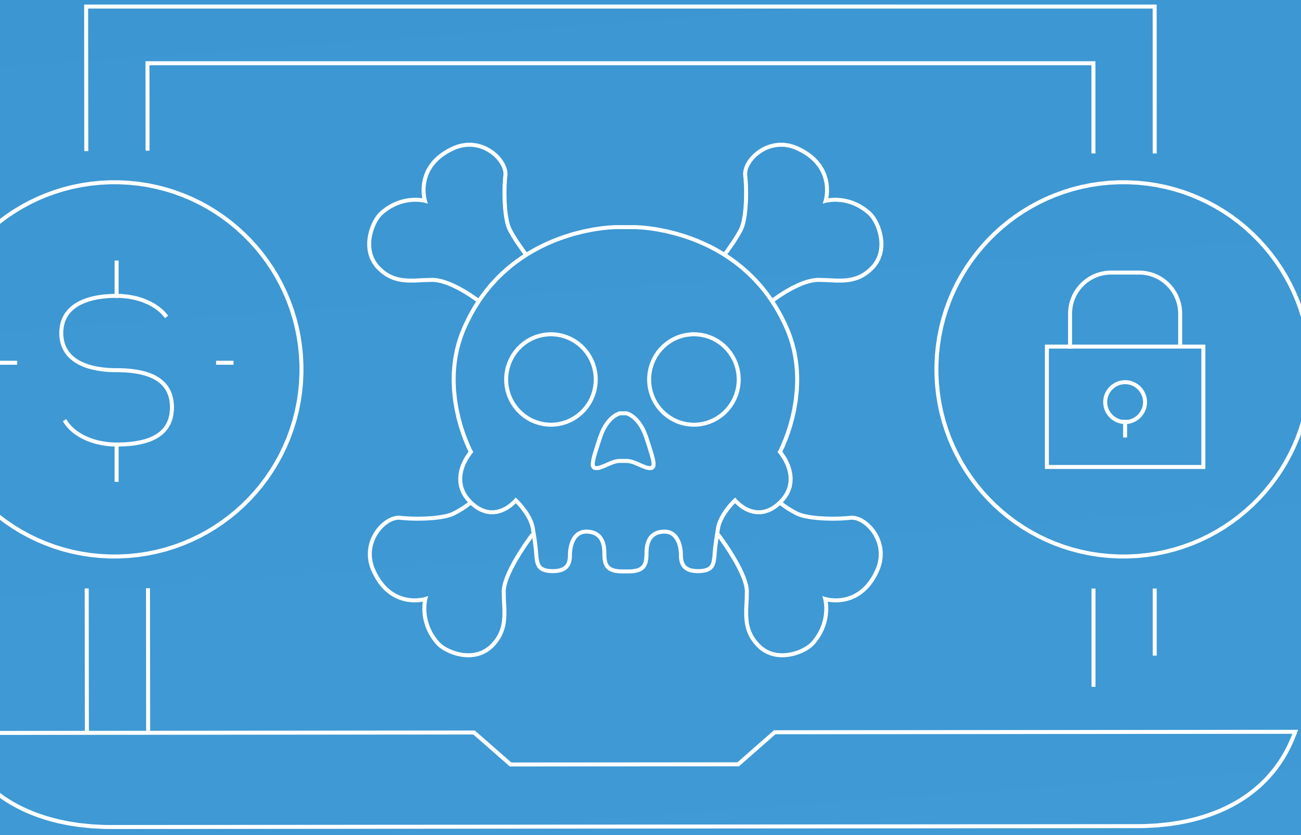
schellman
Quality, above all.

Schellman's CSET Ransomware Guide

Contextual help through CISA's checklist



Overview

Ransomware continues to rapidly evolve and is designed to encrypt files on a system or endpoint, rendering that data unusable. Threat actors then demand a ransom in exchange for the decryption mechanism. These criminals have threatened to sell or leak data that has been exfiltrated unless the ransom is paid, and sometimes will do this anyway once the ransom is paid. While tactics continue to evolve, there are some basic, intermediate, and advanced activities that organizations can implement to prepare themselves for the ransomware incident.

