BURR FORMAN LLP

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

Articles / Publications
06.22.2021

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

It is hard to find a news post without a story on a ransomware attack. The National Security Council has issued an open letter warning all businesses to be alert and prepared for ransomware attacks. Various industry groups have issued multiple alerts with tips specific to businesses in their field. Unfortunately, it often takes getting hit by a ransomware attack to accept the idea that all businesses are potential victims of ransomware attacks. If you have not yet taken action and developed your own plans for responding to a ransomware attack, here are some tips for getting through a ransomware attack without an existing plan.

There are a lot of different types of cyber-attacks from social engineering attacks, exploitation malware, insider attacks, and extortion, and confirming whether or not your systems were compromised is the first step in determining the appropriate response. When suspicious activity is detected on your computer systems, always start by verifying the attack. This article focuses on responding to ransomware attacks, but many of the steps apply in any cyber-attack. If your first indication of the ransomware attack is the encrypting of files, there will not be much verification required. Even without a customized incident response plan, knowing who to call first and knowing what to do, and what not to do, until those consultants are on board to assist can go a long way in mitigating the long-term impact of the attack.

TRIAGE

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

Internal Team

When you become aware your systems are encrypting or encrypted, the staff should take immediate steps to shut down and/or isolate the affected systems, networks, machines, and devices to prevent the encryption from spreading any further. While the IT team is involved in that effort, the internal incident response team should be assembled. The specific individuals that should be on the team vary between businesses based on how responsibilities are allocated, but people with these roles should be included. Security officers, compliance officers, or privacy officers, if they exist who have knowledge of the company's security measures and internal policies and procedures should be included. Whoever is responsible for your company's IT operations is a must-have for your response team, and that person may recommend including other key members of the team. In addition to those individuals, the company's internal legal team and appropriate members of the management team, including the individuals responsible for HR, accounting/finances, risk management, and operations should be included.

The internal incident response team should be contacted and assembled using telephone, text, or other communication channels that do not involve the use of the compromised systems, and this team should be prepared to set up independent email accounts (such as a Gmail account) to use for the duration of this incident. These independent email accounts should be utilized until the internal IT team or a forensic consultant declares the company email system to be clean and functioning properly.

External Team

The next step is to pull the external incident response members into the loop. Starting with the organization's external counsel allows the incident response team to discuss the incident and the required response actions in the context of meeting legal obligations and supports a claim of attorney-client privilege with respect to the discussions that are to come. While it is desirable to have legal counsel who is already familiar with your operations, if your usual counsel does not have experience with data breaches, you will want to rely on your counsel or your insurance carrier to help you identify appropriate legal counsel with ransomware incident response expertise. In fact, you may find that your cyber-insurance carrier requires you to use breach counsel from their approved panels unless you have negotiated otherwise.

Insurance

One of the first things you should do with your breach counsel is to review your insurance coverage to determine the type and scope of your coverage and any requirements for receiving the full benefit of your coverage. If you are not certain about the scope of coverage you have, you will want counsel to review your policies (cyber and others) to determine what your coverage includes and how it should apply to this incident. If your breach counsel has been selected and engaged by your insurer, you may want your own counsel to review the policies for this purpose. As part of the insurance review look to see:

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

- Do you have coverage for a ransom payment, and if so, what conditions must be met for the ransom to be covered? Is the ransom payment part of the overall coverage limit or is it a separate coverage limit?
- Do you have coverage for legal fees related to the investigation of the incident, recovery from the incident, and complying with notice obligations resulting from the incident?
- Do you have coverage for a forensic consultant?
- Do you have coverage for the cost of hardware needed to recover your systems?
- Do you have coverage for the cost of sending required notices and the cost of providing identity theft protection and credit monitoring where required or voluntary?
- Do you have coverage for the cost of a help desk to field questions?

