Hashed & Salted | A Privacy and Data Security Update
April 2022

What Now? A Business Guide to Navigating Ransomware Attacks

An organization that wakes up to a locked screen and a ransom demand may understandably ask, "What now? How do I get my business back up and running?" In recent years, ransomware has become a common source of business disruption for large and small organizations alike. Media headlines are littered with news of ransomware attacks debilitating business operations of entities across sectors, including critical infrastructure services, IT service providers and financial institutions.

Ransomware and other forms of cyberattacks are on the rise. In light of recent global events, the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) issued a "Shields Up" alert, warning of a potential increase in cybersecurity attacks on U.S. organizations. The White House has also issued a Statement by President Biden on our Nation's Cybersecurity, stating that it is critical for U.S. organizations to harden cybersecurity infrastructure in today's cyber threat-heavy global environment.

This article provides a high-level overview of reactive measures that impacted organizations should take in response to a ransomware attack, as well as proactive measures they should take to mitigate risk of a ransomware attack in the first instance.

What is ransomware?

Ransomware is a type of malware pushed by threat actors to deny an impacted organization the ability to access files on its own computer systems and networks. Threat actors have increasingly deployed two-pronged ransomware attacks, in which they (1) encrypt files on an entity's computer systems and (2) exfiltrate sensitive data contained within those systems, including confidential, proprietary and personal information. Once a threat actor executes a ransomware attack, an impacted organization will be locked out of its own systems and will typically receive a ransom demand requiring payment of a substantial sum in cryptocurrency in exchange for the decryption key and, where relevant, a promise by the threat actor to refrain from leaking exfiltrated data on the dark web. Recent reports estimate that in 2021, the average ransom demand issued by threat actors rose to approximately $2.2 million.

Reactive measures

Organizations impacted by a ransomware attack should consider the following reactive measures:

- **Engage external experts**. When impacted by a ransomware attack, an organization should immediately engage external experts, including legal counsel to help navigate legal obligations stemming from the incident and to oversee investigations by additional experts under legal privilege, IT forensics consultants to assist with identifying the scope of impact to the organization and assisting internal teams to identify necessary remediation steps, and additional

Attorney Advertising

experts as appropriate to assist with threat actor intelligence, negotiations and payments.

- **Develop a communications plan.** Where an incident results in a large-scale business disruption, impacted organizations should ensure that internal and external communications limit legal and reputational risks. While customers may push for answers regarding a system outage, it is important to refrain from speaking too soon, at least until a forensics investigation has further identified the scope of impact to the organization. Internal and external communications should generally relay the facts as known to the organization at the time. As further discussed below, it is important to carefully consider whether the "B" word (breach) applies before using the term in initial communications, as this is a legal term of art that requires consultation with legal counsel and forensics experts.
- **Law enforcement notification.** Entities in certain sectors may have a legal obligation to report ransomware attacks and payments to law enforcement agencies. For example, in March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which requires covered entities in the critical infrastructure sector to report a ransomware payment to CISA within 24 hours, and a covered cyber incident within 72 hours. Reporting obligations under the Cyber Incident Reporting for Critical Infrastructure Act will apply to certain entities (as further defined through rules promulgated by CISA) that fall within one of the 16 critical infrastructure sectors identified under Presidential Policy Directive 21 (PPD-21): chemical, commercial facilities; communications; critical manufacturing; dams; defense industrial bases; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems. Entities that are not covered by a specific legal obligation to provide law enforcement notification of a ransomware attack may still choose to report the incident to federal law enforcement, including the FBI and the U.S. Secret Service. Law enforcement may be able to provide an impacted organization with critical threat actor intelligence to aid in an investigation and related remediation efforts. While it is important to remember that certain discussions with law enforcement may waive legal privilege to otherwise privileged information regarding an incident, the FBI is usually most interested in log activity and other limited information that likely will not be privileged in the first instance. Steps can and should be taken to limit what is shared to information that is not personally identifiable, company confidential information or otherwise privileged information. Counsel should be involved in those discussions and can help assess the scope of information that can be shared. Impacted organizations should work with legal counsel to determine whether law enforcement notification is appropriate under the circumstances.
- **Ransom payment.** Several factors may incentivize an impacted organization to pay a ransom demand, including the desire to halt the attack, regain access to encrypted data and systems, restore disrupted business operations, and prevent threat actor leakage of exfiltrated data, the leakage of which could result in legal and reputational risks to the organization. It is important to determine whether payment of a ransom demand is appropriate based on the forensic evidence. For example, if an entity's investigation reveals that the threat actor has not actually exfiltrated sensitive data from company systems and the company is otherwise able to restore encrypted data from backups in an efficient manner, payment of a ransom demand may not be an appropriate course of action. On the other hand, where an entity determines that it is unable to restore business operations without access to the decryption key, it may consider paying the ransom to reduce operational downtime; however, organizations should bear in mind that payment of ransom does not guarantee that the threat actors will restore access to data or refrain from disclosing or otherwise compromising sensitive data or assets. Legal, business and reputational risks should always be top of mind. Prior to making a ransom payment, it is crucial to consider the regulatory risks associated with payments in violation of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) guidance. OFAC guidance prohibits U.S. persons from engaging in transactions, directly or indirectly, with persons on OFAC's Specially Designated Nationals and Blocked Persons List, under a strict liability regime. It is

