Ransomware Framework: A Prevention, Response & Recovery Guide

Written by Cibecs - https://cibecs.com/endpoint-backup-security-quiz/

This framework can be used as a guide to manage the risk organizations face in light of ransomware attacks.

Objective: This framework aims to help IT managers and CIOs gauge their organization's level of readiness to mitigate ransomware events, identify and establish preventative measures and what to do, how to respond and recover in the event of a ransomware event.

What is Ransomware

Ransomware is a type of malware cybercriminals use to block access to a user or organizations data in exchange for a ransom. These digital criminals usually encrypt the files on your system or copy over data and delete it from company devices and hold this information "hostage" until the money demanded is paid.

During the initial infection, the ransomware may attempt to spread throughout your network to shared drives, servers, attached computers and other accessible systems. Extortion is increasingly common and in the event an organization refuses to pay the ransom, stolen data may be leaked or sold on the dark web.

In short, ransomware is a potential headache for unprepared IT administrators.

Ransomware Vectors

Ransomware comes in many shapes, forms and variations. Ransomware has also evolved over time and will continue to do so in order to circumvent the modern cybersecurity measures that have been created to stop these malicious attacks.

Below we list the most common types:

- **Crypto ransomware also known as encryptors**
  This is the most common and well-known form of ransomware. The aim of this form of ransomware is to encrypt the important files and data within the data environment. The information is inaccessible by users without a decryption key. These attacks often require the ransom to be paid in a set time period. If the deadline isn't met the data is destroyed or compromised.

- **Lockers**
  This kind of ransomware locks endpoints, applications and files making the organization's system inaccessible. The aim of this attack is to extract funds in exchange for restoring functionality to locked devices and systems.

- **Scareware**
  This is a form of malware that gains access to a system or device and poses as legitimate software alerting you to detect a virus or other issue on your computer and directs you to pay to resolve the problem. Some types of scareware lock the computer, while others simply flood the screen with pop-up alerts.

- **Doxware or leakware**
  This type of attack threatens to distribute sensitive or confidential information online or leak it to third-parties. Depending on the targeted business this form of ransomware is exceptionally dangerous as the data may be leaked regardless of the ransom being paid.

- **Ransomware as a Service (RaaS)**
  Is a newer form of ransomware that has started gaining traction. It refers to malware that is hosted anonymously by a "professional" hacker that handles all aspects of the attack. This can be compared to software-as-a-service in the Whitehat realm where people pay a subscription for software that provides a useful service. RaaS operates the same way but is the malicious version of this type of software business structure.

Ransomware, as mentioned above, is a malicious software used to take sensitive information hostage through encrypting, deleting or threatening to release valuable data and only releasing or restoring this information in exchange for a ransom.

However, how ransomware enters your environment is known as an attack tactic, method or vector. It is the mechanism used to infiltrate an organization's data environment. There are various tactics that can be used.

Below are a few tactics (vectors) that are used to deploy ransomware:

- **Malware**
  - **Description:** Is a malicious software used to infect endpoint devices or networks. There are different forms of malware that are used to perform different actions. All ransomware utilizes malware programs to block access to or encrypt sensitive data in return for a ransom.
  - **How it is used:** Malware prevents systems from functioning or data access unless a ransom is paid.
  - **Malware variants:**
    - Trojans: file or software that seems legitimate that often contains ransomware.
    - Spyware: invades endpoint devices to steal information.
    - Rootkits: provides unauthorized access to end user devices without being detected.
    - Ransomware: encrypts or blocks access to data until a ransom is paid.
    - Worms: used to disrupt networks and consume bandwidth.
    - Keylogger: used to gain unauthorized access to accounts by recording keystrokes.

- **Phishing**
  - **Description:** Is a type of scam used by hackers or cybercriminals. It entails sending fraudulent messages that look as if they come from a reputable source encouraging users to share personal info or install malicious software to gain material that can be used to extort the user.
  - **How it is used:** Phishing has a host of negative effects such as loss of money, valuable information, business disruptions, etc.
  - **Phishing variants:**
    - Email Phishing: Is when hackers utilize email as the channel to perform phishing scams. This is the most common form of Phishing.
    - Spear Phishing: The targeting of specific individuals or groups of individuals within a company. This form of phishing is to target individuals who have access to more user information such as HR or financial managers. These attacks are usually more specific, and research is done on the target or targets making these communications very convincing.
    - Whaling: A form of spear phishing where the cybercriminal targets high-profile business stakeholders. The data obtained from these executives are often used to extort large sums of money through blackmail. Another form of whaling is when cybercriminals impersonate high-profile individuals to gain access to sensitive data or money through influence of employees.
    - Angler Phishing: an online scammer pretends to be a customer service or support accounts to convince a user to provide personal information or login

details. Often occurs on social media platforms such as Facebook, Instagram or Twitter.