This process that you have undertaken to gather data points about where your organization stands with respect to this evolving threat is a great step along the path of cybersecurity posture maturity. The intention behind collecting the data points in the following questions is to boil-down complexities of ransomware preparedness into actionable information suitable for executive-level sponsorship of your organization's cyber risk mitigation strategies. In short, for this process to be successful, the better the inputs, the better the outputs.

Instructions

Read each statement and include a checkmark if that statement is true. Ensure that your responses are indicative of the current status of the organization or business units' cybersecurity program.

1. Yes: the organization or business unit **fully performs** the activity specified in the statement
2. No: the organization or business unit **does not perform** the activity completely

Data Backup

The core attributes of ransomware are that ultimately an attacker gets in and they identify critical data and they encrypt it in such a manner that you you can't get access to it until you pay them to decrypt it (until you pay the ransom).

The most important thing related to ransomware preparedness is: do you have a backup and a backup that is separated from the environment? So that if an attacker was able to get into the network and they were able to encrypt sensitive data that you have got an independent backup of it sitting somewhere. That is key to have a backup that can go back to for at least 30 days.

- □ Important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days.

Do you do at least an annual restoration process where you simulate a disaster or some sort of attack that's occurred and you have the means to go back to your backup and show that you can, in fact, restore that data to a new environment.

- □ Data backups are tested at least annually.

Web Browser Management and DNS Filtering

These attacks typically come in through phishing attempts to get you to click on a particular malicious link and or go to a particular page and enter authentication credentials or other types of information that would allow the Attackers to get into. to get into the network.

A lot of this starts at the web browser and so making sure that your web browsers are configured, are updated, and configured to potentially block malicious traffic (no malicious traffic), DNS filtering when you have sites and links that an attacker may point you to that are meant to look like a legitimate site but are not, in fact, a legitimate site.

Web browsers are one of your first points of protection to be able to identify suspicious links and suspicious sites that the attacker may be attempting to redirect you to.

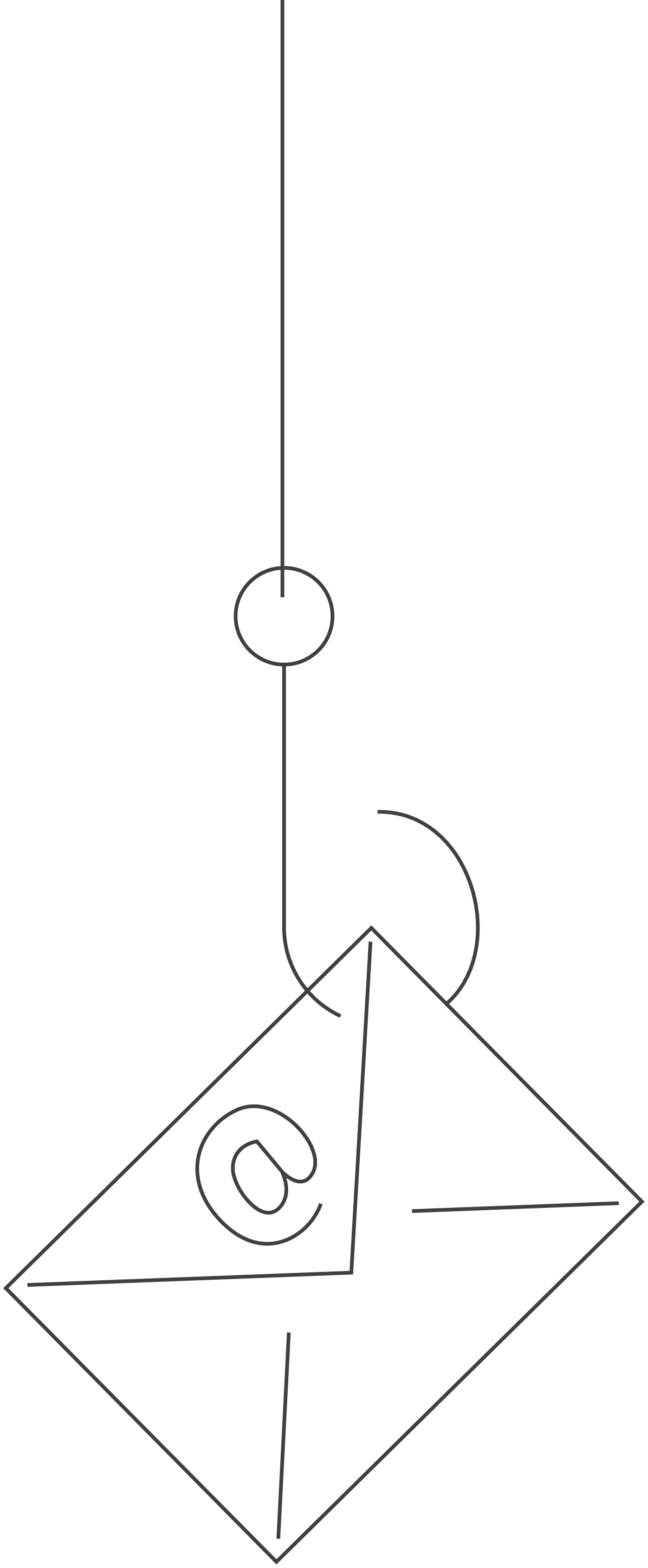
- □ Malicious web content is being blocked using DNS filtering via methods like DNS resolvers and DNS firewalls.
- □ Web browser security settings are managed.

