CLM 2018 Cyber Summit
October 11 & 12, 2018 in Atlanta, GA

Effective Preparation against Ransomware Attacks:
A Case Study

I. Ransomware Attacks: Understanding the Threat Landscape and Real World Risks

Encryption attacks, more commonly known as ransomware, are one of the major cyber threats facing businesses today. No company is immune from threat of attack – any business that is connected to the internet is at risk. Industry experts estimate that a business falls victim to a ransomware event every 40 seconds. In 2017, monetary damage from ransomware attacks was estimated to have exceeded $5 billion, and some industry analysts expect that figure to more than double by 2019, up to $11.5 billion.

These attacks are becoming increasingly sophisticated both in the reach of the attack vector and capabilities of the malware variants used to perpetrate attacks. Whereas ransomware used to focus solely on locking down a company's files, many variants are now capable of exfiltrating a company's data as well. This introduces a host of potential legal ramifications in addition to the often severe monetary consequences that inevitably accompany a business shutdown caused by encryption attacks.

Intrusions Resulting from Breaches in Vendor System Security - The All Too Common Scenario

A small mortgage broker specializing in servicing residential buyers maintains current technological system protection that are reasonable and financially practicable. This broker partners with a number of different vendors that facilitate different parts of the closing process, and the parties are in constant communication as part of their daily business.

For example, a loan assistant receives an email from one of these vendors with what appears to be a secure link to access documents relating to an upcoming residential real estate closing. What the loan assistant does not know is that a hacker has infiltrated the vendor's email account, and has sent a fraudulent email posing as the vendor.

The loan assistant clicks on the link embedded in the email, and is redirected to a site where he is prompted to enter his network credentials to retrieve the documents. Once the loan assistant enters his credentials, the hacker now has access to his business email account.

The hacker logs into the email account and enters search terms intended to yield access to personal information of the mortgage broker's customers. Because brokerage employees use the same credentials to access their email accounts and other parts of the network, the hacker is also able to log into the company's network environment through an open Remote Desktop Protocol port and launches malware that (1) harvests information from the system about employees and customers, and (2) after the harvest is complete, launches a system-wide encryption attack that infects all servers, computers and other devices connected to the network, resulting in a total shut down of business operations.

The company has a series of policies and procedures for regular back-up of critical data. However, the back-up system is online and connected to the network. As such, the malware encrypts not only the primary files, but the back-ups as well, leaving the company with few options other than to pay the ransom to retrieve their data.

Additionally, even if the data can be retrieved, the attacker's acquisition of the vast amount of consumer personal information that the company collects to facilitate real estate transactions has separate legal consequences that cannot be as readily remediated.

There are a number of measures, both technological and institutional, that could have prevented this scenario with adequate planning. Once an organization has suffered such an attack, there are also effective measures an organization should have in place to remediate the potential consequences of the incident.

II. Effective Preparation Requires a Holistic Approach

A. Information Security

1. Ensure that remote access connections are secure

Most businesses permit remote access to their networks, either for the purposes of employee convenience, or for use by third party IT vendors conducting network maintenance. Remote Desktop Protocol (RDP) is the single most common means of access for ransomware attackers. If RDP access is not a business necessity, it should be disabled. If RDP access is a must, it should always be behind a Virtual Private Network (VPN). Additionally, disable any unused telnet ports.

2. Regularly backup your data – offline

The most efficient countermeasure against an operations shutdown from ransomware attack is an effective data backup policy. For organizations that regularly back up data, an attack may have only a short-term impact because files can be restored without resort to paying the ransom. Business and operations critical data should be backed up daily, or at a minimum weekly, and back-up systems should be tested on a regular schedule to ensure that data can be successfully restored.

However, even the most efficient backup systems can be rendered useless in restoring business operations if the backup system is online and therefore vulnerable to attack. Many ransomware

variants are capable of corrupting both primary and backup data. Taking backups offline shields them from corruption by the malware used to perpetrate the encryption attack.

3. Endpoint detection systems/software updates

2017 and 2018 are seeing the trend in ransomware attacks moving away from use of malicious executable (or .exe) files to deploy malware. A recent Ponemon Institute study found that 77% of successful attacks in 2017 utilized so-called "fileless" techniques. This poses a challenge for traditional antivirus and other security products, which focus largely on analyzing executable files in order to detect system vulnerabilities.