important to determine whether a threat actor is a sanctioned party prior to making a ransom payment to avoid strict liability penalties.

- **Legal notification requirements:** As noted above, it is important to carefully consider whether the "B" word (breach) applies when considering legal notification obligations resulting from a ransomware attack. The term breach or security breach should not be used casually (or otherwise) in any discussions regarding what has occurred without legal guidance. Under the U.S. state data breach notification statutes, "breach of security" is a defined term that includes unauthorized access to and/or acquisition of "personal information," as defined by applicable state law. Legal counsel, along with IT forensics consultants, will be able to assist an organization in determining whether an incident amounts to a notifiable breach under the U.S. state data breach notification statutes and other applicable law. Where a ransomware incident results in a notifiable breach under the state statutes, notice is generally required to be given to affected individuals and, in some jurisdictions, to state regulators. Additional legal notification obligations may arise under sector-specific laws, including, for example, under the federal Health Insurance Portability and Accountability Act (HIPAA).
- **Contractual notification requirements.** Service providers impacted by a ransomware attack should review contractual agreements in place with customers to identify applicable contractual notification obligations arising from an incident. It is important to promptly review all contractual terms in place to identify customer-specific notification triggers and related notice requirements, particularly given that such requirements may differ from those under the state- and sector-specific breach notification statutes, including but not limited to with respect to the scope of information covered.

Proactive measures

Entities of all sizes should implement proactive measures to mitigate risk of a ransomware attack in the first instance. The White House recently issued a Fact Sheet: Act Now to Protect Against Potential Cyberattacks, urging U.S. organizations to adopt controls aimed at mitigating the risk of cybersecurity incidents. Below is a high-level summary and insights regarding the White House guidance:

- **Implement multi-factor authentication**. Entities should mandate the use of multifactor authentication (MFA) for remote access to company networks. MFA has separately been described by the N.Y. Department of Financial Services as "an essential part of cybersecurity hygiene." MFA makes it more difficult for threat actors to gain access to company systems and networks, and therefore lessens risk of a ransomware attack. Of note, the California Attorney General has also long taken the position that MFA is critical to maintaining "reasonable security."
- **Encrypt your data.** The White House guidance urges entities to encrypt data to prevent threat actor use of stolen information. Encrypting data both in transit and at rest may also help to mitigate data breach notification obligations stemming from a ransomware incident under the U.S. state- and sector-specific data breach notification statutes. Notably, many breach notification statutes provide an exception to the definition of "breach," and a safe harbor to notification obligations, where data is encrypted and the encryption key has not also been compromised in an incident. Also, again, the California Attorney General has identified encryption as a measure critical to maintaining "reasonable security."
- **Adopt appropriate monitoring and security controls.** Entities should deploy security tools, including monitoring technology, on computers and devices to monitor for and remediate security threats on an ongoing basis. The White House guidance further provides that entities should work with cybersecurity professionals to ensure that systems are patched and protected against known vulnerabilities. Entities should also adopt an appropriate password policy and change passwords on an ongoing basis to ensure that previously compromised passwords are useless to threat actors.
- **Back up data regularly.** The White House guidance notes that entities should back up data and ensure that they have offline backups beyond the reach of threat actors. It is good practice to maintain system backups outside an entity's own network environment. Notably, an entity may be able to minimize business disruption

caused by a ransomware attack by rebuilding systems with its own backups, which in turn may eliminate the need for the decryption key held by threat actors.

- **Provide employee training.** Entities should educate employees on common attack vectors that threat actors use to gain access to computer environments. It is also important for companies to run tabletop exercises to test incident response plans and prepare for actual cybersecurity events.
- **Engage with law enforcement.** The White House guidance further urges entities to proactively engage with local FBI field offices or CISA regional offices to establish relationships in advance of a cybersecurity event.

Related Professional

Alaa Salaheldin . . . . . asalaheldin@loeb.com

6940 REV1 04-22-2022