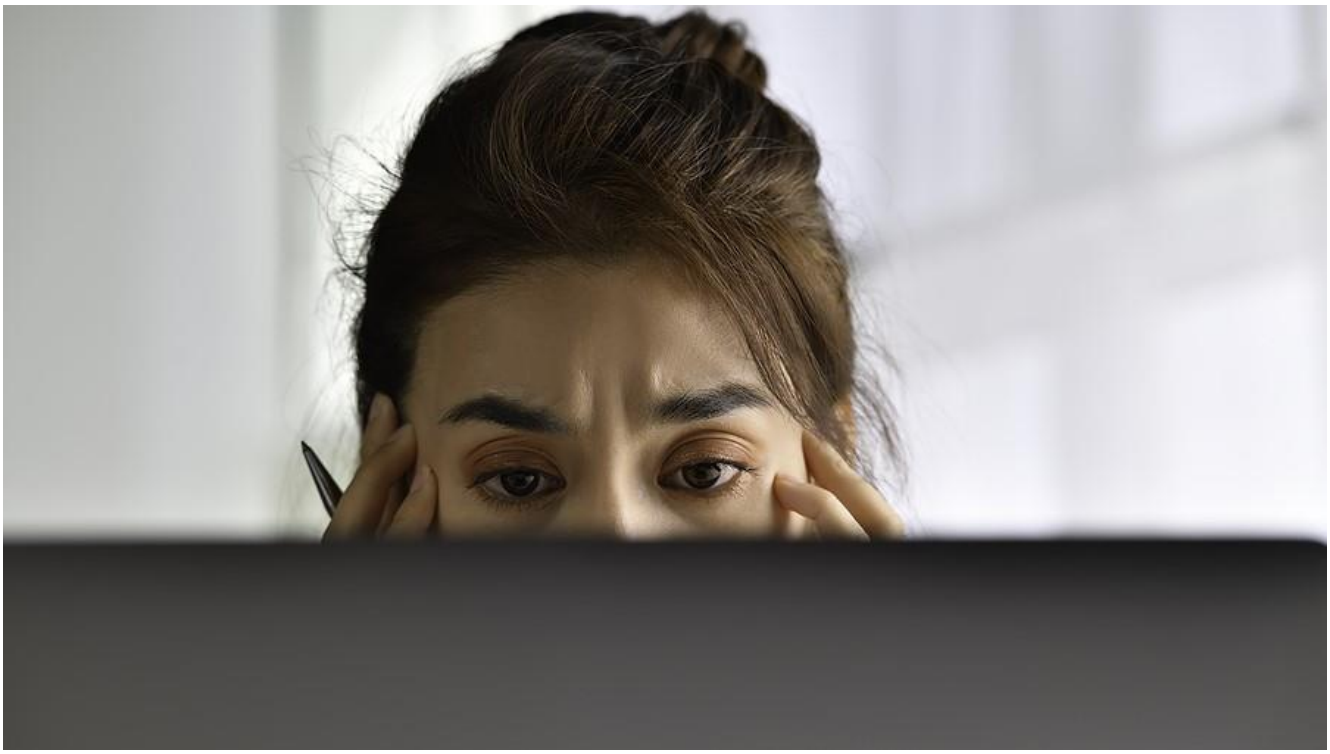
Shorten the Long Ransomware Recovery Process with Expert Help



In an all-too-common scenario, an employee logs on to their computer on Monday morning to find a welcome screen with a ransomware demand. The ransom ultimatum kicks off weeks, even months of costly damage control. However, understanding the factors involved and enlisting the right team and tools can help shorten the ransomware recovery process.

Depending on the type of ransomware involved and how long it has been in the system, the impacts can prove wide-ranging. In a classic attack, the bad actors encrypt data, making it inaccessible. In some cases, hackers also steal the data. They may even use stolen data to target the organization's customers or suppliers.