- **Malvertising**
  - **Description:** Also known as malicious advertising whereby a hacker gains access to a legitimate advertising account and uses it to spread malware or the cyber attacker injects malicious code into the advertising networks so when users click on a legitimate ad they are redirected to a harmful website.
  - **How it is used:** For organizations malvertising damages their reputation and can have a negative effect on their business. For users who click on the links it can provide access to their or their organizations sensitive data and cause a ransomware attack.
  - Some sites that have displayed these dangerous advertisements:
    - The New York Times
    - BBC
    - MSN
    - News Week
    - Realtor.com
    - AOL

- **Social Engineering**
  - **Description:** Is a term that is used to encompass a broad range of harmful activities that are usually achieved through manipulating unexpecting individuals into granting them access to devices, information or networks.
  - **How it is used:** Hackers use social engineering to exploit human error to gain access to sensitive data, company networks and financial records that can be used to extort these organizations or individuals within the business.
  - **Examples of Social Engineering are**:
    - Phishing: a hacker sending fraudulent messages in the hopes of users providing sensitive information.
    - Baiting: whereby online criminals provide users with something free in exchange for information.
    - Pretexting: where a scam artist creates a pretext or fabricated scenario to con someone into providing sensitive personal or financial information

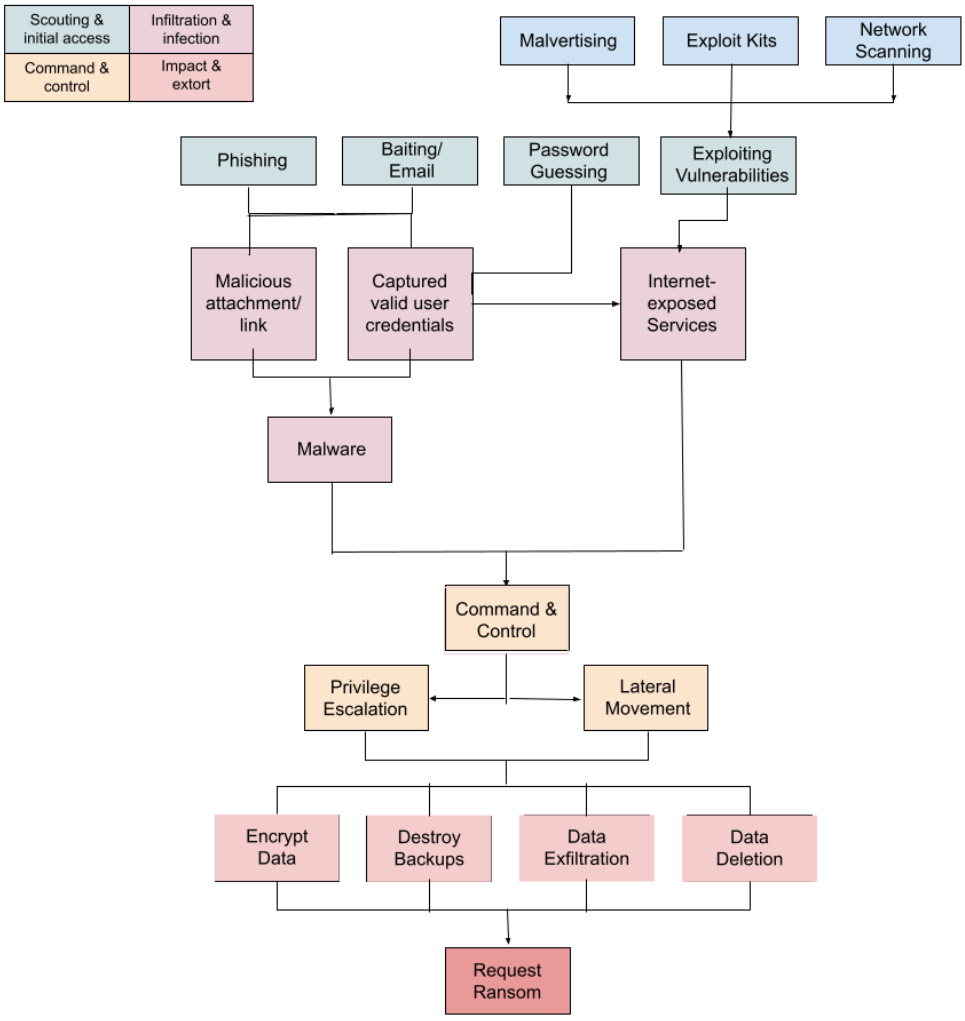
- **Exploit Kits**
  - **Description:** Are comprehensive tools or packs of tools that are used to identify and exploit vulnerabilities in users' systems in order to distribute malware or perform other malicious acts. These 'kits' are usually automated and activated as soon as users visit a compromised website or click a malicious link or download an infected

file. These intrusive toolkits usually utilize vulnerabilities in popular operating systems such as Adobe Flash, Java, or popular browser plugins or add-ons.