Forensics

Your breach counsel should engage a forensic consultant to assist in the investigation and recovery efforts. Forensic consultants offer a variety of services, including investigations to identify the cause of the incident and extent of the damage, analysis of the compromised data if necessary, and recommendations on improvements to harden the system against future attacks. The forensic consultant should be engaged through your breach counsel in order to provide a basis for the consultant's report (if any) to be protected by the attorney-client privilege. When selecting a forensic consultant, look for someone skilled in responding to ransomware attacks as well as someone who has immediate availability to assist. To the extent having someone on-site at your facilities rather than working remotely is important, you should make sure that the forensic team includes on-site support in their cost proposals.

While we are touching on the topic of proposals from consultants, you will want to review cost and approach proposals from your vendors, but this is not the time to engage in protracted negotiations over the terms of these agreements. You want the costs to be reasonable for the service and the scope of the services bounded, but be reasonable with compromises on other terms of the agreement to get the investigation started as quickly as possible. When making those trade-offs, balance the costs of the services against the cost of your operations continuing to be off-line as well as the costs of claims that could arise from regulators' penalties or from claims asserted by the individuals whose data was compromised.

Record Keeping

With your team fully assembled, make sure someone is designated to keep a record of all your efforts, generating a timeline of your response to the incident. Such a timeline can be relevant for receiving your insurance coverage, responding to inquiries from regulators, and responding to lawsuits. Having one person designated to keep track of this timeline helps ensure a consistent tracking approach and avoids having to collect notes from a variety of people.

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

Non-Linear Activity

As you jump into the next phase of response efforts, it is important to remember that these activities rarely occur in a linear fashion. Be flexible and encourage your team to be flexible, responding to the demands of the incident as they arise and relying on your outside consultants to guide you through the process.

COMMUNICATIONS

Setting up a consistent cadence for team communications throughout the process is helpful for providing structure to the investigation and recovery effort. You may need to start out with multiple meetings each day and then reduce the frequency of the meetings or adjust the attendees for the meetings as the efforts progress. We recommend an agenda that addresses the following topics:

- Recovery efforts
- Investigation results
- Negotiations with threat actor, if any
- Insurance communications
- Communications with personnel
- Communications with suppliers, vendors, and customers
- Contractual requirements
- Notice obligations and timeline

CONTAINMENT

To the extent you have not yet contained the incident, containment should be the top priority. Make sure all affected systems, applications, devices, and data have been taken off-line, isolated, or shut down. While it is instinctive to move from containment to recovery as quickly as possible, remember that you need to investigate and understand the attack in order to meet your legal requirements. Try not to delete any logs, reimage any machines or computers, or reformat/reinitialize any devices until you have pulled any relevant logs or records or created images for use in the investigation. The forensic team can provide guidance about what needs to be saved to facilitate their investigation.

INVESTIGATION

If you have not already, find the ransomware demand. Before anyone accesses the formal demand from the attacker (threat actor), be sure that everyone is in agreement on whether or not to contact the threat actor and how to direct those conversations. Decisions on this front include not only whether or not you might consider paying a ransom, but also whether you want to talk to the threat actor at all.

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

Assessing your back-ups is also a necessary part of the investigation because having viable back-ups has a significant impact on whether and how you might negotiate with the threat actors.

The forensic provider will begin working with your internal IT resources to investigate the breach. Make sure that the scope of work includes the forensic consultant answering and reporting on the following information:

- When and how the breach was discovered by your team;
- When the breach occurred – attackers often access systems hours, days, or months prior to kicking-off an encryption process;
- The type of breach / type of ransomware;
- The method of intrusion / how the breach occurred;
- The devices, systems, files, etc. that were compromised – number and type; and
- Whether the data in the compromised devices, systems, and files included any personally identifiable information or protected health information of your employees, contractors, clients, customers or patients, or confidential information or trade secrets of your company or of your vendors or customers.

The forensic consultant should also be able to assist with a review of the compromised files to determine which individuals' information was compromised or must be considered compromised.

