Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Ransomware Active Attack Response Best Common Practices

May 2023

The reference URL for this document is https://www.m3aawg.org/ransomware_bcp_2023

Table of Contents

Table of Figures

Terms, Definitions, Abbreviations and Acronyms

This document uses the following abbreviations.

ARRA	American Recovery and Reinvestment Act of 2009 (USA)
BC/DR	Business Continuity and Disaster Recovery
C&C	Command and Control
CCPA	California Consumer Privacy Act
CISA	Cybersecurity Infrastructure Security Agency (Division of DHS, USA)
CISO, CxO, etc.	See Section 2.6, "People"
COPPA	Child Online Privacy Protection Act (USA)
CPRA	California Privacy Rights Act
DFIR	Digital Forensics and Incident Response
DHS	Department of Homeland Security (USA)
FBI	Federal Bureau of Investigation (USA)
GDPR	General Data Protection Regulation (EU)
HIPAA	Health Insurance Portability and Accountability Act (USA)
IAM	Identity Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MAC Address	Media Access Control Address (quasi-unique device identifier)
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
SOC	Security Operations Center
TCPA	Telephone Consumer Protection Act (USA)

1. Scope

1.1 Introduction and Overview

Ransomware is a form of malicious software loaded by attackers onto a platform, such as your computer, an enterprise server, data storage arrays, filesystems, or other points of vulnerability. The ransomware restricts access to resources such as files, services, backups, logs, databases, and other tools, with the intention of extracting payment from the owners who depend on those resources.[1] Restricting access often involves the encryption of files, but can also involve exfiltration (stealing the files), deletion, or defacement (altering the original data), depending upon the motives of the malicious actors. Attackers will often provide payment instructions at the site of the attack in the form of notes on desktops, printed pages, or updated wallpaper. They may also reach out through other means. The promise is simple: pay the ransom, and they will provide the key and restore the system functionality. The reality is unfortunately more complicated.

Ransomware has become an increasingly common practice with low barriers to entry for malicious actors.[2] Victims struggle to understand how or why they find themselves in this situation. For the malicious actors, however, it's often merely a numbers[3] and economics[4] game, and the victims are simply unfortunate enough to have had a vulnerability exploited. Sometimes, the malicious actors are more interested in exfiltration, corporate espionage, or service disruption.[5] At other times they will follow through on paid ransoms and deliver the decryption key.[6,7] In some cases, victims have certain obligations (reporting, non-payment, involvement of law enforcement) based on the jurisdiction they reside in, or based on what data may have been compromised; healthcare data in the United States, for example, may be protected by statutory reporting requirements if the compromised victim is a Covered Entity or a Business Associate.

1.2 Purpose of Document

This document addresses the options available if you realize that you are a victim. It explains how to consider risks and alternatives in resolving the recovery and supporting continuity for your business, and how to tackle those issues.

The target audience for this document is the team responsible for the information technology within the organization, particularly the CISOs (Chief Information Security Officers) and CPOs (Chief Privacy Officers) of small and mid-sized enterprises. Most recommendations will also apply to larger companies, although larger companies may have other organizational structures. Critical players in the recovery from a ransomware event can be found in section 2.6, "People."

The objective of this document is to offer a simplified path through all the stages of the ransomware recovery. The document helps explore options available at each stage and offers insight on which parties to engage at each step, such as law enforcement, enterprise executive leadership, insurance, legal teams, or others. It will also discuss useful tools, recovery options, likelihood of decryption, notifications, regulatory compliance, and more. The objective is NOT to provide a single path that is a one-size-fits-all approach to

---

[1] https://www.cisecurity.org/insights/spotlight/election-security-spotlight-ransomware-attacks
[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
[3] In the EU, €10,1 billion is estimated to have been paid in ransoms during 2019, up €3.3, a 365% increase in detections in businesses in 2019; 66% of healthcare organizations experienced a ransomware attack in 2019. See https://www.enisa.europa.eu/publications/ransomware.
[4] Sophos, "Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year." Sophos, 27 April 2021, https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.
[5] https://www.cisa.gov/stopransomware/ransomware-reference-materials-students
[6] https://www.nomoreransom.org/
[7] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

dealing with ransomware, nor is it to tell you how to resolve each decision point. Those will be unique to your organization and situational context.

If you suspect that ransomware may have just moved from the more theoretical area of news happening to other people into the realm of the real, the applicable, and the urgent, proceed to the following section, "First Awareness of Ransomware Victimization." This section aims to help those who have recently experienced, or are currently experiencing, an attack. It provides a guide for the types of decisions that need to be made during the course of an ongoing attack and addresses how to consider aspects of decisions where there will be pressure to act quickly.

If you are looking for help in **preparing in advance against ransomware threats** or **how to conclude the closure steps after recovery**, external resources are available; these can be found in section 2.8, "Post Incident."

2. First Awareness of Ransomware Victimization

Step Advice

Read through this entire document first.

Even though you may think you don't have time, it's important to look ahead and to understand all the steps that may be involved. Your situation is unique. It may not follow the sequence laid out here. Some activities will happen out of order, people may be unavailable, some decisions may not be needed, others will be forced ahead of when you'd like to make them, some decisions not listed here may need to be considered. **Keep notes on everything, starting now.**

2.1 Runbook

There are several subsequent phases to how to respond to ransomware. Read this one first and treat it like a checklist. You will see some roles identified for each step. Details on these roles and their potential availability can be found below in section 2.6.1, "Internal Resources," and section 2.6.2, "External Resources and Services."

Step Advice Find a new notebook, create a notes space within your notes app, or dedicate space specifically for research and documentation during this activity. If you haven't yet created a physical offline copy of this document, this is a good time to create such a reference.

Step Advice **DO NOT TURN OFF MACHINES SUSPECTED OF COMPROMISE**.
Avoid the intuitive response of simply turning off equipment suspected of compromise. More further on.