Host Intrusion Prevention Systems, for example, work in your system to learn user behavior, and by doing so, can be stop attacks by detecting activity that is inconsistent with normal user actions. Intrusion Detection Systems monitor systems in real time to detect network abnormalities. When anomalies are detected, alerts are immediately sent to a designated individual within your organization.

It is also critical to ensure that security software is kept up-to-date on all machines and devices that are connected to your network. Updates often include patches for the most current security vulnerabilities. Equally as important is confirming that your operating system patches are up-to-date, as encryption attacks frequently exploit operating system vulnerabilities.

4. Conduct Employee Awareness Training

As described above, ransomware can be deployed through phishing attacks, which require an end user to open the malicious attachment or click on the URL to execute the malware. Therefore, it is critical to an organization's security that its employees are knowledgeable of the threats that can be posed by phishing emails and are trained to be vigilant in recognizing and reporting suspicious emails. Organizations should provide periodic mandatory training on phishing emails and other vectors of ransomware attacks, and designate an individual in your IT department to whom employees can ask questions if they suspect an email is suspicious. When the email address belongs to an existing contact, but the employee is in doubt about the authenticity of the sender, it always best practice to pick up the phone and call the sender to confirm the message.

B. Legal and Organizational

1. Develop an Incident Response Plan

It is imperative that organizations develop, in consultation with key stakeholders, an incident response plan that will enable the organization to act swiftly and comprehensively to remediate any potential data security incident. These plans are also often a de-facto mandate of the information security standards promulgated by many U.S. state and international authorities and thus, are often key to regulatory compliance.

An effective incident response plan designates all departments within an organization that must work together to effectively respond to an incident. Companies should designate key members

of each department who will be responsible for executing their department's role in the event of an incident, and the method by which decision-makers will communicate and collaborate. It is equally important to test the logistical feasibility of the plan by testing it through training exercises during which the key personnel walk through a simulated response to an incident.

2. Protect Data In Possession of Third Party Vendors

There are inherent risks associated with information being processed, transmitted or stored by third party service providers. To protect your organization from shouldering the financial burden of attacks originating with a vendor, it is important to ensure that your contract contains provisions that provide protection to your data and appropriately shift the risk of loss to your vendor in the event that an attack on your vendor's systems corrupts your company's data as well. Important provisions include requiring the vendor to comply with prescribed information security practices, indemnification against third party claims arising from an incident that originates with the vendor, limitation of liability clauses, and additional insured provisions, including a requirement that the vendor carry cyber liability insurance.

It is also important to understand your organization's rights under third party vendor agreements, particularly provisions regarding your right to audit their information security systems. In the event of a breach, should your company have failed to exercise these rights, as discussed below, the ability to recover from your vendor damages relating to third party claims may be substantially impaired.

C. Insurance

1. Understand and maintain essential insurance coverages

There are a variety of policies available to protect your organization from cyber security incidents, including the costs an organization may incur to respond to such incidents, and other first party costs and/or third party claims.

a. Cyber: Cyber policies are unique as they have both 1st and 3rd party insuring agreements. First party insuring agreements usually include: cyber incident response, BI, Digital Data Recovery and Network Extortion. Third party includes: cyber, privacy and network security liability as well as media liability in some cases.

b. Business Interruption: Ransomware attacks have caused significant impacts to businesses, and these businesses have mitigated those losses through business income and extra expense insuring agreements. Cyber insurance has continued to grow to $1.84 billion in premiums in the US in 2017, a 37% increase from the prior year. These policies are even being expanded as insurers consider reputational harm insuring agreements as well.

2. Understand the claims management process

A critical part of the incident response plan is the direction to notify your insurance carrier immediately in the event of an attack. Your carrier can deploy tremendous resources on your behalf, walk you through the mitigation and remediation processes, and recommend experts who can assist you with each phase.

There are two tracks for insureds during this process that must be done in concert with each other: tendering the claim to the carrier and working with the adjuster as well as engaging the incident response coach and other vendors to remedy to incident.