- **How it is used:** These exploit kits are mechanisms utilized by hackers to deliver and deploy ransomware on unsuspecting user devices or company networks.
- **Exploit kit infection stages:**
  - Step 1: Make contact through malvertising, phishing emails or harmful website links.
  - Step 2: Redirect the user to a malicious website hosting the exploit kit or piggyback on a download of a legitimate plugin to exploit vulnerabilities.
  - Step 3: The exploit kit infiltrates and identifies weaknesses in the user's system. Malware is downloaded through the identified vulnerability.
  - Step 4: User's device is infected, and ransomware is deployed and activated

There are many other channels and mechanisms hackers identify and use every day to exploit the vulnerabilities in user environments and on their endpoint devices to gain access and deploy malware.

Phases of a Ransomware Attack



- **Scouting & Initial access:**

  Hackers analyze the user network and look for a way to gain access. Based on their initial analysis they will identify which weak areas to target and deploy the appropriate attack vector.

- **Infiltration & Infection:**

  Next, the attacker deploys a range of tactics or methods to gain access to the data environment such as phishing, password guessing, network scanning, exploiting vulnerabilities and so on. Once malware has been successful in exploiting a weak spot and gained access to at least one device the hackers move to the next phase.

- **Command & Control:**

  The hacker attempts to gain access to all devices connected to the network through command and control, lateral movement and privilege escalation. The goal here is to target privileged user accounts and inventory all valuable data spread across the environment.

- **Impact/ Extort:**

  Once all the valuable data has been identified and inventoried, backups are destroyed, data is encrypted and exfiltration (unauthorized transfer or copying of data). After this is complete the organization is usually notified, and a ransomware amount is demanded to restore data or access to data.

Ransomware Prevention Controls

To help prepare your defenses we have identified the critical controls that can be used at each phase of a ransomware attack to prevent or hinder the event.

Implementing these controls should highlight the potential gaps in your data environment defenses and provide you with the tools needed to stop a ransomware attack in its tracks.

Required Critical Controls:

- **Secure internet-exposed services:** Today's business landscape is a mosaic of internet-connected online services. These services can often provide easy access to your organization's environment by acting as a gateway from user endpoint devices through the service/ application to the internet. If this gateway is not managed or secured it can create a weak point in your environment that is susceptible to attack.

Reducing these services to the bare essentials and ensuring these services are kept up to date, or are only connected to the internet, when necessary, can reduce your risk.

- **Patch software & systems:** A common trick all cybercriminals have in their hacking arsenal is identifying and exploiting vulnerabilities in well-known software that have not yet been updated. Software companies often strengthen these weak points through providing regular updates to their software known as 'patches'.

  Patches are released in an effort to reduce these soft spots in their programs. It is essential that you keep your organization's software up-to-date and implement these patches as and when available to reduce the risks associated with these programs.

  It is not only software that requires patches to reduce risks but also hardware such as printers or any other hardware that utilizes the internet and programs on your network.

  The best way to keep track of this is by instituting a patch management strategy for your organization, its devices and software.

- **Two or multi-factor authentication:** Setting up multi-factor verification is no longer an option but essential to preventing unauthorized access in a landscape where offline and online spaces are blurring together. This is especially important for cloud-based software or programs that are utilized through logging in on the internet. Besides ensuring users utilize strong passwords and keep them in a secure password manager, multi-factor authentication is the only way to reduce unauthorized access of sensitive information kept on online profiles, accounts and the like.

- **Disable macros:** Macros are programs or bits of code used within office software programs to enhance capabilities by automating repetitive or regularly actioned tasks. When downloading these macros or automations your users can be unintentionally welcoming malware onto their device and into the work environment. Be sure to use secure defaults and configurations for macros in your organizations to prevent the occurrence of these incidents.

- **Allow listing for applications:** Application whitelisting as it was previously known is a security protocol that sets the permission for running programs. In other words, it is the control over what applications can run within your environment. This ensures only trusted files, programs, applications and or software to perform tasks. These permissions are usually controlled by the organization's IT administrators. This system also blocks unauthorized applications from performing tasks, which are reviewed by IT and allowed or blocked depending on their intentions.

- **Logs and alerts:** Make use of a central endpoint logging system that enables you to set up logs and alerts for all endpoints within your environment to allow for early detection and investigation. Having a central log that provides device feeds provides the visibility required to prevent ransomware or other malicious software.

  Once this system is established be sure to set up events or occurrences that when they take place an alert is sent to the IT administrator to notify the team of the incident so they know when something odd or unexpected occurs and can investigate further.

- **Password managers:** Utilizing password managers within your organization and providing users with a password manager program is a great way to ensure strong passwords and safeguard them from malicious attacks. In combination with Multi-Factor Authentication (MFA), this will prevent the majority of unauthorized access incidents, and reduce the harm of phishing or credential theft.

- **Network segmentation:** Divides the network into smaller parts with the intention of improving the network's performance and enhancing security. A segmented network hinders the spread of malware by preventing an outbreak from spreading across the entire network through enabling additional controls and levels of access for different segments.

