Responding to Ransomware Attacks

By Peter T. Berk, Funkhouser Vegosen Liebman & Dunn

1. Task Overview and Checklist

1.A. Task Overview

This Smart Task is designed for the practitioner who has been tasked with developing a plan to respond to, and prevent, ransomware attacks. Such attacks are an increasing problem for ecompanies worldwide. Since early 2020, ransomware attacks have increased in number, sophistication, and cost. Increasingly, threat actors are infiltrating a company's network weeks, or even months, before deploying malware to conduct reconnaissance of the environment, identify vulnerable hardware and data, and gather information about the company. Threat actors are also now exfiltrating company data and then threatening to release it, including by posting it on their "shame" sites and/or the dark web, to further pressure companies to pay the demanded ransom.

In anticipation of a potential attack, organizations should develop specific policies and procedures to respond to such an attack. These policies and procedures should be reviewed regularly (i) in coordination with the organization's Incident Response Plan (IRP), which should address broader aspects of incident response and potential legal reporting requirements, as well as (ii) in light of advancements in technology, organizational changes, risk assessments, and other relevant facts.

1.B. Master Checklist

1. Relevant laws
    a. In general
    b. OFAC
    c. FinCEN
    d. Computer Fraud and Abuse Act
    e. 18 USC Sec. 2339B
    f. Trading with the Enemy Act and International Emergency Economic Powers Act
    g. Foreign Corrupt Practices Act
    h. Other considerations

2. Implement processes to protect against ransomware attacks

    a. Use antivirus software at all times
    b. Consider keeping backups offline
    c. Reduce the attack surface
    d. Keep all computers patched with security updates
    e. Use security products that block access to known ransomware sites
    f. Configure systems and software to allow only authorized applications
    g. Enforce controls
    h. Implement and endpoint security policy
    i. Introduce as blocker/script blockers to employee browsers
    j. Develop a disaster recovery/business continuity plan
    k. Provide security awareness training to employees
    l. Restrict file access to \"need to know\"
    m. Only do business with vetted and proven vendors
    n. Evaluate ransomware detection technology

3. Responding to an identified ransomware attack

    a. Engage incident response team and plan
    b. Stop the threat
    c. Identify impact of the attack
    d. Evaluate the attack
    e. Retain counsel
    f. Consult forensic investigator
    g. Use prior backup data
    h. Review cyber insurance policy
    i. Negotiate ransomware payment
    j. Conduct due diligence on threat actor
    k. OFAC review
    l. Notify law enforcement
    m. Obtain necessary approvals for payment

n. Decrypt the organization's information
o. Validate threat removal

4. Conducing a ransomware attack post mortem analysis

a. Conduct post mortem and take corrective action
b. Erase ransomware from company systems
c. Audit vulnerability results
d. Implement regular organizational training
e. Be vigilant

2. Relevant laws

2.A. In general

The U.S. government's official position already strongly discourages the payment of data ransoms. Numerous federal statutes already criminalize making a variety of payments that are similar to ransomware payments.

2.B. OFAC

The Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an updated advisory in September 2021 to "highlight the sanctions risks associated with ransomware payments related to malicious cyber-enable activities." The OFAC advisory noted the increase in ransomware demands increased during COVID-19. The advisory warned that the facilitators of such payments on behalf of the victims—like financial institutions, cyber insurance firms and other companies involved in incident response and digital forensics—may be (i) encouraging more ransomware attacks, and (ii) risking violation of OFAC regulations. Specifically, U.S. individuals who engage in transactions with people or entities listed on the Specially Designated Nationals and Blocked Persons (SDN) List can be held strictly liable for civil penalties for violating this prohibition – even if, as the advisory warns, they did not know the transaction was prohibited. If the payment is made knowing that the transaction is improper, criminal penalties may also be available. The advisory also notes that organizations can reduce the risk, or mitigate the amount, of any sanctions by implementing and improving its cybersecurity practices (especially those highlighted by the Cybersecurity and Infrastructure Security Agency's guide), and by reporting the attack and any potential payments.

2.C. FinCEN

The Department of Treasury Financial Crimes Enforcement Network (FinCEN) issued an updated advisory in November 2021, to financial institutions on types of ransomware attacks and payments, red flags indicating a potential ransomware payment, and regulatory obligations that may be triggered by handling, processing and facilitating ransomware payments. The FinCEN advisory cautioned that such activities, which typically require an institution to receive and transfer or convert funds, could constitute money transmission and impose additional obligations and mandates under the regulations.

