may have an urgent need to understand how much money the bad actor is seeking, it is often advisable to delay until an organization has a plan and a team in place. Otherwise, the threat of an ever increasing ransom may become yet another pressure on the organization. It is also advisable to work with consultants that are familiar with the bad actor and have experience negotiating with the bad actor or similar bad actors. You can often get insights into for how much a bad actor settled other ransomware attacks.

4. What does a sophisticated ransomware attack look like?

A sophisticated ransomware attack looks, at first, the same as any advanced cyber-attack. The bad actors first gain access to your network by, for example, exploiting a human or technological vulnerability in security. Once on the network, the bad actors conduct reconnaissance to map the network and tries to move laterally into other adjacent computer systems. The bad actors may – but not always – try to mine whatever value they can from the network, exfiltrating any data that they come across. They may – but not always – disable any backup systems to impede or prevent restoration of inaccessible and inoperable systems, and may – but not always – take steps to destroy log files that may have otherwise later been used to shed light on the bad actors activities during the intrusion. The use of the ransomware software itself happens at the end of the attack, at a time of the bad actors' choosing, and after they have accomplished whatever other goals they had for the intrusion.

5. Who is carrying out these attacks?

The most sophisticated ransomware attacks are carried out by a form of criminal organization known as "ransomware-as-a-service." Here, a central criminal group provides tools, training, and the infrastructure to process ransomware payments and publicize exfiltrated data. "Affiliates" of the group then carry out individual attacks and split the proceeds with the main organization. Practically, this structure has had two significant consequences: 1) the use of such a scalable arrangement has led to ever increasing numbers of these types of attacks; and 2) not all affiliates of a group have the same level of sophistication, so determining the group involved will not necessarily provide insight into what a particular set of bad actors might have done while on your network.

6. Why are ransomware attacks particularly difficult to respond to?

The use of encryption during a ransomware attack has the effect of making the response to a ransomware attack exceedingly difficult. For example, the log files that might typically be used by a forensic analysist to determine what an attacker did while on the network and whether data has been

exfiltrated, may be encrypted and inaccessible. Accordingly, it may be impossible to determine how the attacker first gained access to your network, whether files were exfiltrated, or even what specific files may have been on the network at the time of the attack. Practically, this means that a company may first learn that data was stolen when some or all of the data is published by the bad actors. Accordingly, decisions about issues such as remediation and statutory notice may need to be made based on sub-optimal and limited information and may ultimately be wrong. In such circumstances, it may be more important than ever to be in position to show regulators that the company acted reasonably and timely despite, perhaps, having made certain (understandable) mistakes in its incident response, should that turn out after the fact to be the case.

7. How should you respond to a ransomware attack?

An organization should follow its typical incident response plan for a sophisticated cyber-attack, with the additional work streams, including: 1) determining the best way to restore or rebuild the impacted systems; and 2) managing any ongoing extortion and the enhanced risk of negative publicity that such an attack poses. If the initial point of compromise cannot be determined an organization should consider whether compensating controls, such as enhanced monitoring, can be employed to prevent the bad actors from regaining access to the network and decrease the likelihood of future attacks by other actors. Should the attack become public – either through required statutory notifications or the actions of the bad actor – regulatory investigations and litigation might foreseeably follow. Accordingly, an organization should consider at the inception of the incident response which activities will be conducted under privilege and which will be conducted as ordinary course (and discoverable) business activities.

8. Build your team

In order to maintain privilege for various aspects of the organization's incident response, the response should be directed by counsel and not conducted as an internal, ordinary course, IT exercise. An organization should retain an experienced forensics vendor to investigate the intrusion and advise on containment and remediation. This vendor can be retained directly by outside counsel as a best practice to strengthen the privilege claim over its efforts. Finally, demanded ransom payments can be negotiable, and if an organization is considering paying the ransom, it may want to retain specialists in such negotiations in order to achieve the best (and least expensive) possible outcome. The bad actor is less likely to negotiate in bad faith if it risks its credibility and thus the likelihood of future payments from other victims.

9. Should you notify Law Enforcement?

Generally speaking, notifying law enforcement of a ransomware attack can have several practical benefits: 1) a company can gain valuable intelligence on the bad actors; 2) law enforcement may be able to assist with system restoration; 3) law enforcement may be able to recover a ransom payment that was made; and 4) a company can better portray its response to the incident in a positive light and potentially deflect accusations of intentional concealment. A company that chooses to work with law enforcement should give due care however to the circumstances under which it provides such information both to preserve any claims of privilege over the incident response and to prevent voluntarily disclosed information from being obtained by other branches of the government who may view your company less as a victim and more as a revenue source.

10. Will you be obligated to provide notice of the attack?

With regard to statutory notice, the answer will depend on the contents of the impacted data (which you may not be able to determine because of the encryption) and whether data was actually exfiltrated (which, again, you may not be able to determine because of the encryption). Indeed, there have been circumstances where the bad actors claim to have exfiltrated data, but the data is never published as threatened, and it is possible that no exfiltration actually occurred. Assuming you are able to determine what files were on the system, the notice question will likely hinge on whether applicable statutory notice laws are triggered by mere "access" or if they require "acquisition." Even in the absence of exfiltration, the mere encryption of the files might qualify as "access." Acquisition-triggered notice typically requires more – some level of likelihood of actual intrusion into the contents of the files. Notice may also be required by a company's contracts with its clients, customers and vendors. Contractual notice will depend on the specific requirements of each contract. Where a company is unable to gain a complete understanding of what files may have been impacted and whether those files were acquired, a company will need to make the best determination it can make under the circumstances, and prepare for the possibility that it will subsequently come out that it unintentionally made a wrong call.

11. Industry specific rules and guidance, such as the SEC, may require additional disclosures

The SEC's 2018 Statement and Guidance on Public Company Cybersecurity Disclosures provides general guidance to companies about considerations for when to disclose a cyber-incident, including a ransomware attack. According to the guidance, disclosure requirements are tied to materiality, which requires a company to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading." The SEC will consider information to be material if there is a "substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available." A company's financial statement disclosure may include expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services. Because these disclosure requirements indirectly encompass cybersecurity incidents, it may be necessary to disclose not only successful ransomware attacks, but also attempted attacks. The regulatory risks of making any ransom payment, as well as the broader criminal goals of Ransomware attacks today, will likely mean that more attacks will need to be reported as material events.

12. To Pay or Not to Pay?

The decision of whether or not to pay a ransom is often a difficult one. In the abstract, we all know that paying a ransom emboldens criminals and leads to more ransomware attacks. And the payment of a ransom does not necessarily mean that access to the data will actually be restored. Such considerations are not at all easy or simple for a company whose operations have been impeded, with no easy restoration in sight. If a company is considering paying a ransom, it should consider: 1) hiring a professional with experience in negotiating down ransom payments; 2) whether there are any legal prohibitions on paying a particular bad actor, such as an entity subject to OFAC sanctions; and 3) notifying law enforcement prior to paying the ransom, to, among other things, increase the chances that the bad actor might be identified and the ransom recovered. It is important to note that the decision of whether or not to pay the ransom and whether or not statutory (or contractual) notice involve independent considerations. Indeed, it may be the case that a company that pays a ransom, thus avoiding the publication of stolen data by the bad actors, will still need to provide statutory

notice, resulting in the attack still becoming public knowledge despite the payment.

National Law Review, Volume XI, Number 182