  Additionally, network segmentation can make compliance easier by separating networks that process payments or collect sensitive information from the rest of a company’s network. This means only certain parts of the network would require auditing.

- **Principle of least privilege (POLP):** Means only giving users access to certain resources, networks, applications and so on if they require access to complete a task. This principle means that if a user is compromised, the attacker can only access a limited number of resources and not infiltrate an entire organization. This gives the IT department time to secure the network and get rid of the threat.

  As a general rule when assigning permissions, give the least amount of access required.

- **Backups:** Play a major role in defending against ransomware by adding an additional layer of protection to your endpoint environment. By having a 'clean' copy of your sensitive data that is kept separately and encrypted you can prevent having to pay ransomware hackers to regain access to your own information. Hardware can easily be replaced but data can't and from a compliance standpoint you need to be able to prove you have these protocols in place.

  When it comes to backing up data not all software is created equal. You need to select a provider that not only backs up your data but secures your information.

  Ideally your data backups should be automated and set to recur at intervals that meet the needs of the organization. For example, a bank would require backups every second versus an advertising agency may only require daily backups.

- **Firewalls:** Are essential in protecting against malware as it blocks certain damaging websites, file downloads, and links from opening if they present a risk to the user. In essence a firewall prevents malicious attacks from accessing a computer network or user device via the internet. Firewalls provide additional security through monitoring the traffic that moves through the organization's environment.

  Firewalls can also be configured to isolate critical systems from other users or networks within your organization's environment, further supporting network segmentation as mentioned above.

- **Anti-malware software:** Detects, prevents and safeguards against malware software and viruses from entering a user's endpoint systems. Regularly scan endpoints to detect, block and remove any suspicious items from user devices.

- **Email filtering:** Email phishing is a major route for ransomware attackers to infiltrate organizations. A robust email filtering system will quickly identify and block malicious emails, attachments and spam from entering the organization's environment. However, user education is essential, as some mails may slip through the cracks and if users are able to identify threats, it can prevent malicious software gaining access to the users and organization's environment.

- **Disable Remote Desktop Protocol (RDP):** The Crypto locker and some other malware accesses target computers using Remote Desktop Protocol (RDP), a Windows utility that allows others, usually an IT administrator, to access the desktop remotely. If you do not need RDP, you should disable it to avoid RDP exploits.

IT managers and security teams must equip themselves with the weapons they need to safeguard an organization's entire internal environment from ransomware. The only way to adequately execute this is to completely understand the company's landscape and attack surface. Once IT has a complete picture of the company's environment they can implement the tools, systems and resources needed to create a solid defense and contingency plan in the case of an attack. A good place to start is through defining each and every component, connection, service, endpoint that is part of or has access to the organization's environment.

Next, segment each area of concern and implement the relevant controls to isolate each component from the rest of the organization to prevent the ability of malware to spread in the case of a breach.

Ransomware Prevention Checklist

Prepare, Implement and Secure

- Provide regular and thorough user ransomware education and awareness training, to enable users to quickly identify malicious activity and safeguard themselves.
- Conduct random 'attacks' such as simulated phishing campaigns, each quarterly to help users identify threats that get passed email filters.
- Map out attack scenarios and establish contingency plans for each.
- Establish an incident response plan that can be followed in the case of an attack.
- Schedule third-party audits of your environment to access your level of security.

Enhance Defenses through Controls

Software Safety Controls:

- Implement email filters, web filters, firewalls and other tools or systems to protect end users and the company network from malicious traffic.

- Ensure all software patches are up-to-date and are kept that way.
- Establish a software management strategy.
- Redirect remote users through the secure corporate gateway to limit compromising the organizations environment by those accessing the internet remotely.
- Make use of a network VPN.
- Employ traffic monitoring to easily detect the movement of data across the organization and flag suspicious activity such as mass copying or deletion of files.
- Automate software updates to be sure updates are installed as soon as they are released to prevent vulnerabilities from being exploited.
- Disable Remote Desktop Protocol (RDP) when not in use.
- Logically segment your network and add controls for additional security.
- Disable the use of Macros in office software.
- Make use of an intrusion or malicious detection system to alert you to potential ransomware attempts.

Endpoint Safety Controls:

- Implement a robust software and/or hardware backup solution for all company endpoints that enables backups to be automated to a secure store.
- Ensure backups are kept secure to prevent backups being compromised.
- Backups should be easily accessible to the IT team and restoring data from the secure store should not be overly complicated.
- Data backups should not only be secured but encrypted to prevent data loss and unauthorized access.
- Regularly test the integrity of backups as well as the function of the recovery.
- Make use of Data Loss Prevention (DPL) tools or software.
- Implement the principle of least privilege for all users within the organization.
- Use a tool that enables remote encryption or uses a timer to lock files when inactive or not being used to prevent unauthorized access of data.
- Back up your files using a 3-2-1 backup rule, i.e. retain at least three separate copies of data on two different storage types, with at least one not being stored online.