2.D. Computer Fraud and Abuse Act

Computer Fraud and Abuse Act--18 U.S. Code Sec. 1030 (Fraud and related activity in connection with computers): U.S. law already prohibits “demands” for coercive payments such as extortion, ransom and bribery. The Computer Fraud and Abuse Act extends this general prohibition to the digital space by criminalizing payments stemming from threats to damage a government or bank computer, or a computer used in, or affecting, interstate or foreign commerce. This statute allows criminal prosecution of those that commit ransomware attacks, and, through aiding and abetting liability, those who assist in creating the ransomware and others that assist the attackers.

2.E. 18 USC Sec. 2339B

18 U.S. Code Sec. 2339B (Providing material support or resources to designated foreign terrorist organizations): Congress has also criminalized other payments to overseas entities to combat various widespread threats, making it a crime for individuals to make certain types of payment even if they did not seek or receive any benefit. Section 2339(B) makes it a crime for a person to provide material support or resources to a designated foreign terrorist organization.

2.F. Trading with the Enemy Act and International Emergency Economic Powers Act

Trading with the Enemy Act (“TWEA”) and the International Emergency Economic Powers Act (“IEEPA”) are key pillars of the United States’ modern economic sanctions program. While the TWEA’s current use is tied to wartime, the IEEPA grants the president broad powers to address an extraordinary threat to U.S. national security, foreign policy or economy that originates, fully or in substantial part, from outside of the United States. The president must first declare a national emergency relating to the threat.

2.G. Foreign Corrupt Practices Act

Foreign Corrupt Practices Act (FCPA): This statute was enacted in 1977 to combat the widespread problem of U.S. companies making corrupt payments to foreign officials. 15 U.S. Code § 78dd-1 prohibits covered entities from making any corrupt payment, or giving anything of value, to a foreign official in exchange for obtaining or retaining business in that country. The FCPA defines corrupt payments as any offer, promise, authorization of payment, or payment made with an intent or desire to "induce the recipient to misuse his official position." A thing of value broadly includes any improper or unfair benefit given to a foreign official. The payer's wrongful influence can be evidenced by a foreign official violating a duty through an act or omission that secures an improper advantage or influences an official act or decision. The party does not need to be successful in its payment to an official—the recipient does not need to solicit, accept or receive the payment—for there to be a violation. Nor does the party need to know the identity of the recipient to violate the FCPA so long as the payment is made "corruptly"—giving anything of value with an intent to wrongfully influence the recipient. The effect of the FCPA's broad language is that conduct both in and outside the United States can be subject to enforcement, meaning that an individual can be found liable for making a specific payment to any general foreign party or official.

2.H. Other considerations

The takeaway from the discussion of the laws outlined above is that most of these laws, like the FCPA, will not apply in the common ransomware scenario because the offending party often has only a tenuous connection to a government official or jurisdiction. Even if it does, a prosecutor would have to prove that the payer knew this, which is equally improbable.

Finally, while the focus of the laws identified in this SmartTask relate to payments, many, if not all, states have adopted state information security requirements and/or breach notification laws. The definitions of events that require notification to state attorneys general or individuals can include situations in which a company's system has been compromised by ransomware. Additionally, a successful ransomware attack may indicate a vulnerability in the organization's system requiring notice under certain legal frameworks. Please consult the SmartTask on incident handling for assistance in this regard.

3. Implement processes to protect against ransomware attacks

3.A. Use antivirus software at all times

An organization should ensure that it has a reputable antivirus software operating effectively, and set-up to scan emails, removable media, etc., to help protect against ransomware and other malware improperly or inadvertently obtaining access to your network.

3.B. Consider keeping backups online

Ransomware is designed to seek out connections between the hardware it has infected and other devices, peripherals, servers, and any other item that is connected. This includes any on-line, connected repository of back-ups of your system. If the ransomware has infected a back-up and the organization utilizes that back-up to restore its system after the attack, the organization will have effectively re-infected itself. And if the ransomware is triggered and has infected the system back-ups, those back-ups will also be locked and will not be a tool the organization can use to restore its system – making it more difficult to quickly recover from the attack without paying the demanded ransom.

3.C. Reduce the attack surface

Gain full visibility and block unknown traffic coming into and on your network. Many tools are on the market to assist with traffic monitoring. An organization with significant internal traffic is well-advised to retain one of these offerings and train a team dedicated to tracking it.