COMMUNICATIONS

With Personnel Regarding Operations

As the containment, recovery, and investigation begin, you will likely need to communicate with all of your personnel about work schedules. Transparency and honesty in these communications are important, but you should limit the communication to the facts that are known at the time. Early in the process company personnel may only need to know that there has been a cyber-attack and the company is working to restore its systems. A message such as "During the time restoration is underway, everyone is instructed to [not come in] [come in only if notified by their supervisor] [come in but not log on to the system] [other instruction]" may be sufficient. Assure your personnel that you will keep them informed, but avoid speculating about the expected outcome of the investigation or the impact on their personal data. In addition, to the extent it is consistent with your company culture and any agreements with your personnel, remind them of their confidentiality obligations to the company and that for the time being this is an internal matter.

Media

Because it is always possible that information can be leaked to the press by an employee, a customer, a vendor, or the threat actors, it is important to prepare a media hold statement to have on hand if needed. As with employee communications, be honest, stick to the known facts, and do not speculate. If possible,

work with a public relations consultant that has experience in cyber incident crisis management so that they can help guide you to an appropriate tone for such a message.

Law Enforcement

In the case of a business email compromise where funds have been misdirected, we recommend an IC3 complaint be filed immediately. In the case of ransomware attacks, the timing for notifying the FBI can be more discretionary, but it is helpful to keep in mind that the FBI may have information that can be helpful in negotiating a ransom, knowing what to expect from your particular threat actor, identifying indicators of compromise, potential pot-holes in the recovery process, etc., and for that reason, we usually recommend involving law enforcement earlier rather than later. Your breach counsel and/or your forensic provider can provide contacts for notifying law enforcement that would be above and beyond filing the basic IC3 complaint.

With the Threat Actor

Somewhere in the investigation process, you will need to decide whether or not to contact the attackers and find out what the ransom demand is. Officially the FBI and United States governments do not recommend paying ransoms, but in practice, many victims find that the financial cost-benefit analysis leads them to determine paying the ransom is in the best interest of the business. With certain exceptions, see below, it is not illegal to pay a ransom, but you should thoroughly vet that option with your response team and particularly with your breach counsel to ensure you have considered all the pros and cons to such action.

To negotiate with the threat actor, the first step is to access the communication channel provided in the ransom note and find out what the initial ransom demand is and what the corresponding threat is. In most recent cases, the ransom demand is for a decryption key to help restore your systems as well as a promise not to publish, release, sell or trade your information to other parties. The release of data can be a powerful threat when the compromised data includes personally identifiable information or protected health information or key corporate secrets.

If you decide to contact the threat actor, consider whether to have someone on your team make contact, whether to have your forensic consultant make contact, or whether to engage a third-party consultant to make contact on your behalf. Most, but not all, forensic teams have a negotiator on staff to help with this process, but if you are facing a particularly large ransom or particularly sensitive data being compromised, you might prefer to engage someone whose entire business is to negotiate with threat actors and facilitate payments in cryptocurrency. These organizations sometimes receive criticism for facilitating criminal activity, but they can also offer an extra layer of assurance during the process because of their experience with these types of negotiations and the crypto-currency payment.

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

Vendors / Customers

While the investigation and threat actor negotiations are ongoing you will need to assess the status of your obligations to your vendors/suppliers and to your customers. You may find that you need to give notice to some of these vendors, suppliers, and customers because you will be unable to meet your contractual obligations to them due to the business interruption (e.g., force majeure or other potentially applicable notices). Also, you may be required by your contract to notify the vendor or customer of a data breach regardless of the information that is compromised. In particular, if you contract with any government organizations, you will need to comply with your data breach reporting requirements. To the extent any of your vendors, suppliers, or customers are individuals, you may also have obligations to notify them regarding exposure of their personally identifiable information.

One key hurdle in determining your contractual requirements for purposes of force majeure notices or breach notifications is that your contracts are often stored electronically on your system and have been encrypted by the ransomware. Maintaining either the contracts or a summary of the key provisions of these contracts in paper form or in separate, secure backup files can be extremely helpful in this circumstance.