Phishing Prevention & Awareness

Phishing is probably the most common means for a ransomware attacker to get into a network—sometimes they'll use a malicious email of some sort, or they may even get in via text. Your user base needs to understand that these attacks are out there, and by and large, a lot of people are aware already. But you should also understand that these attacks can occur in a very surgical manner—an email or text may appear incredibly legitimate like it's coming from a company, a partner, or someone with whom you do business.

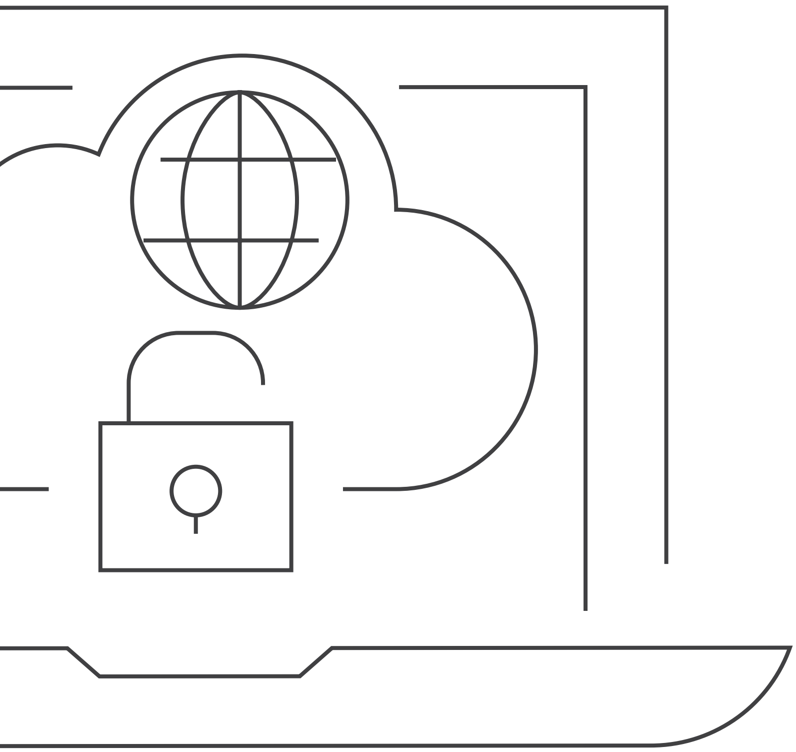
Therefore, increasing phishing prevention and awareness means testing your users regularly to see if they identify suspicious emails—this will make them more cognizant. Instill a culture that will have everyone asking questions when an email comes in that appears to have some issues associated with it.