User Safety Controls:

- Conduct regular penetration tests to highlight weaknesses at user level.
- Automate policy across your organization to ensure user data is continuously being backed up to prevent missing or losing data.
- Provide regular training and communications on the latest ransomware types and how to spot them so users are aware of what to look out for.

Ransomware Response

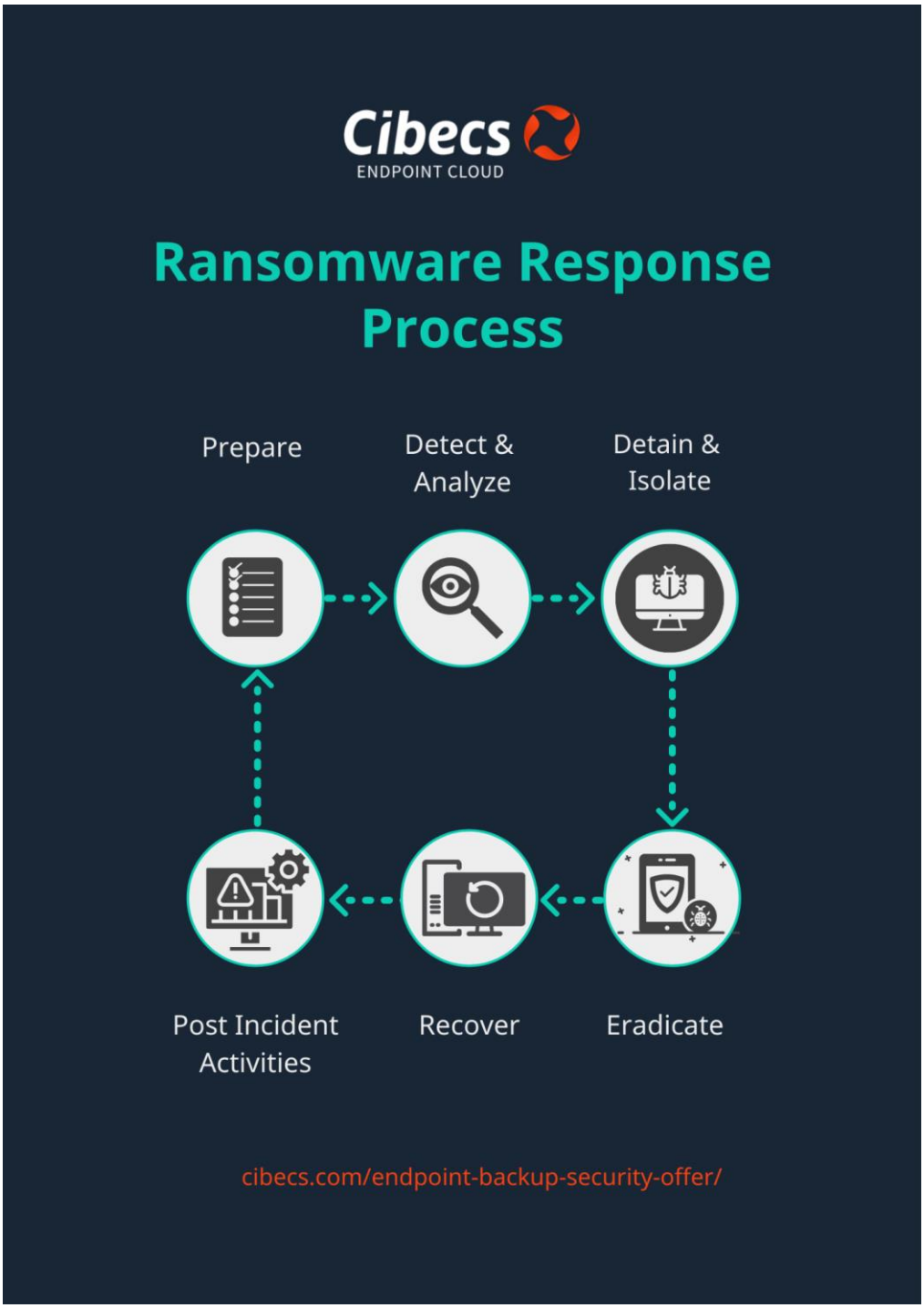
Early Detection Signs

If you know what to look for there are a number of behaviors that can indicate the presence of a ransomware infection, such as:

- **Unusual file system activity**, such as a mass number of files being created, deleted or updated. This is usually the first sign that malicious software has entered a device and is searching for vulnerabilities to spread the infection.
- **Increased CPU and disk activity** that no one understands or can explain.
- **Inability to access certain files**, malicious attackers will often encrypt certain files that they identify as valuable and block user access to this information.
- **Suspicious network activity** is when abnormal or out of the ordinary activity is flagged. This behavior can be anything from strange user access requests, file permissions or data changes or user's being online at odd hours and behaving strangely.
- **Software uninstalls** such as the removal of antivirus or other security software.
- **Active directory access:** many attackers try to access Active Directory as a way to infiltrate the organization's domain and gain control over the entire organization's data or environment.
- **Test attacks**, hackers will often run small 'test' attacks to identify weak spots or vulnerabilities within your network. However, if you have endpoint detection and response tools, they will usually pick up this behavior.

