2022 Ransomware Preparedness Guide

How to Better Prepare and Protect Your Organization Against Ransomware

Quorum®
1-Click Instant Recovery

TABLE OF CONTENTS

INTRODUCTION

To say ransomware attacks have surged dramatically is an understatement.

Check Point Research saw a 41% increase in attacks in the first half of 2021 and sees a 93% increase year over year,[1] whereas SonicWall noted a 151% year-on-year increase in ransomware attacks in its 2021 Cyber Threat Report.[2]

The average ransom also increased dramatically. The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020, according to National Security Institute.[2]

In 2021, the largest ransomware payout was made by CAN Financial, an insurance company, at $40 million, setting a world record.[3]

Even the Biden Administration took notice. In Biden s Executive Order on improving the Nation s Cybersecurity, the White House informed the public that the government has stepped up efforts to stop ransomware attacks.[4]

Nowadays, being attacked by ransomware is not a matter of if, but when.

In this guide, you will find the basics and groundwork on how to prepare for a ransomware attack. The guide covers people, process, and technology, and how to leverage all three to prevent, detect, and mitigate ransomware.

If you wish to dive deeper into a specific area in this guide, feel free to contact us at info@quorum.com. Quorum backup and disaster recovery solution has helped 100+ companies successfully recover from ransomware, and we are happy to share those experience with you.

1. *Ransomware attacks continue to Surge, hitting a 93% increase year over year.* https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/
2. *The Growing Ransomware Wave.* https://www.nsi.org/2021/02/15/employee-cyber-security-awareness-ransomware-wave/
3. *One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack.* https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5
4. *Executive Order on Improving the Nation's Cybersecurity.* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

01 Employees are the First Line of Defense

Your employees are a doorway into your organization s network. Education about ransomware and cybersecurity is the lock against cybercriminals.

Emplo ee Awareness Can Help Prevent Ransomware Intrusions

The regular target of a hacker is an individual, because you and your employees are a doorway into your organization s network. Cybercriminals know this, and they employ social engineering and phishing to get the keys through that doorway.

According to the FBI,[5] phishing was the most common type of cybercrime in 2020 and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019, to 241,324 incidents in 2020.

To help minimize this risk, employee awareness and training is essential. Below are 5 ways to help you and your employees minimize this risk:

5. Internet Crime Report. FBI.
https://www.ic3.gov/Media/PDF/AnnualReport/2020_C3Report.pdf

1. Train Employees to dentify Phishing Attempts

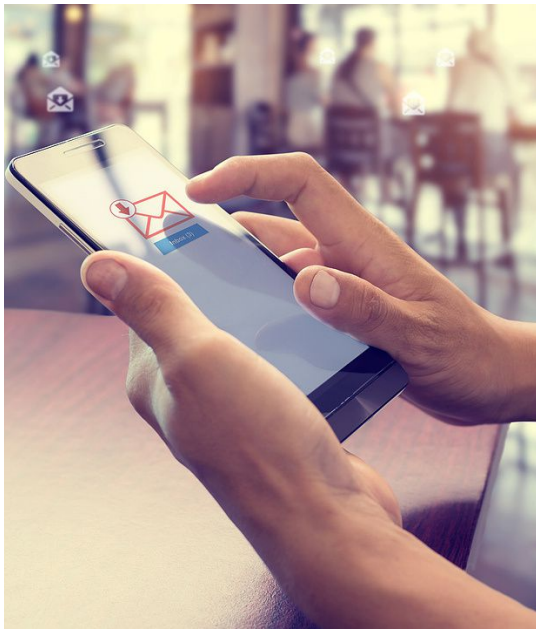
Many ransomware attacks gain entry from phishing and spear-phishing to steal login credentials. Other times, these attackers use names of your fellow employees to send emails containing malware or links to malware infected websites. Employees should learn to look at the sender s email address and not just the name of the sender. If the email contains a link, employees should also learn how to check where the link goes without clicking it. The act of empowering employees with knowledge of how email phishing and spoof websites can help them identify and stop a ransomware attack at its starting point.

2. nstruct Employees to Report Suspicious Emails mmediately

If employees immediately report and forward suspicious emails (usually to the IT or security team), the IT or security team can send a company-wide email notifying everyone to identify and delete the phishing email. Even when an incident happens when an employee opened an email and entered credentials into a spoof site, timely action can help mitigate the threat and stop the incident from a ransomware infection.