3.D. Keep all computers patched with security updates

Patches are software and operating system updates that address security vulnerabilities within a program or product. IT staff should regularly monitor (or have automated systems that monitor) third party software and hardware vendors for patches and updates.

3.E. Use security products that block access to known ransomware sites

Website blockers come standard in most web browsers. Phishing and malware detection is turned on by default and may prompt messages like this:

a. The site ahead contains malware: The site you start to visit might try to install bad software, called malware, on your computer.
b. Deceptive site ahead: The site you try to visit might be a phishing site.
c. Suspicious site: The site you want to visit seems suspicious and may not be safe.
d. The site ahead contains harmful programs: The site you start to visit might try to trick you into installing programs that cause problems when you are browsing online.
e. This page is trying to load scripts from unauthenticated sources: The site you are trying to visit is not secure.

3.F. Configure systems and software to allow only authorized applications

Practice Tip - It is good practice for an organization to maintain a list of whitelisted and blacklisted programs and applications for internal use, but it does require a certain level of administration assistance. Specifically, an administrator will have to be tasked with identifying the whitelisted applications available for use on individual employee systems. The administrator will do this by first assessing applications required by the employee base and then ensuring with IT partners that each meets the organizational standards for being whitelisted. This whitelisted list will need to be maintained and updated over time.

3.G. Enforce controls

A good place to start for organizations seeking to enforce database, application and user level controls is to leverage Multi-Factor Authentication (MFA) for access to individual computers, email, and the network where possible.

3.H. Implement an endpoint security policy

Organizations should implement an endpoint security policy that prevents noncompliant endpoints from connecting to network. In practice, a good first step is to restrict or prohibit the use of personally owned devices on your organization’s networks and for telework or remote access unless the employee takes extra steps to ensure security (e.g., multi-factor authentication, IT approved hardware and software security on the device, etc.).

3.I. Introduce ad blocker/script blockers to employee browsers

Ad blockers can work in multiple ways. The first way is where the ad blocker blocks the signal from an advertiser’s server, so the ad never shows up on your page. Another way ad blockers work is by blocking out sections of a website that could be ads. Having these ad blockers installed and active helps avoid employees inadvertently clicking on ads that could be malware.

3.J. Develop a disaster recovery/business continuity plan

Suggested components to a disaster recovery/business continuity plan include:

- Identify the scope of the plan.
- Identify key business areas.

- Identify key personnel and stakeholders.
- Identify critical functions.
- Identify dependencies between various business areas and functions.
- Determine acceptable downtime for each critical function.
- Create a plan to maintain operations in the event of a disaster including the following elements:
    - Shut down all non-essential networks immediately to prevent spread.
    - Shut down online connectivity to the network (e.g., WiFi and Bluetooth)
    - Notify key personnel and coordinate with appropriate outside professionals (lawyers, insurer, etc.); and
    - Alert local authorities and the FBI

3.K. Provide security awareness training to employees

Training should be provided to all employees, when they are hired and on a regular basis afterwards. Training should give employees the proper tools to use and people to contact when they suspect a possible attack. Employees should also be trained how to spot suspicious emails, websites, and other telltale signs of a potential intrusion. An organization may also want to consider, as part of the training: (i) conducting test runs in which individual employees are asked to identify suspicious behavior on their systems (or otherwise) and to respond to that behavior in accordance with the training; and (ii) hiring an outside vendor to test employees by randomly sending fake phishing emails to determine whether additional training is needed.

3.L. Restrict file access to "need to know"

An employee’s access to specific systems, programs, data and other network resources should be limited to that which is necessary for their duties. Access controls should focus on what the employee needs to do their job for the organization rather than simply on job title.

Practice Tip – There are a number of third party software programs on the market today to assist organizations with access permissions, credentialing, and tracking/monitoring at the file, database, and system level. An organization that is building out its technology and related security should consider appropriate products to assist in access control.

3.N. Only do business with vetted and proven vendors

Organizations should assess and evaluate vendors for their security controls, and track those controls in the organization's internal vendor assessment repository.

Important Note – An organization should monitor vendors' security status and controls so that any patches, known fixes, or changes are tracked and can be referenced in the event that the third party vendor is involved in the attack. This will be important information relevant to the investigation, and, when time is of the essence, it will be helpful to have this information to refer to in an easily accessible repository.