Identifying any form of malicious software in your company's environment is never good news. However, establishing critical controls and putting the right protocols in place can help remove the infectious software before it has time to do any real damage. Therefore, having the skills to identify and recognize the early stages of an attack are crucial to safeguard the organization and its users. Many early warning signs are easily detectable by those who know what to look for and have put the necessary monitors in place.

Ransomware Response Process



- Prepare

  It is imperative that you have the correct mechanisms in place to identify an attack. As mentioned above there are early detection signs a trained IT manager will be able to identify. It is also essential that users know what to look for, this makes users an additional asset to preventing an attack. Be sure to provide users with the process they can follow to report any suspicious activity on their device or network that they have noticed.

- Detect & Analyze

  If ransomware has been detected the next step is to analyze your environment and determine the impact and reach of the malicious software, the strain of ransomware and what version. Once you have this information you can contain the virus and prevent it from spreading any further. However, if you do not know what you are dealing with, taking any actions could potentially increase the spread of the infection and do more harm than good.

- Detain & Isolate

  Once the reach and type of the infection has been established, the infected areas, devices and network segments need to be isolated from the rest of the organization's environment. This will also allow you to activate additional protection controls depending on where or how far the malware has penetrated the organization's environment, user network and devices. After successfully detaining the threat, the IT team will be able to evaluate the infection and establish the eradication options and put together a plan or action that best responds to the attack.

- Eradicate

  Once you've contained the issue, you need to find and eliminate the root cause of the breach. The cause of the breach will need to be removed or the weak spot reinforced, in the case of software weaknesses or network blind spots. All malware needs to be securely removed to prevent reinfection. After the ransomware has been removed a full audit should be done to ensure the entire environment has been secured and all software updates and patches have been performed.

  IMPORTANT NOTE: If any trace of malicious software or vulnerabilities remain in your company systems, you will continue to be at risk.

- Recover

  Recovery and restore processes can commence once the infection has been completely eradicated from the system. If no data was corrupted, you should be able to use a decryptor

to regain access to your data. A better option is to ensure you keep regular, updated backups from which you can restore important data.

During the recovery process be sure to wipe previously infected devices, and format and restore from scratch to be sure that no infected items remain on the device or network as this will cause reinfection.

- Post Incident Activities

  Examine what systems and defenses helped hinder the attack and what didn't. Relook and improve on areas that failed to work. Establish a post ransomware attack meeting and consider the following:

  - Updating ransomware response plans based on what was learnt
  - Auditing defenses, reinforcing, and improving tools used to stop an attack
  - Perform tests to identify other weak areas in the organization's environment
  - Prepare a post attack report for senior management
  - Continue to monitor and improve defenses
  - Report

    Many compliance regulators as well as the FBI require that you notify them of any ransomware attack. To notify the FBI, you can visit their Internet Crime Complaint Center to submit your incident report. Depending on where you are located, your next step should be to inform your local authorities, especially if your region has data protection legislation in place.

    Below is all the information you will need to provide when reporting an attack to the FBI.

    - Date of the ransomware incident.
    - Name of ransomware and the version that was identified.
    - Victims' information such as company name, region, industry and organization size.
    - Attack vector: how the malware infiltrated your organization.
    - Ransomware amount demanded or threat made in the case of leaking information.
    - Attackers Bitcoin or Cryptocurrency wallet information.
    - Amount paid if any (note the FBI does not recommend paying attackers)
    - Damage incurred due to infection - includes financial loss or costs incurred due to the attack and ransom paid.
    - Your statement.

Ransomware Response Checklist

Immediate Response

- Switch off device's wireless functionality.
- Disconnect and isolate the infected device from other devices as well as the network.
- Turn off infected endpoint device/s only in the case that the device is unable to be removed from the network to avoid further spread of the ransomware infection.
- Remove infected devices from shared drives.
- Disable shared drives.
- Secure & isolate backup data if they are not kept in a separate store.
- Change all passwords.
- Issue an organization-wide alert to make everyone aware of the attack and next steps.

Analyze, Identify and Control

- Determine the spread of the infection through identifying the number of infected devices and what data has been compromised.
- Identify the type and version of the ransomware used to attack the organization.
- Identify the mechanism, tactic and channel used to infiltrate the network or end user device.
- Establish the root cause or 'patient zero' within the environment.
- Secure and try to prevent further vulnerabilities.
- Establish whether a decryption tool can be used to regain access and secure data impacted by the attack.
- Check logs to check for any data leaks.
- Search your environment for malware, software, crips and files that could have been copied.
- Identify and prioritize critical systems for restoration and recovery based on the assessment of the attack.