Step Advice ***DO* DISCONNECT COMPROMISED MACHINES FROM THE NETWORK. If they are using an ethernet cable, simply remove that cable.** Direct network connectivity to known compromised machines should be severed.

Step Advice It's possible that infected machines are connected over Wi-Fi, maybe even over multiple access points or extenders. At this stage, you may not know which machines are infected and which are not. The intuitive step would be to turn off Wi-Fi routers or to create a new SSID/password. **Do not do this.** Doing so may disable mission-critical, safety-critical, or security-critical devices connected to your system (e.g. DNS, insulin pumps, or corporate alarm systems, respectively). **Consider instead network segmentation, quarantining devices, or turning on MAC address filtering to use allow lists and block lists as a tool**

for network attachment management. Look for each external access into your network, systems with cellular connectivity, redundant routers for multiple modes of connectivity, etc.

Step Advice Isolate and/or inspect the corporate authentication and authorization system (e.g. Active Directory). These are often the initial target of infiltration and can be the way back into the network after or during recovery.

Step Advice Prioritize protecting any backup systems or access to those systems. This will be critical to the subsequent efforts; you are looking to isolate and then confirm the integrity of the backups.

Decision Point One of the very first real decisions you will need to make now is if and when to bring in help from your insurance company. Take a look at section 2.5.1, "Engaging the Cybersecurity Insurance Policy and Incident Response Team."

Step Advice This is only the initial stage of the process. Pace yourself and don't try to hurry this.

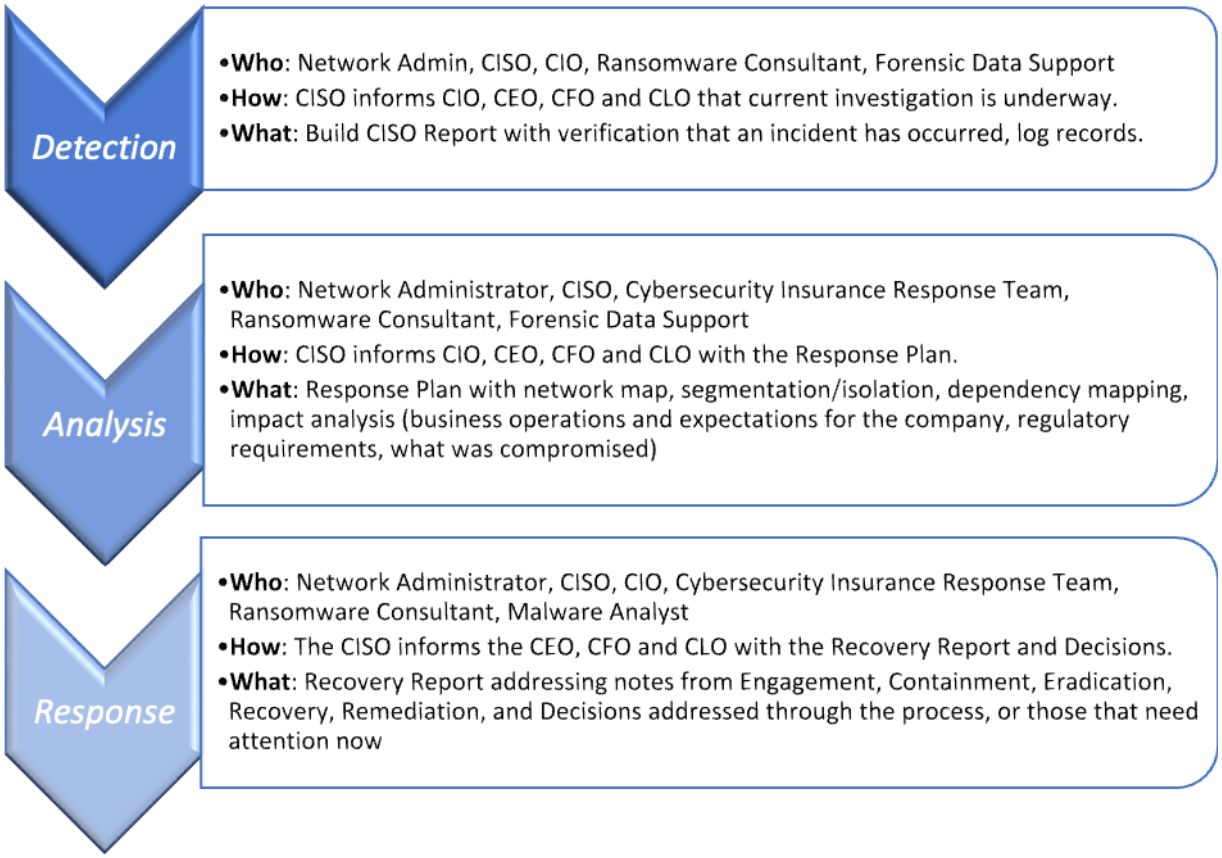

Figure 1: Process Overview

2.2 Detection

Who:

- Network Administrator
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Ransomware Consultant (see section 2.6.2, "External Resources and Services")
- Forensic Data Support (see section 2.6.2, "External Resources and Services")

How: The CISO informs the following officers that an investigation is underway:

- CIO
- CEO
- Chief Financial Officer (CFO)
- Chief Law Officer (CLO)

Signs of a ransomware attack

This phase is the first part of the incident response. It is important to verify that an incident has occurred and to determine the type of attack. Often with ransomware there will be specific signs:

- Files are renamed with new extensions.
- Unusual filenames for .doc or .docx files.
- Files are inaccessible and unreadable.
- Systems may be unstable, or may crash as critical files may have been encrypted.
- Web sites may be defaced or altered. This may be an indicator, or it may be the entirety of the attack. Analyze what may have been compromised and how to address needed changes.
- Pages may be printed with ransomware notification and demands.
- Attackers may have made themselves known through other methods as well (e.g., press or social media).