3.O. Evaluate ransomware detection technology

As with any software, an organization should routinely assess whether its security software is properly mitigating risk – including that of ransomware – for the organization. Each organization is unique, and each experiences unique types of possible ransomware threats. An organization should ensure its software technologies are responsive to their particular demands.

---

4. Responding to an identified ransomware attack

4.A. Engage incident response team and plan

Upon identifying a ransomware threat, the organization should engage its incident response team (IRT) and incident response plan (IRP) immediately.

Practitioner's Tip – It is important for an organization to work with its internal and/or external legal counsel to have a good understanding when, whether, and how investigations can be protected under the attorney-client privilege. There are necessary steps and practices to ensure the protection that may need to begin immediately upon identifying the attack. Courts are becoming more stringent in their analysis of whether attack investigations and remediation steps are privileged, so anything an organization can do to increase the possibility of protection can be beneficial.

4.B. Stop the threat

Care should be taken by the organization's Information Security (IS) team, or external ransomware/cyber-attack response vendor to cut off the threat by disconnecting affected systems from the network; systems should not be restarted or rebooted, as doing so could cause the loss of key forensic evidence or indicators of compromise.

Practitioner's Tip – An organization's incident response plan (IRP) should identify outside vendors to assist with the response to, forensic examination of systems impacted by, and remediation after a ransomware attack. Utilizing the organization's own internal IT or IS personnel can be risky because: (i) such personnel are not commonly called on to testify, which can be necessary if litigation arises; (ii) such personnel can have a personal stake or bias in favor of protecting themselves and finding others to blame; and (iii) having them focus on the attack can take them away from other important jobs to keep the organization's business running.

4.C. Identify impact of the attack

The IRT, in tandem with the IS team, should identify the scope of the affected systems and whether it is possible to restore from back-ups. Often, the threat actor will try to encrypt or disable back-ups.

4.D. Evaluate the attack

If restoration from back-ups is not possible, the IRT should evaluate risks associated with engaging the threat actor.

4.E. Retain counsel

The IRT should retain outside legal counsel experienced in data breach response. Legal counsel will advise on legal obligations, including statutory and contractual obligations, related to the incident.

4.F. Consult forensic investigator

The IRT should engage a forensic investigator from the list of approved forensic investigators. Having legal counsel formally retain the forensic investigator can increase the chance that the attorney-client privilege and work product doctrines will apply to the investigation and communications related thereto, which is important given that, as noted above, courts are limiting these protections.

Practitioner's Tip – Many forensic investigation companies that are experienced in ransomware and breach response have libraries of decryption keys from known ransomware. Thus, the forensic investigator may be able to assist in decrypting the files without utilizing the back-ups or, as noted below, paying ransom. The investigator will still need to check and clear all of the potentially impacted systems, devices, peripherals, etc. to ensure that the ransomware is fully removed from the system, lest it re-infect the system and re-lock all of the files again at a later date.

4.G. Use prior backup data

Using prior data backups can reduce the severity of an attack's impact on the business. Backups can be a ready source of company information to get the business back up and running as soon as possible. Daily data backup procedures should include processes to store data off-site, without any connections to the organization's IT systems (for the reasons noted above). The organization, however, should carefully consider how long it retains these backups. For additional information on data retention, see the Smart Task on Establishing a Data Retention and Disposal Framework.

4.H. Review cyber insurance policy

If the organization has a cyber-insurance policy, the policy should be reviewed to determine what is covered, what notice may be required to the insurer, whether certain vendors are required to be used, and other requirements necessary to ensure coverage.

Practitioner's Tip – It is usually worthwhile to also review an organization's other – i.e. non cyber-insurance – policies. Other policies (including Commercial General Liability, Umbrella, Property Damage, etc.) can sometimes provide additional or other avenues for coverage depending on their terms.

Important Note – An organization should consult the SmartTask on Evaluating Cyber Liability Insurance to determine cybersecurity coverage limits.

4.J. Negotiate ransomware payment

If the organization decides – after consultation with legal counsel, any involved insurer, the IRT, the forensic investigator, and relevant organization stakeholders – to communicate with the threat actor, the IRT should engage a third-party ransom negotiator in coordination with legal counsel. Such third parties will be experienced in negotiating with threat actors and will have a crypto-currency (e.g., bitcoin) wallet available to utilize for the payment.