3. Educate Employees on Suspicious Email Attachments

Employees must also learn not to open attachments unless it is from a legitimate source, where the sender s email address is correct and is of a trusted person. One example of ransomware delivery via email attachment is invoice scams. The email looks like it is from a colleague or business associate. The email attachment contains an invoice, typically in a PDF, Word, or ZIP file format. When the file is opened, the malware code will execute and infect the machine.



4. Make t a Rule Not to Reuse Passwords

Sometimes, passwords are stolen without notice until a cybercriminal starts using it. Weak, reused, and stolen credentials are sometimes available on the dark web and are behind 61% of hacking-related breaches, according to Verizon s 2021 Report.[6] When cybercriminals purchase these passwords, they usually start using bots or automation tools to test which accounts they can gain access to.

5. Only Download Files from Verified and Known Sources

A tactic known as drive-by-download is used by cybercriminals to have the user unintentionally download malicious code onto a device. These attacks look for vulnerabilities in browsers and other software on the device, which is then exploited to install ransomware. Though your security team can create download and software update rules on company devices, employees should also be trained to recognize the dangers of drive-by-downloads.

Pro Tip

All employees should receive at least one ransomware awareness training. However, it is quite common for people to forget as time passes. A tried-and-true approach is to have the security team send regular monthly or quarterly reminder emails reminding them to be vigilant about spotting and reporting phishing emails, as well as other security-related best practices. This will help refresh the memory of the ransomware awareness training. It is equally important to revisit training annually at a minimum.

6. DBIR, 2021 Data Breach Investigations Report. Verizon.
https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

02 Tools & Best Practices to Prevent & Detect Ransomware

Besides employees, what are other doorways to your organization s network? How do you secure them and find out if you re infected by ransomware?

Ransomware Prevention & Detection Tools

Endpoint Protection

Endpoint protection can be used to prevent malware from executing its code on the endpoint, such as the employee s computer or mobile device. Endpoint protection typically requires a small agent program to be installed on the endpoint device and operates similar to an anti-virus software. When a suspicious file is detected, the file will be uploaded to a quarantine zone for further analysis before they could be executed. Endpoint protection is great for preventing infection from email attachments.

Vulnerability Scanner and Patch

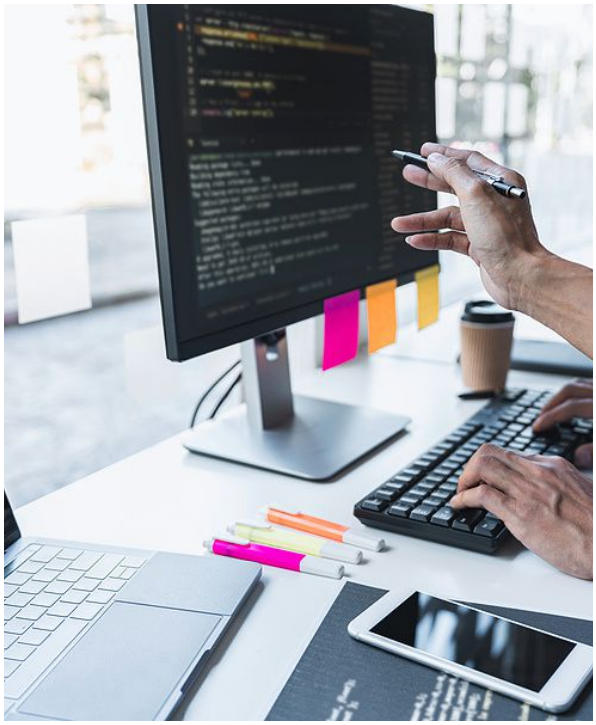
This method detects entry points where cybercriminals can potentially gain access to. This tool first discovers all the devices connected to the network and then scans each in order to compile software inventory. The scanned results will list all the software versions of each device and will notify system administrators to apply the patch to outdated versions, effectively shutting down potential entry points that can be exploited by cybercriminals.

Ransomware Rollback

This is used for ransomware detection instead of prevention. Tools that have ransomware rollback monitors the files within a system and keeps track of what program or process applied changes to each file. When changes were made to files, such as being modified, deleted, or encrypted by malware, this tool can be used to reverse that encryption. This is must be used in conjunction with the organization s data backup.