There are other instances where potential victims are notified, often through other electronic means (SMS, email, etc.), but are not actually victims of a penetration of corporate defenses.

Confirm that systems are all operable, accessible, and that defenses are intact:

- Use tools to scan storage for malicious files or activity.
- Check logging records.
- Confirm authorization changes.
- Look at authentication effort records.

If you can confirm that you were a victim, can you identify which systems were impacted and which were not?

After identification, it's time to move on to next steps.

If you think you were not victimized, or are unsure, there remain activities to consider in section 2.4, "Response." These may indicate that an adversarial actor still has some access to some of your systems or network, and that defenses need to be refreshed and extended.

Key to this stage is the preparation element of the deliverable (below); this preparation includes how your organization is going to respond, who makes decisions, what process to follow, who will be interacting with the systems, and how that will be done.

Deliverable The CISO then shares the result of the Detection activity, including:

- its initial scope,
- the systems affected, and
- clear communication of the next steps (see section on Analysis below).

The CISO should inform others that:

- there may be a halt to regular business activities,
- decisions will need to be made related to this ransomware activity, and
- additional resources may need to be brought in to help.

Calmly informing others that there is a plan and a strategy being followed will help in prioritizing resources throughout the process. As it is common for there to be reactions to incidents of this nature, it is worthwhile to work with the CHRO to see if counseling options can be made available.

2.3 Analysis

Who:

- Network Administrator
- CISO
- CIO
- CLO
- Cybersecurity Insurance Incident Response Team (see section 2.6.2, "External Resources and Services")
- Ransomware Consultant (see section 2.6.2, "External Resources and Services")
- Forensic Data Support (see section 2.6.2, "External Resources and Services")
- Potentially, Outside Counsel (see section 2.6.2, "External Resources and Services")

How: The CISO shares the Response Plan with:

- CIO
- CEO
- CFO

After confirming victimhood, it's important to understand more of what your organization will be addressing. This activity involves scoping

- affected systems
- data boundaries
- users impacted
- projects/products/services impacted
- customer-facing elements, and
- public-facing elements

It's important to evaluate the type of compromise versus your capabilities. Were attackers able to access unencrypted data? Were attackers able to modify data? Would your organization know if attackers were able to modify data?

Attempt to ascertain the type of malware that was used, how the network was compromised, and the systems linked to. Make sure to note all vulnerabilities discovered in this process; a Malware Analyst (see section 2.6.2, "External Resources and Services") is helpful at this discovery stage.

Step Advice During this process: KEEP ALL NOTES in the notebook referenced at the start of this section.

Step Advice Create a section of your notebook for descriptive information about the malware. Consider the following questions:

- Are files still usable?
- Is there a time limit for response?
- What are the demands?
- Is it a single threat or are there multiple actors/demands?
- How easily can the enterprise switch to alternative methods of revenue generation and work management?

Step Advice In evaluating scope, assemble the following and use for systematic evaluation of scope:

- Map of the network
- Identity of connection/routing points
- Map internal segmentations

Identify and prepare to activate any segmentation protections available.

Prioritize:

- Critical operations
- Network security
- Sensitive data stores
- Personnel files
- Financial support systems

Step Advice

- Update malware/antivirus solution and scan every machine for malware, even those machines that do not behave suspiciously.
- Determine the type of malware or ransomware found.
- Look at online descriptions of this particular malware to know what it does and what it attacks.
- Make a list of known infected machines.

Step Advice Under guidance from the Ransomware Consultant, Cybersecurity Insurance Incident Response Team, and Forensic Data Support,

- Begin the analysis and capture of log files and forensic information from infected machines.
- Plan out the segmentation and isolation of systems as best as possible.

Remember to look in log files for any Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), firewalls or other perimeter or internal defense systems. They may not seem to be in the attack path, but can help identify other potentially compromised systems.

Step Advice With the CLO, and often Outside Counsel,

- Determine which local, regional, or national notification requirements apply to your organization.
- Determine the time constraints, content expectations, and receiving parties for this information.

The CLO should communicate this to the other executives and manage the messaging with the CMO.

Notification activities typically occur in the Response step, below, but the timeline may dictate adjustments to this schedule.

The key output from this phase is a Response Plan that includes the following (NOTE: some of these documents may already exist, and could be used as a starting point):

1. A network map highlighting or identifying the infected system, existing boundaries, and any new boundaries if any were put in place ahead of the Response activities.
2. A segmentation and isolation plan for infected systems.
3. Dependency mapping between systems. Databases, for example, may be used by several systems. The integrity and consistency between databases where one gets restored but others are not can lead to application and linking errors later.
4. Impact assessment on business operations and expectation-setting for the company. This assessment also includes answers to what types of data were compromised (or could have been compromised): business transactions, financial data, confidential information, health data, personnel records, or other protected data. Are there regulatory requirements around disclosure for the type of data potentially compromised? These may include – but are not limited to – HIPAA, COPPA, TCPA, GDPR, CCPA, CPRA, and PIPEDA.
5. Legal may have additional expectations and questions about the potential for liability, credit reporting, and additional regulatory requirements. Much of this depends on the nature of the business.
6. A backup/restoration plan for each highlighted system or dependent system.

The Response Plan should be checked by the Analysis team for completeness and accuracy before being shared through the CISO.

Decision Point The CISO will share the Response Plan with the rest of the team. The Response Plan will help the enterprise to determine if law enforcement will be brought in and the scope of that engagement (if scope can be adequately controlled). Please see section 2.5.2, "Engaging Law Enforcement, and When."

The next order of business is to prevent further damage or intrusion.

2.4 Response

The Response Phase is segmented into four sub-phases: Engagement, Containment, Eradication, and Recovery/Remediation.

Step Advice During the Analysis phase, you identified segmentation protections available. Activate those per plan. It is in the Response Phase where the team will take the first real action on the network and devices.