- □ Annual tabletop exercises that include phishing response scenarios are conducted
- □ Users are trained to recognize cyber threats like phishing.



Once your employees are educated, you can also make things simpler for them by using email filtering software—tools like Mimecast and others will screen email that comes in, identify the phishing attempt, and say, "hey, this is not what it appears to be."

- □ Email is filtered to protect against malicious content.



Network Perimeter Monitoring

Network perimeter monitoring can help in a similar way, but how you approach this will depend on the degree that you manage your network or if you've outsourced to cloud providers.

If you have a set of assets within your control of your network, you need to make sure that you are guarding and monitoring perimeter traffic—use firewalls, intrusion detection mechanisms, and the like. To supplement these tools, you also need to understand the types of traffic that you expect to come in and out of your network. Is it web? Is it connection? Is it VPN? Something else? Make sure that you're restricting traffic to those particular types of services.

This understanding will allow you to more easily monitor that traffic for anomalies and things that shouldn't be happening.

- □ Perimeter network traffic is monitored.
- □ Internal network traffic is monitored
- □ Networks are segmented to protect mission critical assets.
- □ The organization has established a baseline of network traffic and is it used to identify anomalous activity.

Asset Management

NISTIR 8374 is a very good resource for ransomware preparedness, and within that, asset management is a key component. You need to understand:

- Where your assets are
- Where your sensitive data is
- Where it is in your network
- How does the data flow

You can start to answer all of these questions by first listing all your hardware and software assets. With that inventory, you can then determine where the data resides and remove unsupported or blocked items from that environment. From there, you can discern your relevant processes in dealing with anomalies among these assets, including introductions of new hardware or software, quarantining rogue items, securing configurations, etc.

□ The organization's hardware and software assets have been inventoried and is the inventory managed.

□ The organization has removed all unsupported hardware and software from its operating environment.

□ The organization detects rogue hardware and alerts key stakeholders.

□ The organization quarantines and/or removes all rogue hardware.

□ Documented and approved secure configurations are used to manage the organization's hardware and software assets.

□ Standard baseline images are used to control hardware and software configurations.

□ The organization manages system configurations using security hardening guides.

Patch and Update Management

Once you've got your asset management approved, you also need to check how you're maintaining those assets to make sure that they're up to date. You don't want to fall victim to this common scenario: an attacker comes in by way of a phishing campaign, gets into a system, and finds a vulnerability created through either misconfiguration or a lack of the latest security patches. They're able to then exploit the system before jumping around to other vulnerable systems as well.

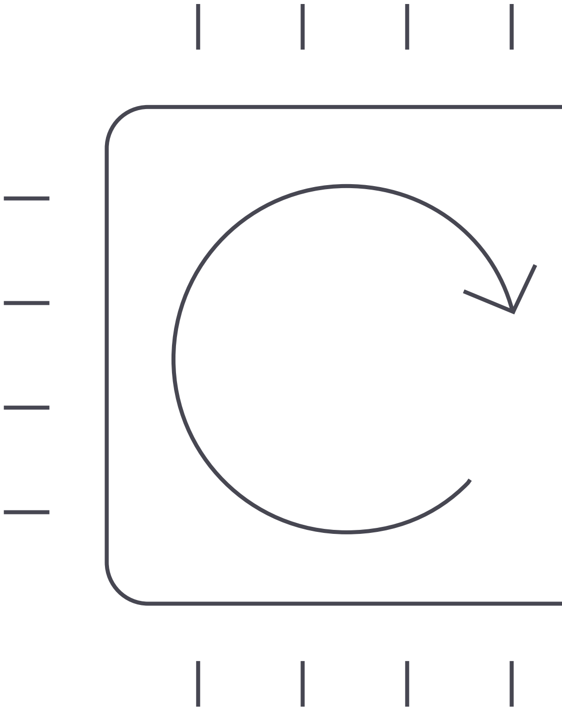
You must not only make sure that your public-facing systems are patched but also that your internal-facing systems are too, including all of your internal network and system components. Patching must also happen timely—you need to understand how many days it takes before you typically patch something when the data involved is sensitive.