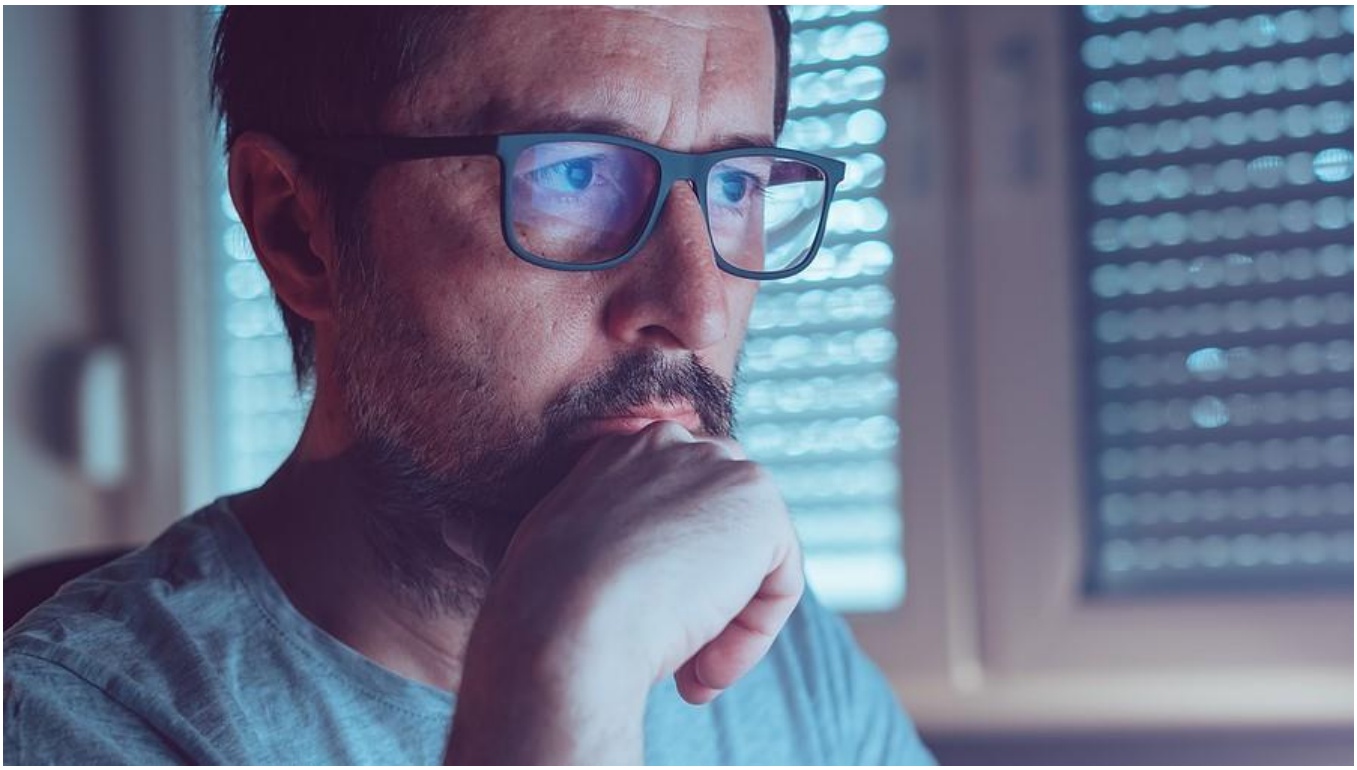
Recovering from a ransomware attack includes several phases. The organization must first detect the attack and determine its source. They then halt the spread of the attack, remove the bad actors from the system and finally proceed with recovery. Recovery time can vary from a few days to many months and may involve completely rebuilding the affected systems.

Early Detection Critical to Rapid Ransomware Recovery

In many cases, organizations do not discover the breach until ransomware has been active in the system for weeks or months. By the time a ransom demand appears, hackers can be deeply embedded

in the network. Eradicating the bad actors and recovering from the infection then proves both time-consuming and costly.

Multiple signs can indicate a ransomware infection. Ideally, companies have implemented antivirus and malware detection software that will sound an early alarm when an anomaly occurs. But a sophisticated ransomware attack can sometimes bypass those systems.



Other signs can include unfamiliar file extensions or files that have changed names. Likewise, increased network activity or suspicious communication from the network to outside sources can indicate the presence of a hacker. Finally, slow or inconsistent system performance and encrypted files raise a red flag.