4.K. Conduct due diligence on threat actor

Prior to making any payment, the organization should conduct due diligence concerning the threat actor. Although it will not always be possible to identify the threat actor, payment to certain nation-state actors or criminal organizations may violate the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) sanctions list, as explained above in the background on law section.

Important Note - OFAC has designated numerous malicious cyber threat actors under its cyber-related sanctions program, including perpetrators of ransomware attacks. An organization that materially assists, sponsors, or provides financial, material, or technological support for sanctioned activities may itself be subject to sanctions, even if the organization did not know or have reason to know it was engaging in a transaction with an OFAC-sanctioned person or entity.

4.L. OFAC review

If the organization has decided to make a payment, the ransom negotiator should have processes and procedures in place to determine if the suspected threat actor is subject to OFAC sanctions. The IRT, however, should ensure that the negotiator has followed its procedures. To do so, the IRT should request that the ransom negotiator confirm in writing that it conducted an OFAC check and it had no information that the threat actor was subject to OFAC sanctions.

4.M. Notify law enforcement

Prior to making any ransom payment, the IRT should ensure that appropriate law enforcement is notified. This can be done either by contacting the FBI or Secret Service directly, submitting an online FBI report on https://www.ic3.gov/ or submitting a report to the Cybersecurity & Infrastructure Security Agency on its reporting system. The recent OFAC guidance also suggests reporting the incident to OFAC and the Treasury's Office of Cybersecurity and Critical infrastructure Protection if there is a risk that the actor is on the sanctions list.

4.N. Obtain necessary approvals for payment

If the ransom negotiator confirms that the threat actor is on the OFAC sanctions list, the ransom cannot be paid without risk of sanctions unless the such payment has been discussed with and approved/licensed by:

> U.S. Department of Treasury's Office of Foreign Assets Control
> Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov
> (202) 622-2490 / (800) 540-6322
> Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480

The organization should also ensure that there are no other prohibitions on payment, and obtain any other necessary approvals.

4.O. Decrypt the organization's information

Once the decryption keys have been recovered (or obtained through the forensic investigator or another source), the IRT should work with the forensic investigator to ensure that, prior to decrypting the data, there is no ongoing threat to the organization from the attack.

4.P. Validate threat removal

Once data is restored, the IRT, in conjunction with the forensic investigator should follow the IRP concerning investigation into the scope of the attack, including whether the threat actor has accessed or acquired any sensitive data.

5. Conducting a ransomware attack post mortem analysis

5.A. Conduct post mortem and take corrective action

Organizations that are subject to a ransomware attack should conduct a postmortem on why and how it happened and take corrective action to prevent and detect future attacks more effectively. This assessment entails understanding how the attacker obtained the access needed to enable encryption and lock down company data. To that end, endpoint detection and response solutions that continuously monitor all incoming and outgoing traffic on a network for potential threats can provide transparency and information as to where the attack started and how it progressed. The business can use this insight to help prevent similar incidents from happening again.

Important Note – An organization should consider consulting a third party investigation firm, or even the forensic investigator used to investigate the incident, to conduct this post-mortem analysis. Their expertise may assist the organization in adequately identifying and documenting the manner in which the attack occurred which will help assist the organization in taking remedial measures to assist in preventing future attacks.

5.B. Erase ransomware from company systems

Erasing ransomware from company systems is a priority in the aftermath of an attack. This task can be very difficult to accomplish with confidence if the criminals do not provide the keys to decrypt the infected files. Even if they do, management will still need to be confident the system, devices and files are fully cleansed, preferably without clearing all files and storage devices and starting anew. The organization should review this issue with its legal counsel and the forensic investigator or other firm hired to assist in remediation.

5.C. Audit vulnerability results

Review the organizational policies and procedures for (i) security audits to identify vulnerabilities as they emerge, and (ii) performing maintenance tasks such as software updating and patching immediately to mitigate risk, and update them as needed based on the postmortem.

5.D. Implement regular organizational training

Organizations should implement regular organizational education to minimize the likelihood that endpoint users will fall victim to social engineering tactics in the future as well as to ensure they have a firm grasp on company security protocols in light of the attack that has occurred.

5.E. Be vigilant

Once an organization’s systems have been successfully compromised, threat actors are likely to increase their efforts to compromise the same organization again, at least in the near term. Once the current threat has been eradicated, the organization must remain especially vigilant against a potentially increased number of attacks.