Determine Remedy Options & Implement

Once scope of the attack has been determined there are a few response options.

Response Action 1: Restore & recover data from backup

- Locate backups
    - Audit backups to establish what data is and is not there.
    - Establish the integrity of backups.
- Rebuild the system utilizing non-impacted or infected sources of data.
- Reinstall programs and software from scratch, ensure all patches for software are up to date. Do not trust anti-virus to completely rid your devices from malicious software.

- Assume all passwords and credentials have been compromised and recreate them. (This includes those in a password manager or web browsers).
- Locate and remove the cause of the attack. I.e., phishing email, attachment or corrupted files.
- Report the attack.

Response Action 2: Try a decryption tool.

- Once you have established the strain and version of ransomware, search online to see if a decryptor is available for the ransomware.
- Backup all your data before utilizing the decryptor in case this process does not work.
- Decrypt files.
- Backup restored files.
- Rebuild environment utilizing unimpacted or restored sources. Be careful to not reinfect the environment. Reinstall all software along with the latest patches. Do not trust anti-virus to completely rid your devices from malicious software.
- Assume all passwords and credentials have been compromised and recreate them. (This includes those in a password manager or web browsers).
- Locate and remove the cause of the attack. I.e. phishing email, attachment or corrupted files.
- Report the attack.

Response Action 3: Don’t do anything (lose files)

- Remove ransomware. Do not trust anti-virus to completely rid your devices from malicious software.
- Backup encrypted data and store separately until a decryption tool for the type of ransomware becomes available. (optional)
- Rebuild environment utilizing unimpacted or restored sources. Be careful to not reinfect the environment. Reinstall all software along with the latest patches.
- Assume all passwords and credentials have been compromised and recreate them. (This includes those in a password manager or web browsers).
- Locate and remove the cause of the attack. I.e. phishing email, attachment or corrupted files.
- Report the attack.

Business Continuity Measures

- Keep a log of all systems and endpoints that are unaffected by the attack to exclude them from the recovery.
- After it has been established that the environment is once again secure be sure all passwords are reset and the weak spot in the environment has been reinforced and secured.
- Restore files from the backup store to new devices or newly secured machines.

- Conduct an organization-wide analysis of the company's detection and prevention systems and establish which need to be improved to prevent the incident from happening again in the future or to be better prepared.
- Record the incident, identify weak points and update contingency plans, policies and procedures to prevent future incidents.
- Implement a business continuity and disaster recovery plan (BCDR) that includes backing up critical data and regularly testing the restore process.
- Utilize a ransomware prevention checklist to help mitigate future attacks.
- Only pay the ransom as a last resort. However, you should consider the following factors (1) the FBI advises against this, (2) data is not always restored once ransoms are paid and encourages repeat attacks. (3) The US Department of National Treasury's Office of Foreign Assets Control (OFAC) states that paying a ransom is a potential violation of their regulations and could result in fines.

Ransomware User Education Communication

User ransomware awareness and understanding is essential to protecting an organization's environment and users. The reason for this is human error is usually the cause of a breach. Attackers exploit user weaknesses or lack of understanding to gain access and infiltrate organizations' sensitive information. However, if your users are informed, they can act as your first line of defense when it comes to malicious attacks.

Below is a simple user guide on the 8 Steps to protect yourself from a ransomware attack that can be distributed to your users.

8 Steps to Protect Yourself from a Ransomware Attack

Ransomware is a sophisticated, malicious type of malware that blocks access to your files or computer until a Ransom is paid. The best way to protect yourself is by being prepared.

Step 1: Be Cognizant of Unsolicited Emails

DON'T open an attachment in an email that seems suspicious. To effectively safeguard yourself, don't open any attachments or click links in emails from unknown sources.

DO Go into your settings and unhide or 'Show Extensions' so that you can monitor the file types of all sent email attachments. Be very cautious of the attachments you choose to open.

Examples of Common Email Ransomware Carriers:

- Any unsolicited email that asks you to enable a Microsoft Office feature called macros.
- An email from an unknown person or company with an invoice attached.
- Any email with details regarding an unexpected payment into your bank account.
- An email from your bank requesting that you enter your details, enter their website, or any page, from a link contained in that email.
- An email from a tax association regarding either a payment into your account or a payment due that requests you download any file or directly click on a link.

Step 2: Think Before You Click

DON'T click on suspect adverts or links, even if they are hosted on trusted websites. Malvertising is on the rise so avoid suspicious links, ads and websites.

DO Google Search the product or service if you are interested in finding out more.

Step 3: Don't Talk to Strangers

DON'T open unsolicited messages in any messaging service (including Skype, Facebook, Twitter etc.) without thinking twice. The old adage of not talking to strangers applies, if you don't know the person sending it, rather don't click on it or open it. It might be a virus.

DO make sure your privacy settings on all your social media and messaging accounts are up to date and secure.