PAYING THE RANSOM

If you decide to pay a ransom, you must make sure that the payment is not in violation of the Office of Foreign Asset Control (OFAC) regulations. On October 1, 2020, OFAC issued an advisory confirming that payment of a ransom to a threat actor known to be involved with an organization that threatens United States national security is a violation of the OFAC regulations and subject to penalties thereunder. In order to better implement that regulation, OFAC has added certain threat actor groups, IP addresses, and crypto-currency wallets to their Specially Designated Nations and Blocked Persons List. Individuals and organizations in the United States are prohibited from doing any business with the organizations, individuals, IP addresses, and crypto-currency wallets appearing on that list. Both the party initiating the payment and the party facilitating the transaction (Money Services Business) have liability under those regulations and the penalties can be both civil and criminal.

In order to avoid OFAC penalties when paying a ransom, you will want to obtain an OFAC clearance letter. Because the Money Services Business you use to purchase and transfer the crypto-currency also bears liability for improper transfers, these groups usually perform the OFAC clearance search for you, but you should make certain that the clearance is done and that you retain a copy of the clearance letter.

PRIVACY NOTICES

In most cases, one of the last steps you will take is determining your notice obligations. In the United States that requires analyzing a variety of overlapping state and federal laws and industry regulations and depending on the data you collect and process, international laws. Your breach counsel should walk you through that analysis to make sure you notify everyone who is entitled to receive a notice of this attack,

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

keeping in mind that in most cases, ransomware attacks qualify as breaches unless you can demonstrate that data was not extracted and/or that there is a low risk of harm to the individuals whose information was encrypted as a result of the attack.

The state and federal reporting requirements include the requirement to provide notices to the individuals whose data was compromised as a result of the attack. In addition, depending on the number of individuals impacted in a given state or a given incident, you may also have obligations to report to various state agencies, regulators, and credit reporting agencies. If the scope of the breach is particularly significant or if you do not have contact information for all of those individuals, you may be able to (or required to) use substitute notice to ensure most people receive notice of the breach.

The various breach notification requirements specify not only who has to be notified, but the time frame in which you must provide those notices, the content of the notices, and in some cases include other requirements. In addition, certain states require that you purchase identity theft monitoring and/or credit monitoring services for individuals whose social security number or other financial information has been compromised. Still, other requirements include the obligation to provide a call-in number to answer questions about the breach.

Report/Documentation

As you wrap up your investigation and recovery efforts, you should consider the possible benefit of a written report on the incident. Certain state and federal requirements include final reports on an incident that is maintained for at least five years, and in some cases longer. If a report is not required, there may be reasons to not prepare such a report and simply to work from verbal recommendations for improving your systems. If you do prepare a report, it should be prepared with the involvement of your legal counsel. The report should be accurate and truthful, but in some cases, the facts could be less than flattering to your organization, in which case unless you are required to do so, you might choose to forgo a formal report. If you do pursue a report, some of the topics to consider include the timeline/summary of events that has been maintained throughout the incident, the findings of the forensic group, any communications with law enforcement, a summary of the notices that were sent and any responses received, details on any credit monitoring or identity theft monitoring services that were purchased/provided, and any other information that you or your legal counsel determine may be needed in the future.

Improvement – Looking Forward

In conjunction with preparing that final report, take a good look at where your systems are now, what improvements have been made as a result of the incident, and what recommendations you received from the forensic team, your breach counsel, and other consultants during this process. It is usually not possible to tackle all of these recommendations at once, but this is a good time to prioritize the recommendations that you want to adopt and assign time frames to the items that you plan to implement.

Your Business Experienced a Ransomware Attack, and It Was Not Prepared – Now What?

CONCLUSION

Cyber-attacks are one of the few areas where laws impose affirmative obligations on victims of the crime. As the business victim of a ransomware attack, you automatically incur the responsibility to take action to restore and harden your systems and to notify all parties who have a potential interest in the outcome of the data breach. So if you find yourself in the position of responding to a ransomware attack and you have unfortunately delayed preparation of your own plans and procedures, reach out to and rely on your experts. Trying to work your way through an attack of this type without advance planning or the expertise needed to effectively and adequately work through a ransomware incident can cost your business not only in operational downtime of operations but also in increased chances of having to pay a ransom and of incurring penalties for missing your data breach notification deadlines or other compliance requirements as set out in applicable notification laws.