III. Effective Remediation Requires Swift Action Geared Toward Legal Compliance

A. Data Recovery – to pay or not to pay?

There are both benefits and risks to consider when it comes to the decision to pay or not pay. Depending on what has been encrypted, the ability of the company to restore the information without paying a ransom, and the critical business need of that information, companies are sometimes faced with a critical decision to pay the ransom or suffer longer term business impact. We have observed a number of companies making the payment that enabled them to get back to business as usual. Payments resulted in a quick way to unencrypt the data at issue. These payments facilitated a significant reduction in future economic harm to these companies from a number of perspectives including further reputation harm, lost sales, and costs to recover digital data.

However, there are risks to paying the ransom:

- The exortionist may provide decryption software, but due to file corruption issues, it fails to restore certain critical complex files like databases, virtual machines and email containers.
- The decryption tool decrypts all the files that are stored locally, but fails to decrypt files stored on mapped drives, NAS devices, and external media.
- The extortionist may issue one demand, but come back and ask for a second demand if they believe they can justify it (i.e. the victim is asking for a large number of machines, the victim waited weeks to reach out, etc.)
- The extortionist may have little technical savvy and provide the incorrect decryption keys.
- The extortionist may abruptly stop communicating and fail to provide the keys after payment.

If the organization elects not to pay, risks include:

- Discovering that backups they thought were intact are in fact damaged, incomplete or out of date due to circumstances unrelated to the ransomware.
- Depending on how recent the backups are, restoration from backups will inevitably erase the logs and forensic evidence preserved from the moment of the attack. This will hinder the forensic investigation and possibly limit the incident response team's ability to disprove data access/data exfiltration.

It is often a more effective solution to retain independent forensics to engage in communication with the attacker on your behalf. Most organizations do not have the protocols or resources in place to ensure that the proper precautions to protect the organization's identity, and communicate effectively with the attacker to maximize the likelihood that, if the ransom is paid, the attackers will provide the necessary information for the organization to retrieve its data.

B. Preserving Forensic Evidence of the Attack

As difficult as it may be, it is very important to resist the urge to delete/wipe everything following an attack. If a user account is malicious, disable it but do not delete it. If a machine is compromised, disconnect from the network, shut it down, and set it aside. If you must wipe it in order to get operations back up and running, make a copy of it first. The ability to disprove data access/exfiltration in most cases rests entirely on the preservation of that data.

Failure to preserve a forensic image can have long-ranging legal consequences. In cases where an image is unavailable to determine whether data was exfiltrated, the most conservative legal course may be to notify any client whose personal information would have been available to the attacker based on indicia of access. In addition, many jurisdictions require notification to regulatory authorities in the event of consumer notification, which can lead to regulatory scrutiny of an organization's security posture, and enforcement actions if deficiencies are found. Preservation of an image

It is also important to retain records, hardware/software and logs following an incident for a couple of reasons. First, you want to learn from what happened so you can prevent it from happening again in the future. Second, this information may be evidence in a civil, criminal or regulatory proceeding in the future and you do not want to be subject to a spoliation claim that you did not preserve evidence.

C. Understand and Timely Comply with Legal Obligations

1. Consumer Notification

If regulated data has been acquired by the attacker, an organization may be required to notify its clients that their data has been exposed. All 50 U.S. states have enacted statutes that, generally speaking, require entities to notify consumers if the entity experiences a security breach that results in an unauthorized individual either gaining access to, or acquiring, specific kinds of "personal information," as defined by those statutes. Determining which state data breach notification statutes apply depends upon where any affected individuals currently reside. Therefore, if an entity suffers a breach and its affected customers currently reside in Pennsylvania, Virginia, Louisiana and Oklahoma, the entity must comply with the requirements of each state's statute.

Some states, such as Georgia and Massachusetts, include limited data sets in this definition, such as name and address in combination with: a Social Security number, a driver's license number, or a financial account number (including a debit or credit card number) with the means to access the account. Ga. Code § 10-1-911(6); Mass. Gen. Laws ch. 93H § 1.