Step 4: Always Have a Backup

Most importantly, and the only bulletproof protection from being held Ransom, is making sure you have a recent backup of all your files. This means you are never at risk of losing your data and having to pay a Ransom to get it back.

DO speak to your IT Department about Cibecs, the best endpoint data backup and complete data protection solution for businesses.

Step 5: Stay Up to date

DON'T delay or disable your OS or AV updates and never expect users to perform updates on their own.

DO ensure you run prompt software update policies which can be centrally managed and enforced to all devices on the network.

Step 6: I Hear You Snowden!

DON'T think that simple, more convenient passwords are more sensible in terms of productivity, through reasoning such as "you trust the people you work with" or "I'm simply not hiding anything or it's not important enough". Ransomware tools are designed to exploit any vulnerable device, regardless of who you are, and they ransom your data, and they will use your device to spread further.

DO ensure you have strong password policies enforced to avoid exploits through remote protocols such as SMB or RDP.

Step 7: Sharing Isn't Always Caring

DON'T hesitate in switching off or disconnecting your infected device immediately. The longer the device is online the higher the risk of it scanning and sharing its nasty self.

DO switch off the device or disconnect any Wi-Fi or Lan connection and keep any removable media such as USB drives and flash disks connected to the device away from other devices.

Step 8: Don't Bring a Knife to a Gunfight

DON'T rely on sync or backup tools which utilize SMB shares, even in cases where the SMB exploits are patched a share may be legitimately available to the devices, where it may spread itself and infect other devices sharing from the same server.

DO use the right backup solution, such as Cibecs which offer:

- Centrally managed and automated backups, your users must not be expected to do anything!
- Secure backup protocols, such as SSL.
- Encrypted data at rest, meaning data backed up is isolated and contained so even infected files will not spread to other user's backups.
- Point in time recoveries, allowing you to recover all files or even a single file as it was at a point before infection. Sync tools typically only offer this on a file-by-file basis meaning I.T. can spend hours, possibly even days trying to recover a single user's data.

Compliance Considerations

Organizations need to understand that if personally identifiable information (PII) is affected, lost or stolen in an attack they may be required to notify the relevant regulatory body within their location, depending on which privacy laws govern the jurisdiction in which they operate (e.g., EU's General Data Protection Regulation, The California Consumer Privacy Act).

Bearing this in mind it is essential that your organization fully examines the impact of an attack and makes a list of impacted personal data. Once this has been done your organization needs to notify the relevant parties, however, it is essential that communications are unified to prevent further damage to the organization and its reputation.

This highlights the importance of compliance to data protection and privacy laws, as if those impacted can prove that an organization was not compliant at the time of the attack the company may face additional losses in the form of fines and legal action.

Post Ransomware Communications Considerations

In a case where sensitive company data is leaked, missing or stolen those whose information was impacted will need to be notified as well as the regulatory body that governs data privacy laws in your location.

Below is a list of what to consider when engaging in external communications after a ransomware attack.

- **Present a united front and ensure all company communication is consistent**. This is crucial especially in scenarios involving sensitive or personal information. Consider involving a qualified Public Relations Officer (PRO) to help with the communication post ransomware.
- **Centralize decision-making.** Depending on the extent of damage caused organizations should consider establishing a communications committee to ensure there is a clear plan of action and guidance on the way concerns from customers or those impacted by the breach are responded to.
- **Regulatory & compliance obligations.** After the attack the organization will need to establish the extent or impact of the attack and if it is severe enough that it is required to be reported to the authorities.
- **Contractual considerations.** Depending on the nature of the company's work, contractual agreements with clients, suppliers and other key stakeholders will need to be examined to see if a breach of contract has occurred due to the attack. If data relating to these stakeholders has in fact been impacted, they will need to be notified.
- **Contacting law enforcement or notifying the government.** Depending on the severity of the ransomware event some businesses may contact law enforcement or regulatory bodies about the breach.

Regardless of the impact of the attack or the established remedies, all communications should be coordinated and remain consistent to ensure no further damage is caused to the organization, its reputation or stakeholders post the ransomware event.

Additional Considerations for High-Profile Organizations

Depending on the profile of the organization affected as well as the severity of the ransomware incident there may be additional factors that need to be managed to not impact the profitability and longevity of the company any further.

- **Internal processes, protocols and procedures.** Regardless of how high-profile an attack, companies should follow the established contingency plans and process. Auditing, documenting and reporting is essential to prevent future attacks and maintain corporate governance.

- **Intellectual property considerations**. Ransomware attackers can compromise a company's IP and can result in stakeholder's proprietary information being stolen. It is important to consider and check what is missing and establish solutions post attack.

- **Litigation risk**. Companies need to establish the risk of legal action post attack and the implications of said legal action on the organization's longevity and bottom-line.

- **Stock trading blackout period.** In order to safeguard a company's reputation post attack. Some organizations may consider a stock sale blackout period to prevent key insiders from selling company stock/ shares - this usually includes those involved in the incident response team.