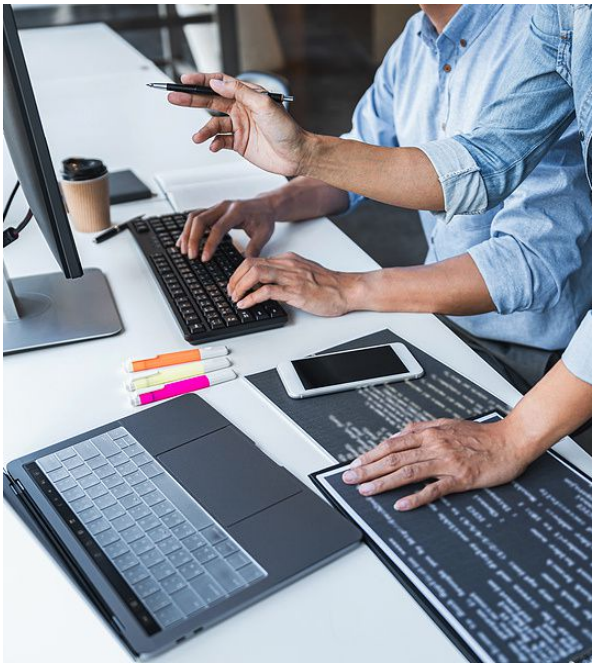
Network monitoring

This tool is used to enhance access management by privileged users and admins. It monitors when the privileged accounts are used, how they re used, and from where. It typically alerts the relevant administrator when a forced access attempt occurs. Some of these tools even automate a response that blocks access and disable accounts when the system thinks the account is compromised.



Conduct Regular Network Penetration Testing

This practice is best performed by third party experts as a method of searching for vulnerabilities in your systems and network, simulating a cyber-attack on your network. It is a way to trying to find entry-points into the system to see where the weakest points are. It is looking into the cybercriminals playbook and trying to make sure you are ready for the oncoming attack.



Conducting regular penetration testing against your network forces your security team to learn real-life experiences on new ways cybercriminals are exploiting company networks.

The goal is to uncover network weaknesses, outdated security policies, insecure system settings, bad passwords, software bugs, configuration errors and more, so that the security team can make the proper adjustments to harden network security.

Importance of Installing the Latest Patches & Software Updates

Whenever new software rolls out, hackers need time to discover a bug in that software that can be exploited to allow the execution of malicious code. Typically, the software vendor and the hacker are racing to discover this bug. If the software vendor discovers it first, the vendor will release a patch or update to fix the bug. If the hacker discovers it first, countless software users will have to fall victim before the software vendor releases an update.

Even if an update is released, there is always a period of time where the software end-user is vulnerable. The user might not update the software because they don t have the habit of updating it, are unaware of it, or constantly hits the remind me later button. That is why this responsibility sometimes falls onto the organization s security team.

Pro Tip

At Quorum, our security team regularly sends out email notifications informing employees to update their browsers whenever a new version comes out. The email notification has proven to be highly effective, where 83% of employees who previously didn t update their browsers ended up updating it within 1 day of the email.

03 Backup & Recovery: Your Last Line of Defense

Restoring your data from backups can be the most reliable way to recover against ransomware. However, how you backup your data matters.

The 3-2-1 Backup Rule is a Great Practice, But Not Bulletproof

The 3-2-1 backup rule is a practice to have at least 3 copies of your data across 2 media types and one copy being offsite. Having multiple backup copies in different locations ensures that you have at least one copy you can recover in the case of a ransomware attack. For instance, you can have a backup in your office, one in an offsite storage space, and another on the cloud. The best approach for this is using snapshot backup at regular intervals throughout the day at a disaster recovery location. This way, you can easily recover data from a ransomware attack on your servers.

The reason why 3-2-1 backup approach is the preferred way to protect against ransomware is because with varied locations and forms of storage, a ransomware attack on one media type or location should not affect the backups on other locations.

Unfortunately, cybercriminals have adapted and adjusted their ransomware attacks to compromise networks even with the 3-2-1 backup approach. Ransomware now lie dormant on network for weeks or months, spreading to as many systems as possible, even to the backups that are offsite. The longer the ransomware lies dormant, the more chances it has to infect multiple snapshot intervals of the backup. That means even when backup copies are restored, the same ransomware file that was backed up can detonate all over again. Though the 3-2-1 backup approach is a great backup method, it is not 100% bulletproof against ransomware attacks.