Step Advice The Analysis phase also included Step Advice on notification requirements that apply to the organization. In the Response Phase, the CMO, often in concert with Outside Counsel and the CLO, will craft the statement that satisfies the legal/regulatory obligation or obligations related to notification of

authorities that a ransomware event has been identified. Different statutory requirements may exist that expand on the scope defined above, but this is the stage where that information is delivered on behalf of the company.

Who:

- Network Administrator
- CISO
- CIO
- CMO
- Cybersecurity Insurance Incident Response Team
- Ransomware Consultant
- Malware Analyst

How: The CISO shares the Recovery Report and Decisions with:

- CEO
- CFO
- CLO

2.4.1 Engagement

You aren't likely to be able to handle this ransomware event by yourself. This is going to get more difficult before the process is complete. Figuring out who will be on the response team early on will save time and effort later. Look at your team, budget, and resources available. Your first goal is to identify who to assign or hire for the following roles:

1. Technical Response Team and Leader
2. Internal Communications Response Team and Leader
3. External Communications Response Team and Leader.

Section 2.6, "People," will be important in granular assignment of responsibilities.

2.4.2 Containment

Several activities fall under this section:

- Separate backups from other systems.
- Remove infected systems from the network, but again, **DO NOT TURN OFF THOSE SYSTEMS**.
- Actively run external port scans on remaining systems to see if unexpected ports are open.
- Run local malware detection on each system to determine further vulnerabilities.
- Make sure you have strong authentication measures in place for each system. Update passwords/access credentials/CERTs for all systems and personnel, not just infected ones. You may have to assume that your entire authentication system data is compromised and untrustworthy.
- Part of this stage will include forensic analysis of the infected machines. This is important not only for compliance, but because it will identify the modus operandi used by the attackers, which will help you identify other systems subject to investigation.

Step Advice The machines you have removed from the network will likely need to be retained (and potentially delivered to investigators). Do not expect to "reset" them and get them back into production. If they are virtual, create new virtual machines for subsequent use when you are at the "Recovery and Remediation" step below (section 2.4.4). If the machines are physical, this is now a great time to upgrade those systems and get those new versions into place. Legal, compliance, law enforcement, and regulatory needs (particularly if health-care related) may need to be addressed and there may be additional research later to determine if data loss or exfiltration occurred.

Consider that no single machine is "too important to isolate." If a machine is infected, it's best to remove it from your network. If the function is critical to your organization, spin up a spare as soon as possible.

2.4.3 Eradication

Each attack, network, system map, mechanism, and residual threat footprint is unique, even if the tools to counter attacks sometimes resemble each other. Your Technical Response Team can now work to make sure there are no remnants of the intrusion still within the network.

Step Advice Restoration has the potential for re-infection, so understanding the date of intrusion and mechanism of intrusion is important. It may seem urgent to get systems back up to keep the company running, but failure to fully understand how access was gained can quickly lead to further outages and wasted time.

2.4.4 Recovery and Remediation

In this phase, your goal will be to recognize and limit the damage, and to normalize business operations as quickly as possible. In an emergency, using backups is the safest and most reliable measure. However, it is only successful if the backup data is "clean" and not itself affected by the attack. As outlined in the previous section, you should keep an eye on a few points in advance and develop a multi-stage recovery plan for an emergency. The faster and more precisely you know which data is affected, the more targeted your countermeasures can be. The goals are to restore your business, gain time, and act effectively.

In some cases, a tool to help decrypt files associated with the attack may be available. This occurs because some encryption keys get reused for multiple attacks if the malicious actor doesn't update their own tooling. Some sites exist to help distribute these tools, but be advised that not all tools advertising help are what they seem. You can find example sites in these footnotes, but exercise caution: *caveat emptor*.[8,9] Law enforcement and cybersecurity experts can help to identify trusted resources for decryptor tools.

Apart from preventing further damage by limiting the extent of the attack and ensuring further operation of your IT environment, you will need to identify the source of the attack. The initial infiltration – before the actual data encryption – may have occurred a long time before its detection.

External legal and technical advisors have proven to be essential. Their hands-on experience will result in a better overview of things that have to be done. They will be able to do an independent analysis of the scenario that has led to the situation.

---

[8] https://nomoreransom.org/
[9] https://www.bleib-virenfrei.de/it-sicherheit/ransomware/liste/

If you have been able to identify and isolate each of the infected systems, and have been able to determine when the infection occurred, you can begin to identify the target backups and copy them to a working drive. If possible, deploy those backups to a separate, independent, non-networked system for re-analysis. Confirm with the Malware Analyst that the system is not infected and does not carry any identifiable latent malware. Ideally, swap that machine in for the previously infected system. If the Malware Analyst indicates that this new system is still infected, the presumptions around initial date of infection were incorrect; reassess and reapply the above technique to find the next newest backup free of malware. Repeat this process for each infected system.

Depending on your situation and on applicable laws, you may be required to classify the data and evidence collected as legal hold. As a result, you should not wipe and reset infected machines, as they may hold critical evidence. In the case of virtual machines, keeping a snapshot of the machine should suffice. In the case of physical machines, consider this event an accelerated replacement plan; if that presents an economic hardship, consider that a backup of the infected machine may be necessary prior to returning it to service.

Decision Point Finally, part of the response to a ransomware attack is the decision of whether or not to make the attack known beyond any notifications that may have been made earlier. (This may happen anyway if the enterprise isn't careful about what is said publicly, or even privately.) Please see section 2.5.5, "Acknowledgement of Victimhood and Notification Requirements," for detailed considerations.

2.5 Decisions

Every decision has a consequence (and a subsequent loss of flexibility or ease in switching approaches later), so understanding the impact of these decisions is important. This is not a comprehensive list of those considerations or their results, but is intended to provide a framework through which additional considerations may be viewed.