Other states have broader definitions. Illinois, for example, also includes medical or health insurance information, as well as biometric data. 815 Ill. Comp. Stat. § 530/5. Maryland has one of the most expansive definitions of personal information, and includes the data sets above, as well as information such as taxpayer identification number, passport number or other number issued by the federal government, health insurance policy or subscriber identification number, and a user name or email address in combination with the means to access the account. Md. Code Ann. Com. Law § 14-3501(e).

The state statutes also prescribe a time by which consumers must be notified of the incident. Many statutes, including those enacted by Alabama, New York, Pennsylvania, Texas, require notification to be made as quickly, or as "expeditiously" as possible, or "without unreasonable delay," consistent with any measures necessary to determine the scope of the breach and restore the affected system's integrity. 2018 S.B. 318, Act No. 396; N.Y. Gen. Bus. Law § 899-aa; 73 Pa. C.S. § 2303; Tex. Bus. & Com. Code § 521.053.

Other states, however, have specific deadlines by which consumers must be notified. Florida requires that consumers be notified within 30 days of the incident's discovery; Vermont, no later than 45 days. Fl. Stat. § 50.171; 9 Vt. Stat. Ann. § 2435.

2. Regulatory Inquiries

There are a number of state regulatory agencies that take an active interest in investigating security incidents that affect consumers' personal information. The data breach notification statutes in numerous states, including California, Connecticut, Indiana, Vermont, Virginia and Washington, require an entity suffering a breach to notify the state attorney general's office in the event that a threshold number of state residents are affected by the incident. Cal. Civ. Code § 1798.82; Conn. Gen. Stat. § 36a-701b; Ind. Code Ann. § 24-4.9-3-1; 9 Vt. Stat. Ann. §§ 2430, 2435; Va. Code Ann. § 18.2-186.6; Wash. Rev. Code § 19.255.010.

Entities experiencing security incidents may have regulatory reporting obligations under federal law as well. Financial institutions may be required to notify various federal regulatory agencies of a security incident involving personal information. Additionally, the Federal Trade Commission (FTC) has jurisdiction to enforce privacy violations, including the authority to conduct investigations and require entities to submit investigatory reports under oath.

Given the number of state and federal entities with jurisdiction to investigate data security incidents, a security incident can result in intense regulatory scrutiny of an organization's privacy and security policies and practices, as well as its response to and remediation of the incident. It is therefore imperative that when faced with an incident, an organization strictly follow its incident response plan, comply with consumer notification statutes, and ensure that it has complied with any applicable information security standards.

D. Consider Third Party Obligations and Exposures

1. Data Breach Class Actions

Not every data breach results in a lawsuit; nonetheless, data security incidents are also accompanied by the ever-present specter of litigation, particularly in the form of class actions. Plaintiffs in data breach class actions have historically found it difficult to overcome two primary hurdles, as federal courts have been reluctant to find:

(1) that the most commonly alleged harm, increased risk of identity theft, confers standing to sue as required by Article III of the U.S. Constitution; and

(2) that plaintiffs sufficiently articulated allegations that defendants breached any duty or that the breach was the legal cause of harm.

Recently, however, courts have become less willing to grant defendants' motions to dismiss based on these arguments and have allowed actions to proceed to class certification. Not surprisingly, faced with the prospect of expending the necessary funds to defend these actions through the certification process and accompanying discovery, many defendants have opted to settle the plaintiffs' claims rather than see the legal arguments through.

Given the costs involved in defending these actions, and the negative publicity such litigation can generate, a key element of any incident response is to be cognizant of the litigation risks and ways to minimize these risks. Similar to avoidance of undue regulatory scrutiny, these measures include prompt and thorough investigation of the incident, timely notification to consumers and provision of appropriate remediation options, and proper messaging when communicating externally about the incident.

2. Subrogation

In the event that a data security incident is caused by the negligence of a third party vendor, your organization may be entitled to compensation based on the terms of the parties' contract or common law negligence. However, as mentioned above, your right to recover, or that of your carrier who has paid your costs under a cyber policy, may be impaired if your company did not know and exercise certain rights under the contract. For example, if your organization had the right to audit the information security posture of your vendor, and failed to do so, you may be found contributorily negligent for the breach, which, in some jurisdictions, bars you from any recovery.