Can Ransomware Encr pt Your Backup Files and Snapshots?

As opposed to lying dormant in backup snapshots, some ransomware strains target and encrypt your backup files. When ransomware infects a network, it spreads to every discoverable device on the network. That means even local backups on the network can be infected. If an infected user has access to a certain backup location, those backup files are likely to be encrypted as a result.

Some ransomware strains can even extend to connect USB and network storage devices, encrypting the files stored in those devices. In some cases, the ransomware can encrypt the files stored on the cloud even those stored on Dropbox, Google Drive, or One Drive. If automatic syncing is turned on and without file versioning, encryption of those files will be synchronized on all devices, effectively worsening the situation.

That is why you should NOT to use cloud-syncing service as your only backup. Instead, a data backup and disaster recovery solution should be implemented where the backup snapshots are immutable and provide an air gap to your data from the network. Even a virtual air gap where the storage is not accessible from the network except under strict circumstances provides a great security model against ransomware. Along with immutable and air-gapped backups, the backup solution should not rely on Active Directory or DNS, thus making its presence harder to discover and minimizes another ransomware attack vector.

Testing Your Disaster Recover Plan is Critical

Regular testing data restorations is absolutely essential to ensure that your data can be recovered intact. You might have a solid plan in place, but many issues can arise to derail that plan. These issues can include miscommunication, technical glitches, and software version updates and compatibility. Sometimes, missing even one critical piece of data can result in errors in restoring your data. Regular testing is the only way to uncover and fix these issues.

It is important to define recovery as getting everything back online so the organization can conduct business as usual. Recovery should not mean that the company is operating at a degraded state, where processes are extremely slow or faulty. Sometimes, this comes down to how robust your backup appliances are. If your backup appliance has the capacity to operate as production servers, then this is usually not an issue.

There is no universal answer to how frequent you should test. To be safe, testing frequency should be based on how much downtime an organization can afford. If the organization can afford days of downtime, testing once or twice a year could be fine. If the organization cannot afford an hour of downtime, then disaster recovery testing should be much more frequent.

Pro Tip

When evaluating your ransomware preparedness, check to see if your backups are immutable and cannot be encrypted. You should also check whether your disaster recovery solution is robust enough to operate as production servers when you clean up your production servers from ransomware infection.

04 Ransomware Incident Response Plan

You know that you organization is infected with ransomware. Now what?

Responding to a Ransomware Attack

If you have an incident response plan specifically designed for a ransomware attack, now is the time to execute it. If you don t have one, below is a general guideline:

Detection

In most cases, detection is when an employee finds it impossible to access files, receive a ransom note, or notice that certain services are no longer accessible. At this point, time is of the essence. All known infection must be identified and isolated to prevent the infection and encryption from spreading. If you can find the infected host, take it offline. At the same time, monitor other devices closely to see if there are more than one infected host.

Analysis

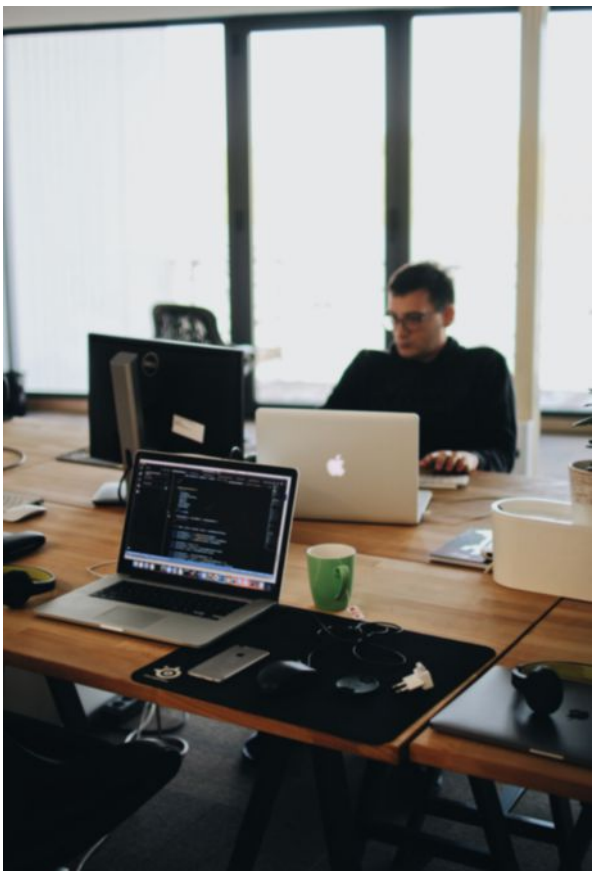
At this point, your goal is to identify the specific ransomware variant that you re infected with. Each ransomware has different capabilities, so knowing its capabilities will clarify what steps are needed in the containment and eradication phase. You will have to identify the root cause (email, drive-by-download, browser, others) and will likely have to consult with a subject matter expert.