2.5.1 Engaging the Cybersecurity Insurance Policy and Incident Response Team

Engaging the insurance company through formalizing a claim is balanced against accepting that premiums may be impacted going forward. While legitimate, this is also why you have the insurance. The cost of not engaging the team may quickly outpace the support obtained from promptly bringing in the help you may need. If the situation can be resolved without filing a claim, it may be possible to avoid this step.

Expected Timing This is one of the earliest decisions; it is usually made when you are first determining if you really were hit with ransomware, or if you can recover. The answer can be obvious and quickly determined in some cases, and in others it may take some time to research; that time can be important.

The contact information for the cyber incident response center for your cyber insurance policy is usually found with the policy. **The policy, incidentally, should be kept offline, and never online where it is reachable through the network.**[10]

Engaging the insurance team often starts with filing a claim, but in some cases the insurance company may offer help on this front before the formality of a claim. Your objective either way is to gain the potential help from the Cybersecurity Insurance Incident Response Team.

[10]Malicious cyber actors search for policies online so they know how much they can ask for and what the coverage limits are for each policy. This information should be offline and available to the legal department and others only as needed.

It is important to understand the coverage and limits provided by the insurance policy (if applicable) and any uncovered costs of action, such as third party incident response, backup and restoration costs.

2.5.2 Engaging Law Enforcement, and When

The decision to involve law enforcement is not always easy or straightforward. The executive team, information security, legal, marketing, and the board of directors all will likely desire to be party to this decision, and to decisions around timing.

Expected Timing This could take place as early as the realization of victimhood. In some cases, it may never happen. In others, it may occur only after the situation has been entirely resolved. Be prepared to answer if and when you expect to do this as part of the Response Plan deliverable from the Analysis section.

Prior to engaging law enforcement, forensic validation of the incident should be complete to the point where your organization is confident a crime was committed.

The concerns with sharing this information include potentially opening up the enterprise's corporate policies to scrutiny, inviting new questions, satisfying another party with updates and status, delays in addressing the breach, and maintaining privilege over findings, or findings that impact to any civil action.[11] Additionally, you will be asked for forensic information, and your systems can be treated as a crime scene, which could have operational impacts should those systems be critical. In the US, the agencies with jurisdiction in these spaces include the FBI, DHS, and Secret Service. In other countries, similar agencies may act in an analogous manner. Ideally, this law enforcement relationship existed ahead of time, but this is not always practical or realistic. Law enforcement may also have areas where they encourage behavior with varying degrees of insistence. If they strongly oppose payment, or restrict your organization from paying the ransom, this relationship has limited your options.

The benefits of law enforcement engagement include experience, potential help in identification of the threat vector, negotiation and in some cases even decryption (they may have the key from another cyber attack). Do not, however, wait for law enforcement agencies to help you restore or secure your systems. They are engaged to address the crime, not to restore your organization's IT. Many law enforcement organizations have taken steps to show that they will treat the victims as victims and work to try to minimize distracting your organization's internal operations.

Depending upon the jurisdiction, it may be a requirement to notify law enforcement or other agencies; failure to do this within specified timeframes may put your organization, and involved individuals, at risk of non-compliance. The CLO should be kept informed and engaged to enable the proper handling of this decision.

To report a cyber incident in the United States, the FBI's Internet Crime Complaint Center can be found at https://www.ic3.gov/.

2.5.3 Payment of Ransom

M3AAWG does not endorse fulfilling ransomware demands as a solution. Paying ransom does not guarantee restoration of system functionality or data accessibility. Furthermore, there is a potential risk of experiencing additional extortion attempts from the same threat actor group.

[11] David Burns and Brian Williamson, "Should companies cooperate with law enforcement during ransomware attacks?", Global Investigations Review, Oct 2022, https://www.gibsondunn.com/wp-content/uploads/2021/10/Burns-Williamson-Should-companies-cooperate-with-law-enforcement-during-ransomware-attacks-GIR-10-08-2021.pdf

Payment of the ransom ends up being a relatively complicated decision process that involves several considerations. Make sure to budget time for this conversation to happen at several levels. Try to have Legal present for all of those conversations.

In the National Cybersecurity Strategy (2023), the White House has this to say about ransomware payments:

> Ultimately, the most effective way to undermine the motivation of these criminal groups is to reduce the potential for profit. For this reason, the Administration strongly discourages the payment of ransoms. At the same time, victims of ransomware - whether or not they choose to pay a ransom - should report the incident to law enforcement and other appropriate agencies.[12]

Expected Timing This decision usually comes after the Analysis phase. There may be times when the investigation or recovery may be more costly than paying the ransom. Ransomware payment is usually the last option left for recovery. There are times when the loss of data subsequent to the last good backup can be extremely detrimental to the business, thus the balancing of costs and benefits takes place.

One of the very first questions to consider is if ransom payments are legal in your jurisdiction. Engage Legal on this step early on and in every conversation on this topic thereafter. Some jurisdictions restrict/prohibit extortion payments of any sort. Some, such as the US Office of Foreign Assets Control (OFAC),[13] may limit it by other factors. Frameworks exist that prevent payment to known suppliers of aid to terrorist organizations. If the actor you are considering paying is on that restricted list, payment could land your firm in regulatory compliance proceedings. While these restrictions may limit the paths available to the enterprise, in some jurisdictions there may also be criminal penalties or personal sanctions that may be levied against decision-makers.

While it's great to understand the nuances of this space prior to being victimized, the motivation at this stage is paramount. Ransoms are negotiable. If you decide to pay the ransom, it's beneficial to know the going rate (which can be as low as 10% of the ask). You also need to understand who you are dealing with and how frequently those particular ransom actors deliver decrypters that adequately help recovery. Once you know this, you may also have some insight into the tooling they used, what decrypters may be available, and where to find them.