□ All public-facing software is patched for vulnerabilities within:
- 15 days for vulnerabilities rated as "Critical"
- 30 days for vulnerabilities rated as "High"

□ All internal-facing software and firewalls are patched for vulnerabilities within:
- 30 days for both vulnerabilities rated as "Critical" and for vulnerabilities rated as "High"

□ All software and firewalls are patched for vulnerabilities within:
- 15 days for vulnerabilities rated as "Critical"
- 30 days for vulnerabilities rated as "High"

□ All software and firewalls are patched for vulnerabilities within:
- 3 days for vulnerabilities rated as "Critical"
- 7 days for vulnerabilities rated as "High"



User and Access Management

Here's where you need to consider what you've implemented to control access—strong and unique passwords, unique identifiers, and multi-factor authentication. Do you have different levels of privileges for your staff? How do you enforce these differences so that only people that are permitted access to particular data systems are granted access to those to those applications?

To go with these different privileges, you should also be conducting role-based security training so that those with more access understand their responsibilities as well.

Your environment should not be completely open, but moreover, you should be logging the access of privileged accounts—you need to know when and what sensitive data is being accessed, not just who is accessing it. That also includes detecting any rogue hardware should a new device be plugged in or a new application introduced. In-depth tracking of this nature will help you in the event that you need to trace back what happened.

- ☐ Strong and unique passwords implemented throughout the entire organization.
- ☐ Two-factor authentication implemented for all privileged (e.g. system administrators) and remote users.
- ☐ Two-factor authentication has been implemented for all users.
- ☐ The principle of least privilege is enforced through policies and procedures.
- ☐ The principle of least privilege is enforced through technical (technology based) restrictions.
- ☐ Audit logs are maintained for all privileged (e.g. system administrator) accounts.
- ☐ Role-based security training is conducted.
- ☐ Rogue hardware is being detected.
- ☐ Users who attempt to install rogue hardware are counseled against installing rogue hardware.

Application Integrity and Allowlist

You may know this as whitelisting instead, but there may be a specifically identified list of applications that your organization allows/needs to run from a business perspective. But what you need to ensure is that anything that is **not** explicitly allowed is denied.

If you do not already have such a documented list of approved applications, you should create one that also includes both how you're managing those applications and how you're denying applications that are not on that particular list.

- □ There is a list of known bad software (a "Blocklist"), and the software on that list is being blocked.
- □ The organization has documented a list of known approved software (an "Allowlist").
- □ The Allowlist is organized by a software publisher, and that list is used to allow only approved software to run on organizational systems.
- □ The organization has documented a list of known approved software (an Allowlist) organized by a software publisher and version number, and that list is used to allow only approved software to run on organizational systems.

Incident Response

This is another key tenet of ransomware protection—you need to establish the capability to respond to an event if it occurs. Your incident response plan should be multi-faceted, with different types of procedures to guide users and personnel when something occurs, including disaster recovery—if data becomes unavailable, do you have/understand the procedures to retrieve your backups and recover accordingly?

Not only should you have a plan in place, but you should also test it through different types of tabletop exercises (and physical incident response exercises as well, if you manage data within your physical premises).