Containment

After analysis, you will identify more devices as potentially having ransomware that was not previously detected. Once a device is identified as potentially having ransomware, the device should be shut down or immediately disconnected from your network. This is when you have to deploy an endpoint detection tool that s beyond basic antivirus protection. If you cannot determine the source of ransomware infection, you will need to terminate all access to file shares to help minimize the risk and impact.

Eradication

Depending on the ransomware variant and the scale of infection, this process can be lengthy. End-user devices, such as those used by employees, and file servers may all have to go through this process. Systems infected with ransomware should be formatted, cleaned, and rebuilt from a trusted source your backups.



Recovery

At this point, it is very important that the root cause of the infection was identified. This way, as you restore from your internal backups, you know which backup copies are clean and which ones are not. Also, if the attack exploited vulnerable systems, this step is where you patch those vulnerabilities to stop the cybercriminals from launching another attack.

When Should You Notif Authorities?

The requirement to notify authorities varies depending on industry, the types of customers and the information stored, as well as local laws. For instance, healthcare providers are subject to HIPAA, and financial institutions that hold sensitive consumer information may be subject to other regulations.

However, in most cases, you must immediately notify authorities once a ransomware attack has been confirmed. In the United States, you must complete the FBI s Internet Crime Complaint Center (IC3) once a breach is confirmed. It is recommended to advice local law enforcement about the incident.

If you decide to pay a ransom, consult with authorities or lawyers prior to find out whether paying a ransom constitutes a federal offense. For instance, paying ransom to cybercriminals from countries under sanctions by the U.S. government will be a federal offense. Those countries, as of 2021, include Russia, North Korea, and Iran.

Pro Tip

Backing up systems and testing system recovery is a critical best practice. Quorum helps customers with ransomware containment, eradication and recovery. Contact us to learn about our process.

Conclusion

Ransomware will continue to evolve rapidly, and its attacks will become more frequent because more and more businesses are opting to pay the ransom for various reasons. Organizations are therefore forced to raise the bar to prepare for ransomware attacks. This guide intends to do just that provide a basic framework on how to prepare against ransomware.

Although there are multiple ways to stop ransomware at its tracks, its continuous rapid evolution will one day weasel way through layers of defenses. At that point, the best bet is to have a solid backup that s immutable and air-gapped like the one that Quorum provides.

How Quorum Protects Your Backups

Quorum s data backup and disaster recovery solution (onQ) has taken several steps to ensure your snapshots are safe and secure. First, the onQ does not share any connections to your production network beyond the cable connecting it. The onQ does not rely on Active Directory, or DNS in order to function. By minimizing these and other attack vectors, the onQ is far less likely to be targeted by a Ransomware attack. Second, onQ also runs a hardened Linux operating system, reducing all security vulnerabilities to an absolute minimum, and further protect it. Finally, all snapshot data is encrypted in motion and at rest, which means previous snapshots cannot be infected, ensuring customers will have an uncompromised snapshot for recovery.

About Quorum

Quorum provides Data Protection solutions helping businesses worldwide to protect their mission-critical data with an all-in-one, easy-to-use, 1-click backup and instant recovery solution. Our onQ product provides backup, recovery and storage replication of your mission-critical data after any storage, system or site failure. Regardless of which deployment environment is selected for your business, Quorum protects mission-critical data under any circumstance and threat. Quorum is modern-day data protection for your business, serving customers worldwide, with offices in the US, UK and business affiliates with offices in South Korea and the UAE. To learn more, visit us at www.quorum.com.

Pick Our Brains for Free

If you wish to dive deeper into a specific area in this guide, feel free to contact us at info@onquorum.com

Quorum backup and disaster recovery solution has helped 100+ companies successfully recover from ransomware, and we are happy to share those experience with you.

Quorum®
1-Click Instant Recovery

www.onQuorum .com | info@onquorum.com
UAE: 00 971 4 2610276