Ransomware payments perpetuate the ransom problem; if there were no option to extort funds through this path, it wouldn't be profitable and there would be less ransomware. This macro view is not incorrect, but it's worth noting that it comes from a place of privilege; like its peers, the enterprise that is under attack also has limited resources. That enterprise may also not have the ability or time to look at other options. While refusal to pay helps everyone, payment may be a necessity in some cases.

It's important to understand that even accepting the decrypter after payment carries its own risks. If you are not completely recovered from the malware, residual monitoring may exist to identify the specific data that was decrypted/undeleted first. This may provide additional information to malware actors for additional attacks in the future. If you do decide to pay, consider the next section, "Negotiating Ransomware Payments."

---

[12] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[13] https://www.globalcompliancenews.com/2021/10/28/ofac-issues-updated-ransomware-advisory-and-designates-suex-as-an-sdn181021/

2.5.4 Negotiating Ransomware Payments

Professional ransom negotiators exist. In fact, they may find you, because they may be aware of this event; you will need to judge their trustworthiness. They may also offer advice on this and other questions. They may even indicate that you should reconsider the (above) decision on paying the ransom.

Expected Timing Negotiating payments occurs after the decision about paying ransoms is complete. This doesn't mean that the Ransomware Negotiator doesn't engage earlier than this step. They can be instrumental in helping understand the tradeoffs and options around likely outcomes.

2.5.5 Acknowledgement of Victimhood and Notification Requirements

Letting the press know that the enterprise is currently being victimized, or was attacked in the past, is a decision with impact to the Legal, Compliance, Marketing, and other departments.

Expected Timing Many threat actors do not publicize companies that are being attacked. In some ways the publicity can run counter to their objectives and has a higher likelihood of engaging law enforcement. The acknowledgement question is usually driven through needs identified by the Legal or Compliance departments and the local regulatory environment. In some cases, victims never acknowledge victimhood. In others, it is a step taken almost immediately.

Acknowledging victimhood may have detrimental impacts on the enterprise; these include the stock price, private valuations, creditworthiness, customer confidence, good will, and name and brand recognition, among others.

In some cases, victims are under legal requirements to disclose an attack. Sometimes the timing is rapid and can be as soon as they know it has begun. It's important to understand what the jurisdictional requirements are for your enterprise. (Often these laws only apply to companies of a certain size, trading status,[14] or in a given industry or sector). In the United States, information on reporting can be found at stopransomware.gov.[15]

In addition to regulatory requirements, many supply-chain relationships now have breach reporting requirements that have been added over the last several years. Your organization may have such obligations to suppliers or to customers. It is important to make sure that the CLO is engaged in a contract review process related to this incursion.

What are the responsibilities you face as a victim? Who needs to know, and by when? How does this impact your business? Have your customers been affected? Have they been notified? Is there a data protection or privacy requirement for you to advise them of this? Have ransomers reached out to your data subjects already? What moral and ethical considerations should you consider in notification questions? Those that might be notified include:

- Law enforcement
- Regulatory bodies
- Elected bodies
- Industry bodies
- Customers

[14] https://www.google.com/url?q=https://www.sec.gov/rules/proposed/2022/33-11038.pdf&sa=D&source=docs&ust=1676059185887151&usg=AOvVaw26lE3B9FzA1LHlK7uiZqyy

[15] https://www.cisa.gov/news-events/news/getting-ahead-ransomware-epidemic-cisas-pre-ransomware-notifications-help-organizations-stop-attacks

- Partners
- Vendors
- Service staff

In some jurisdictions, some industries or companies of a given size have different requirements on notification. Some examples of this include, in the United States, the HIPAA law that covers health-related information about individuals. There are clear definitions of what is and what is not a breach. In the case of the former, there are also reporting requirements, both to the subjects of the data but also to the Department of Health and Human Services. Laws other than those that treat specific ransomware and malware and that may have impact include data protection and privacy laws such as GDPR in the EU, PIPEDA in Canada, and COPPA/HIPAA/ARRA/GLBA in the US. Several US states now have privacy laws that further obligate victims in some situations (e.g. CPRA, CCPA, and other states with similar measures). Aside from Canada, the EU, and the US, sixteen other countries have privacy protection legislation in force, most of which have some level of reporting requirements. These are questions for the Legal Department and Chief Legal Officer as soon they are first read into the ransomware problem.

One consideration is unintentional acknowledgement; that is, submission of documents or log files with identification marks or logos that may inadvertently implicate your company. Also, be extremely careful about communications that admit fault, since this may impact the insurance and regulatory response.

2.6 People

Consider notifications in careful order. There are several people and committees/boards/groups that will need to be brought in. You may need to keep their focus on areas where they can be most helpful. Consider also the benefits of informing the right people of important steps early. Each organization is going to be structured differently. Some may have reporting structures between executives that are unique. The following roles may have responsibilities during this response:

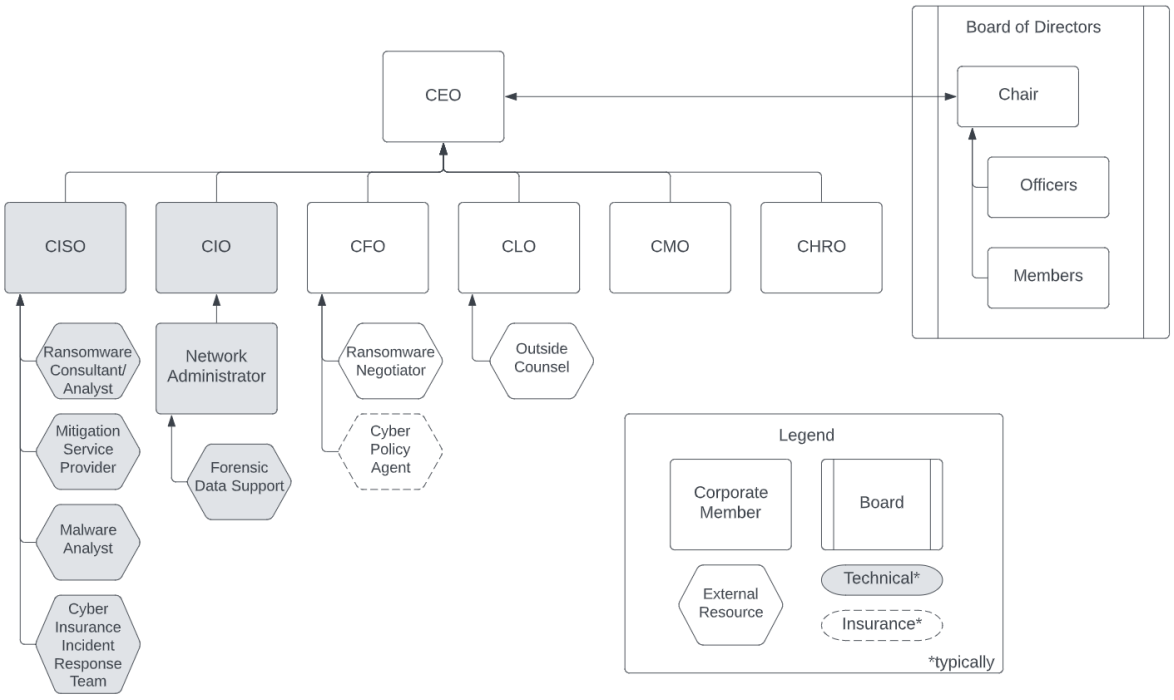

Figure 2: Typical Organizational Roles Involved in Ransomware Mitigation

2.6.1 Internal Resources

CISO: The Chief Information Security Officer (CISO), or the primary person with responsibilities encompassing the security of the enterprise data, resources, computation, and technical operations. The CISO is usually the first to be notified. In a perfect world there is a practiced playbook for the next steps, but none of us live in a perfect world. The CISO should have the contact information for other parties, and should be the one through which the new, highly critical, project of recovery and mitigation should be led. Some organizations have a Chief Security Officer (CSO) who may or may not be engaged in technical security, and therefore may or may not be necessary in the ransomware conversation if physical access wasn't obtained.

CIO: The Chief Information Officer (CIO) is responsible for all information systems and data. Relationships between the CIO and CISO, CIO and executive team, or the board may necessitate a greater involvement in the process. In many cases, the CIO also acts as the CISO. Some other titles and roles that may be part of this process include the Data Protection Officer (DPO) or the CDO (Chief Data Officer).

CEO: The Chief Executive Officer (CEO), or the primary leader for the organization (e.g., President, Chair, etc.) should be informed of the ransomware activity, the actions taken so far, the plan going forward (including the notification efforts), and when to expect an update on progress. This conversation will be important: the objectives are to inform, ask for support/resources, control communication channels, and prepare for upcoming key decisions.

CFO: The Chief Financial Officer (CFO) and their entire department need to be aware of the threat and the status of the investigations related to the ransomware. The current security and verification posture at the

enterprise may need to be escalated with a known threat actor engaged. The CFO also will be part of the conversation around financial decisions related to external resources brought in to help, with negotiations with insurers, and decisions related to payment of ransoms.

CLO: The Chief Legal Officer (CLO), Internal Counsel, or even Outside Counsel will engage from the victim relationship with law enforcement; from a compliance perspective with regulators (engagement with the extortionists who may be on restricted lists within some jurisdictions, breach content, and data protection compliance); and perhaps part of negotiations with ransom actors. Some organizations also have a Chief Privacy Officer (CPO), which is often very legal-focused, but can also be technical and have a mix of responsibilities between Legal and IT departments.

CMO: The Chief Marketing Officer is often responsible for corporate reputation, press relationships, and external messaging. The CMO or their team will need to be engaged in the decisions around how to respond or publish information related to the attack, staying aware of social media, web, and traditional media releases related to the event.

CHRO: The Chief Human Resources Officer (CHRO), or person acting in the lead capacity for the human resources department within the enterprise will be engaged particularly if employee data was compromised during the attack. Timing and scope of informing messaging may have legal and regulatory requirements and impact.

Board of Directors: The Board may be an external group of experienced leaders. It is usually the CEO or equivalent who will need to communicate with the Board about the ransomware and its impact. The Board is usually the final arbiter of difficult decisions and will need to be kept informed and updated during the ransomware investigation and mitigation efforts.

Network Administrator: The person or people responsible for the network architecture, where each system connects, and how. In some companies this may be the same as the CIO or the CISO, above; in others it may be distributed. These technical resources are going to be critical in the analysis and mitigation phases.

2.6.2 External Resources and Services

Outside Counsel: The role for outside counsel is to augment the existing legal team with expertise in ransom payments, terrorism watch lists, cybersecurity policy interpretation, and data breach regulations in each of the legal and regulatory jurisdictions within which the enterprise engages.

Cybersecurity Insurance Incident Response Team: The policy under which the company is covered, if any, may include access to technical and ransomware response expertise or resources. Access to this resource is often restricted to only once a claim has been filed. This may be a call center, on-site consultants, remote expertise, documentation, tools, or any combination thereof; this group will be referred to as the Cybersecurity Insurance Incident Response Team.

Cybersecurity Policy Agent: The cybersecurity insurer will often provide an adjuster and a ransomware team to engage in this process with the insured. The decisions around how much help and boundaries of the engagement will be part of the discussion at the executive level.

Malware Analyst: This specialist can work with the Cybersecurity Insurance Incident Response Team, and may be part of that team in some cases. The Malware Analyst's role is to help scan for, identify, and remove malware from systems and the network. They can also be valuable in determining the time and date of initial intrusion, and the vector of the attack. This can then help in identifying vulnerabilities that may need to be addressed.