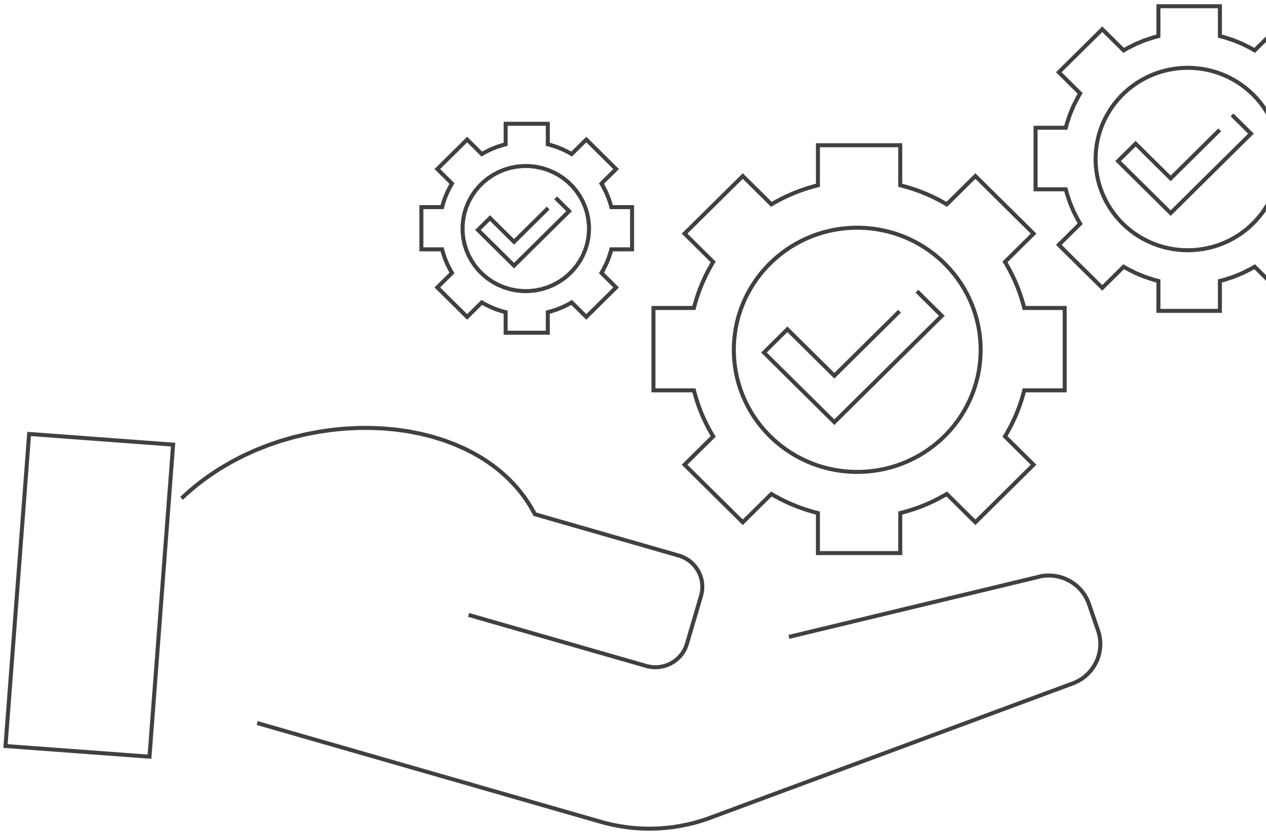
- □ The organization has developed an incident response plan.
- □ Cybersecurity incidents are reported and escalated to the appropriate stakeholders.
- □ Disaster recovery procedures have been developed.
- □ The organization conducts annual incident response tabletop exercises that include ransomware response scenarios.
- □ A physical incident response exercise is performed at least once a year.
- □ A physical incident response exercise is performed at least twice a year.
- □ The organization has implemented redundant systems where appropriate for the purpose of resiliency.

Risk Management

Similar to Asset Management, this is also heavily hit within the NIST standard. You should consistently perform business impact assessments on critical assets and document the criteria used. Your risk tolerance is critical to your security posture, and to be fully informed, you need to track your risks and understand any data capture that's happening.

You should evaluate not only your systems, but also any interconnected ones provided by third parties—cloud services to connect with partners, and so forth.

- □ The organization performs business impact assessments.
- □ The organization has defined organizational risk criteria and tolerances.
- □ The organization considers risk inheritance and exposure between its various interconnected systems.
- □ The organization applies quantitative risk analysis to remediation activities.



schellman
Quality, above all.

Contact Us

To see how Schellman can help your organization with a full Ransomware Preparedness Assessment based on your responses here you can reach out to our team directly.

866.254.0000 | schellman.com