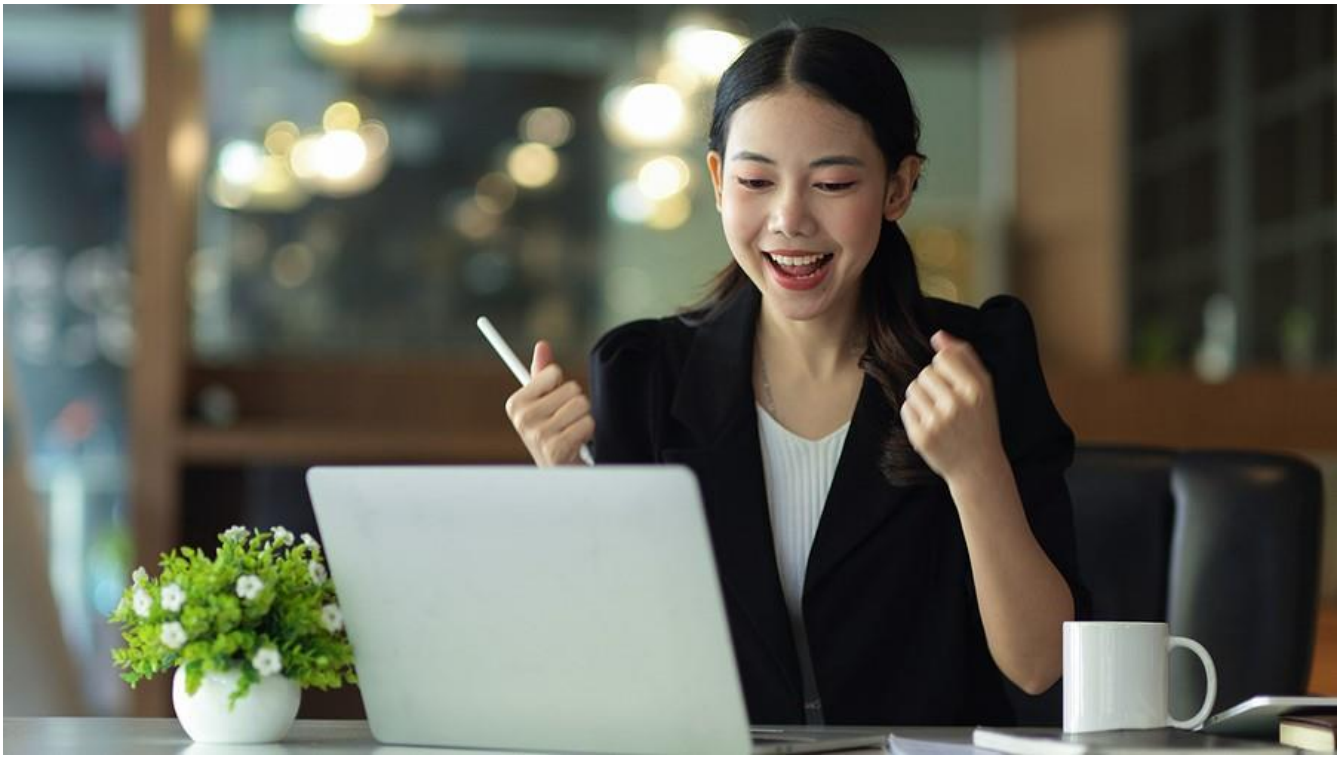
Early detection allows the security team to contain the infection before it has time to spread, thus minimizing the damage. Consequently, constant security monitoring should form an essential part of any cybersecurity strategy.

Common Factors that Increase Cost and Time to Recover

In addition to the time between breach and detection, several other factors significantly impact recovery time and cost. These include:

- **Insufficient disaster recovery plan** – Organizations with well-documented and tested incident response plans have a much greater chance of quick and successful recovery. However, in the absence of an effective plan, companies waste precious time gathering a team and making recovery decisions on the fly.

- **No backups or faulty backups** – Without solid backups, organizations stand to lose critical data unless they can find a decryption key to address encrypted files. Companies should run regular data backups, test the backups and store a copy offline, safe from attack.
- **Type of ransomware** – Some types of ransomware prove easier than others to eradicate. For instance, filecoders such as WannaCry and its variants encrypt and lock files, causing the greatest problem. Understanding the type of ransomware and the gang behind it can help experts determine the best approach.
- **Size and configuration of the system affected** – Small systems typically mean faster recovery. Additionally, if the IT environment was well-managed before the attack, that also aids the recovery process.



Experienced Team and Proven Tools Shorten Ransomware Recovery

In ransomware recovery, the right team and tools can mean the difference between recovery that takes months and one that takes a week or two. That team certainly includes security personnel with substantial experience in incident response and forensics. It may also include cyber breach lawyers, the FBI, communications experts, and a good insurance company.

eMazzanti delivers the expertise and the tools needed to both prevent and respond to ransomware attacks. With eCare Security Operations Center, organizations gain access to highly trained security experts and a top-flight incident response team. 24x7x365 security monitoring deploys in just one hour, delivering critical early detection and remediation.