Forensic Data Support: Determining exactly what happened, when, and how is an absolutely critical part of this process, and one of the important early steps in the process. A forensic data scientist is an expert in preservation, analysis, and discovery of methods, tools, and techniques used by the malware actors. Many organizations do not have a forensic data scientist on staff but consultants can be found in most markets.

Ransomware Consultant/Advisors and Mitigation Service Providers: Organizations, individuals and services exist with varied experience and capabilities. Finding and evaluating help in this space can often be provided by cybersecurity policy agents and law enforcement – but both of these bring their own biases to those recommendations.

Ransomware Negotiator: Specialized consultants in this space, similar to larger Ransomware Consultants, above, can be found, and in the same way defined above. Negotiators are often up to date on the current rate at which ransom actors are accepting negotiated payments and can assist in significantly reducing expected spend in this realm.

2.7 Technology

Several categories of technology exist for detection and response to a ransomware event. First amongst these are endpoint protection tools like anti-malware and vulnerability management vendors. These can, and should, be installed after ransomware infection, to make sure you are using the most recent version. Also, malware is known to deactivate or damage existing installed security solutions. Several free virus scanning solutions are available, too, but be aware that their functionality may be limited compared to the commercially available solutions. Also, using a web-based virus scanner requires you to upload your (potentially infected) files to the site. **Those sites may keep the uploaded samples and may make that information public**; this may pose a privacy risk.

Endpoint detection and response tools provide advanced attack detections that are near real-time and actionable. This type of software is designed to protect individual devices such as computers and smartphones from malware and other threats. Depending on the size of your business there are also managed services that will provide these tools for you. The added benefit for having this functionality deployed in your environment is that you will also be able to better understand the breadth of any attack. Evaluation of the impact and recoverability of any lost data will be more sophisticated, and will help drive your pay/no pay conversations as well. Endpoint security software may even be helpful to install after a first ransomware detection, as it may prevent further malicious changes on the machine, and may help identify suspect processes or programs. It cannot, however, undo the effect of the ransomware. It is important to note that having an endpoint detection and response tool does not mean you won't become a victim in the future. Your organization must implement defense-in-depth practices to best minimize your chances of falling victim to ransomware attacks.

You can use a backup not only as a way to restore your data, but also as a tool to investigate the extent of the infection. By comparing files with their backup versions, you can check if a file or program has been recently modified. When you access your backup, make sure to do it from a non-infected machine. (The attackers might be more interested in stealing your data, and having access to the backups may give them access to more than they would normally have). Also, make sure your backups have not also been compromised. This can be done by making sure the backups are read-only, or by keeping checksums of the backups at another (tamper-proof) location in order to detect any possible changes.

Sometimes cloud storage solutions have built-in backups, or make "previous versions" of files available, allowing you to restore from those versions, or to detect changes in them.

In the event of a ransomware attack, one potential recovery strategy is to use a ransomware decryption tool. These tools can sometimes reverse the encryption performed by the ransomware, allowing the affected files to be accessed again without having to pay the ransom. However, the effectiveness of decryption tools can vary depending on the specific ransomware strain. There is no guarantee that they will work in every case. Decryptors can be found online,[16,17] Do exercise caution with regard to trust of resources. Look for sites that are run by government organizations.

2.8 Post Incident

The final stage of incident response is the post-incident phase. This includes conducting a thorough analysis of the incident, documenting the lessons learned, and implementing measures to prevent similar incidents from occurring in the future. This phase is critical to the overall success of the incident response process, as it allows organizations to identify areas for improvement and take action to mitigate future risks.

Deliverable During the post-incident phase, a detailed incident report should be prepared that includes an overview of the incident, the actions taken to contain and resolve it, and the impact on the organization. This report should be reviewed by the full incident response team and management to identify any areas for improvement in the incident response process.

Step Advice The lessons learned from the incident should be documented and shared with relevant stakeholders. These lessons should be used to update incident response plans and procedures, as well as to train staff on how to stay alert to vulnerabilities, and how to respond to similar incidents in the future.[18]

Step Advice The post-incident phase should include a comprehensive review of the organization's security controls and systems to identify any vulnerabilities that may have contributed to the incident. Based on the findings of this review, appropriate measures should be implemented to mitigate or eliminate these vulnerabilities to reduce the risk of similar incidents in the future. Now that you have some breathing room to prepare against future attacks, there are resources available[19] to help organize this work.

3. Conclusion

In this document, the primary focus has been on what to do in the event of a newly discovered ransomware incident. The realities of finding oneself in this situation do not include the freedom of time, structuring backups and recovery differently, or of improving endpoint protections prior to the infection. The scope of this document is limited to a current attack and initial response. The broader topic of ransomware defense and prevention includes both preparing against ransomware and further recovery from such an attack. Excellent external resources are available to help with definition, preparedness, legal and regulatory implications, and additional follow-up after an incident. [20, 21]

---

[16] https://nomoreransom.org/
[17] https://www.bleib-virenfrei.de/it-sicherheit/ransomware/liste/ (in German)
[18] https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot
[19] NIST and the National Cybersecurity Center of Excellence (NCCoE) have compiled the "Ransomware Risk Management: A Cybersecurity Framework Profile," Barker, Fisher, Scarfone, & Souppaya, 2022, https://csrc.nist.gov/publications/detail/nistir/8374/final
[20] Ibid.
[21] US Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) "Tips & Tactics: Preparing Your Organization for Ransomware Attacks," May 2021,

Legal Disclaimer: This document is not legal advice. M3AAWG strongly suggests that readers work with their company's legal counsel or avail themselves of independent legal advice regarding their rights, responsibilities, and obligations relevant to prevailing legal jurisdictions.

This document is maintained by the Messaging Malware Mobile Anti-Abuse Working Group (M[3]AAWG). As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates or propose an update here.

M3AAWG-143

https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf