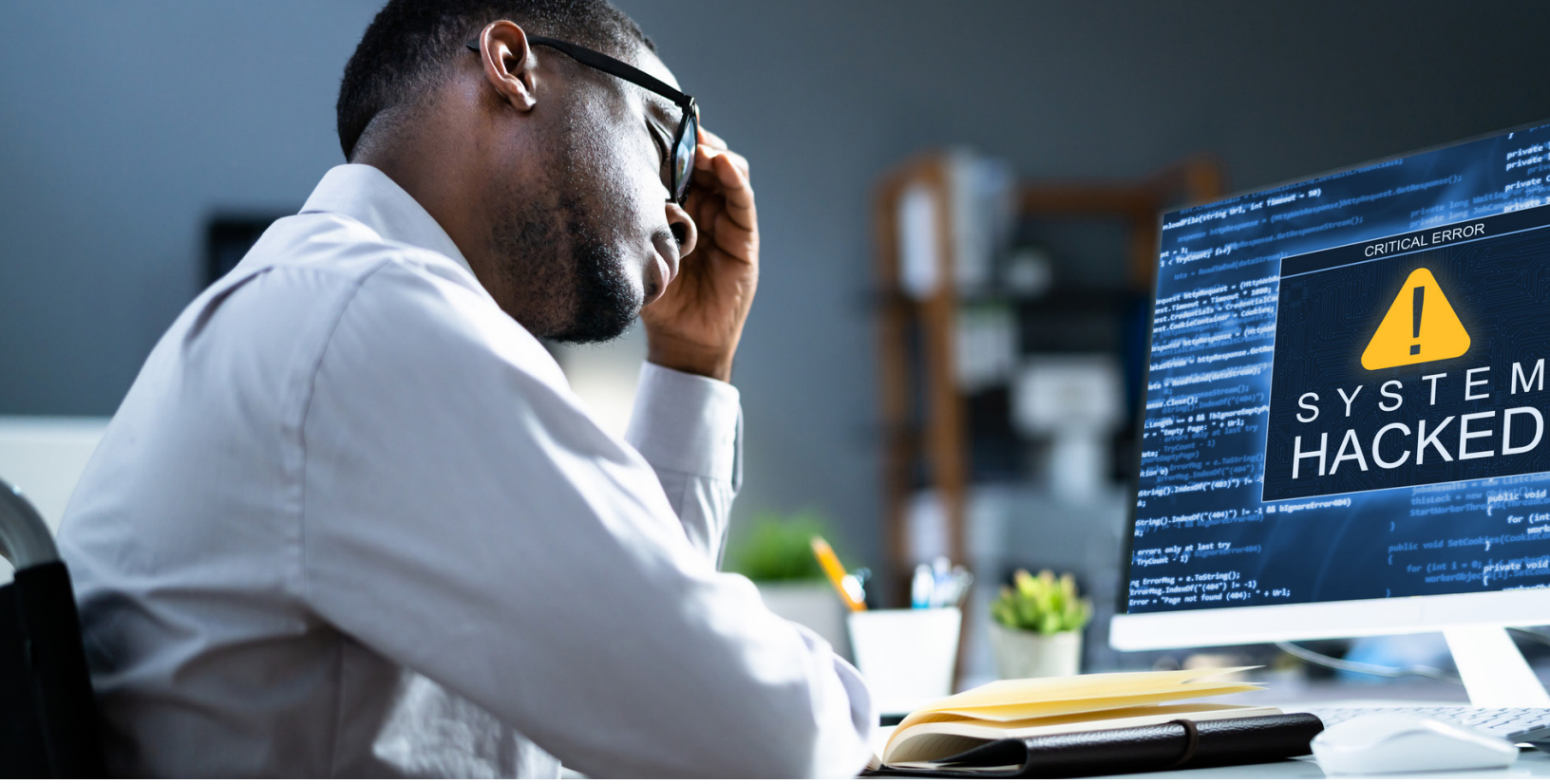
McGowanPRO

Professional Liability Insurance


# Preparing for and Recovering from a Ransomware Attack with Microsoft Security Tools

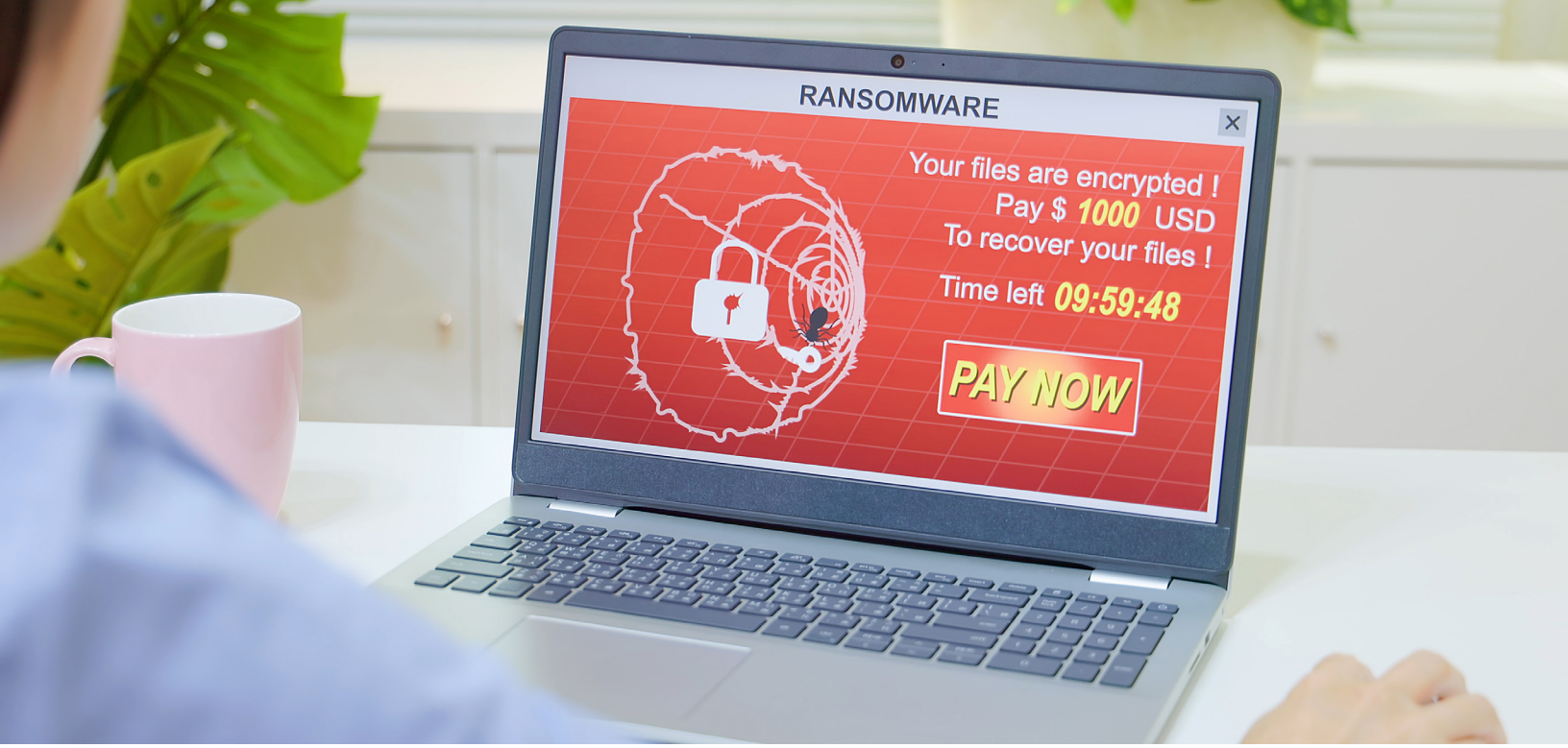



# The threat of ransomware

The threat posed by ransomware is nothing new. In fact, since the advent of the internet, people and businesses have been targeted by cybercrime. Over the years, cybercriminals have developed highly sophisticated methods of attacking companies.

What is new is the growing sophistication and complexity of cyberattacks. For example, Microsoft reports that ransomware attacks grew by an astounding 935% in 2021. But what exactly is ransomware, and how should businesses defend against it? This Ebook will cover topics including:

Table of Contents:




## What is ransomware?

Ransomware is a type of malware (malicious software) that demands that victims pay a ransom to hackers and threatens to:

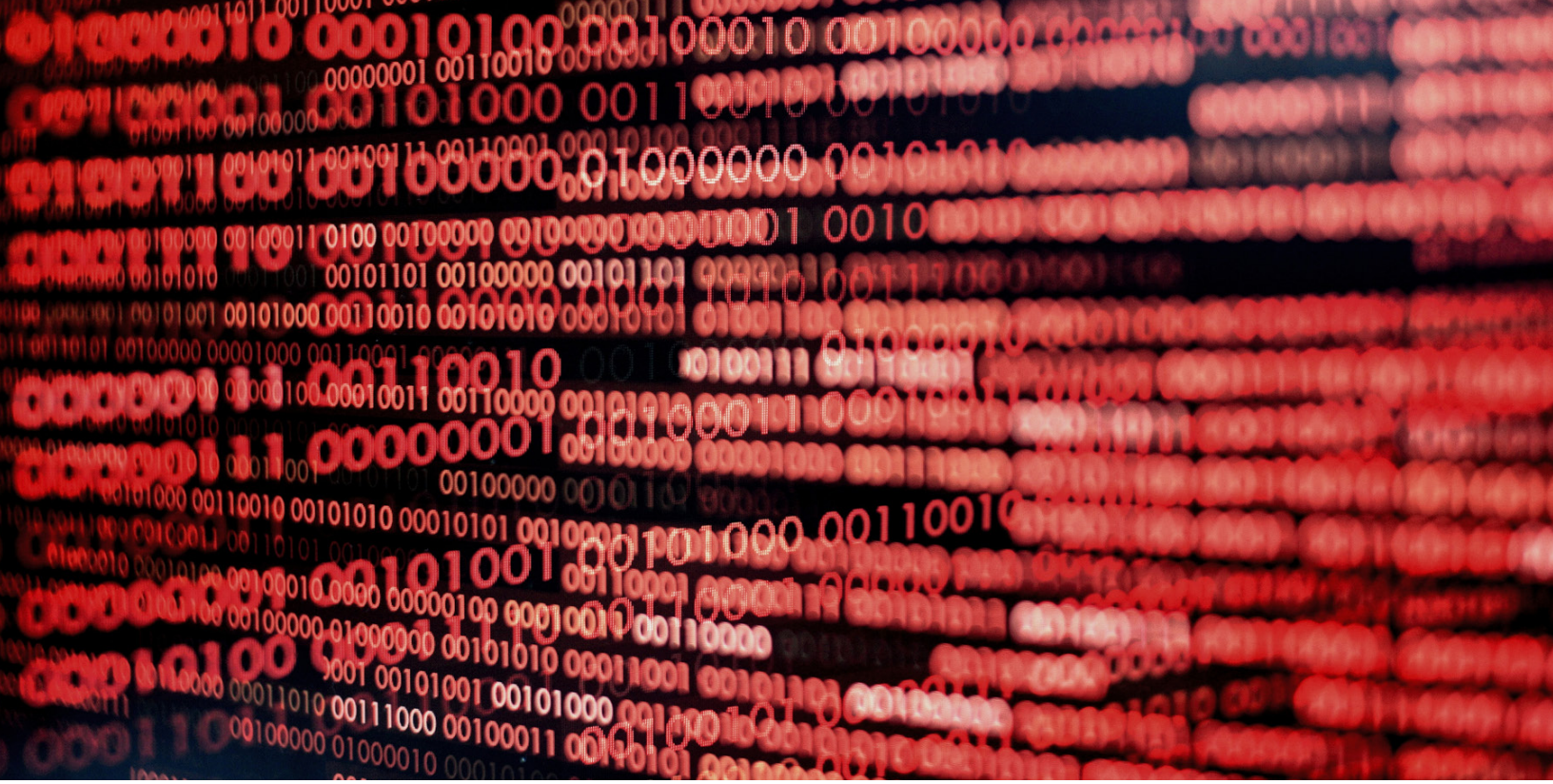
1. Lock access to vital applications and networks.
2. Release sensitive data to the public or competitors.

There are two broad categories of ransomware—commodity and human-operated. **Commodity ransomware** is an automated program. **Human-operated ransomware** is when a person gains remote access to critical computer systems and data, manually manipulating the system. Cyberattacks may include one or a combination of both.

Human-centered ransomware is particularly insidious. Cybercriminals sometimes read internal financial statements to determine an appropriate ransom. Or they may lie in wait and monitor internal communications, waiting for an ideal time to strike.

A culprit behind the explosion of ransomware attacks is the so-called "Ransomware as a Service," in which malware developers franchise their viruses. Amateur hackers can then use the viruses against companies with little coding experience. In exchange, the ransomware developers claim a percentage of the ransom.

Paying the ransom may seem like an easy (albeit painful) solution for many companies. However, it's usually not so simple. There's no guarantee that the hackers will honor their agreement. In addition, the tools they provide to unlock the encryption their malware has implemented against its target files may be amateur and ineffective.



## Common types of malware

Not all malware behaves the same. Let's explore some of the most common types of malware that cybercriminals may use in a ransomware attack to gain access to your core computing systems:

- **Phishing** — Posing as a credible business (like a bank), hackers send a message urging users to click on a link. When the link is opened, it installs malware that steals passwords, banking info, or other valuable data.
- **Spyware** — Spyware installs itself on targeted devices without consent and collects sensitive information. Spyware can also make copies of itself or changes to the computer system without the user's knowledge.
- **Adware** — After installing itself on the user's device, adware displays frequent advertising. It can slow down performance and leave the device vulnerable to other malware attacks.
- **Exploits/Exploit kits** — A type of malware that "exploits" security vulnerabilities. Exploit kits are an assemblage of exploits that scan for various vulnerabilities and, when detected, can dispatch one or more viruses to breach the weak point.
- **Fileless malware** — Malware that doesn't rely on a file or attachment. Notoriously hard to diagnose and repair because it targets firmware, which most antivirus programs don't scan.
- **Macros** — Macros are automated shortcuts in Office and Microsoft 365 applications. Macro malware disguises itself as a macro to infiltrate systems. In response to this, recent Microsoft applications have macros turned off by default. Beware programs asking you to turn on macros!

- **Rootkits** — Rootkits are insidious pieces of malware designed to remain hidden within a system for months or even years. Rootkits can grant hackers admin-level permission and siphon critical information.
- **Supply chain attacks** — These attacks target groups of companies within a supply chain that have interconnected systems.
- **Tech support scams** — Cyber criminals pose as technical support agents and convince users to install malware or give up admin permissions.
- **Trojans** — Packaging themselves inside what appear to be legitimate downloads, trojans can duplicate themselves or download additional malware.
- **Unwanted software** — According to Microsoft, "Unwanted software are programs that alter the Windows experience without your consent or control." Not all unwanted software is malicious, but all malware is unwanted.
- **Worms** — One of the most common types of malware, worms spread through email attachments, text messages, and even social media. Once in a system, it punches through vulnerabilities and duplicates itself. Depending on the type of worm, they may also send sensitive data to a hacker.
- **Coin miners** — Sophisticated cybercriminals can harness the computer systems of an unwilling organization to mine for cryptocurrency.

# Preparing for a ransomware attack

What should a business do to prevent being attacked by ransomware? And what should they do to recover if they are hit? Microsoft recommends a three-phased approach to Ransomware protection and recovery:

- Create a recovery plan
- Limit the scope of the damage
- Make it harder to get in

Ideally, companies should take these steps before an attack. However, they can also serve as a guide to limiting the damage of an attack that has occurred. Microsoft suggests working on phases simultaneously as much as possible, with an ideal implementation of 30 to 90 days after starting.

The provider filed to declare the insurance contract null and void, rescind the policy, and ensure it had no duty to help ICS in its insurance claim. It argued that if the provider had known about ICS's alleged misrepresentation and omission, it would never have approved the policy.

## Create a recovery plan

The goal of the recovery plan is to have a viable set of steps to minimize the risk of an attack, make it harder for hackers to access vital data, and have an alternative to paying the ransom.

**Action Steps**
Work with your IT department or outsourced professional to take these steps:

- Create secure automated backups by migrating to a cloud storage solution.
- Implement a Disaster Recovery as a Service platform such as Microsoft Azure or a similar system.
- Designate protected folders.
- Review permissions.
- Deploy a Zero Trust Model.
- Create a contact plan to contact authorities should a breach occur (see Resource List for FBI Field Offices).
- Codify the recovery plan in a company-wide document.

## Limit the scope of damage

The point of this phase is to limit access to critical files and systems should a hacker enter your network. The hope is to make it so difficult to maneuver that cybercriminals will stop and seek an easier target.

### Action Steps

- Improve detection and response by installing advanced anti-malware products like the Extended Detection and Response (XDR) tool in Microsoft Defender.
- Ensure your IT providers monitor for "brute-force" attacks, such as a password spray attempt.
- Isolate compromised computers.
- Have IT provider help to:
  - Secure all admin workstations.
  - Utilize randomized passwords on the local workstation.
  - Employ privilege mitigations.


## Make it harder to get in

If the last phase was about locking internal doors, this phase is about putting up a razor wire fence around your digital estate.

Making it harder to get in involves:

- Secure remote access
  - Keep software up to date.
  - Properly configure third-party VPN providers.
  - Configure Azure Active Directory to enforce Zero Trust.
  - Install Azure Bastion.
- Email and Collaboration
  - Turn on Advanced Email security via Defender for Office 365 or employ another advanced email security application.
  - Enable AMSI for Office VBA to block Macro attacks.
  - Have your IT provider help you to configure attack surface reduction (rules) in Microsoft Defender.
- Endpoints
  - Block unexpected traffic with firewall and network defenses.
  - Retire unsecured systems.
- Accounts
  - Enforce multi-factor authentication.
  - Increase password security.
  - Monitor permissions.
- Use the Microsoft Attack simulator to find security holes.


# Recovering from an attack

Once you discover a ransomware attack, the key is not to panic. Instead, move through the steps of your recovery plan, which might include some of the following example steps:

1. **Validate backups** — Ensure that offline or cloud backups are not compromised.
2. **Disable syncing on cloud services and email** — Turning off the sync on OneDrive and Microsoft Exchange will prevent the further spread of ransomware across systems.
3. **Remove the ransomware from affected devices** — Run an antivirus scan across all computers and networked drives. You may need to employ more extensive antivirus software, such as XDR, Security Information and Event Management (SIEM), or the Malicious Software Removal Tool (MSRT). You can troubleshoot with Windows Defender Offline if none of these options work.
4. **Recover files from a secure computer** — After removing the ransomware from your digital environment, you can use your backup systems to recover the files. Versioning and file history can help you recover previous file versions.
5. **Recover deleted emails** — Some ransomware will attempt to delete all emails. Once a system is secured, you should be able to recover the emails from Outlook's recycling bin.
6. **Turn sync back on** — After your devices are clean and network drives are secured, it should be safe to enable the sync function on Exchange and OneDrive.

Microsoft also recommends the optional step of blocking specific file extensions to stop the repeated spread of ransomware that acts on specific file types.

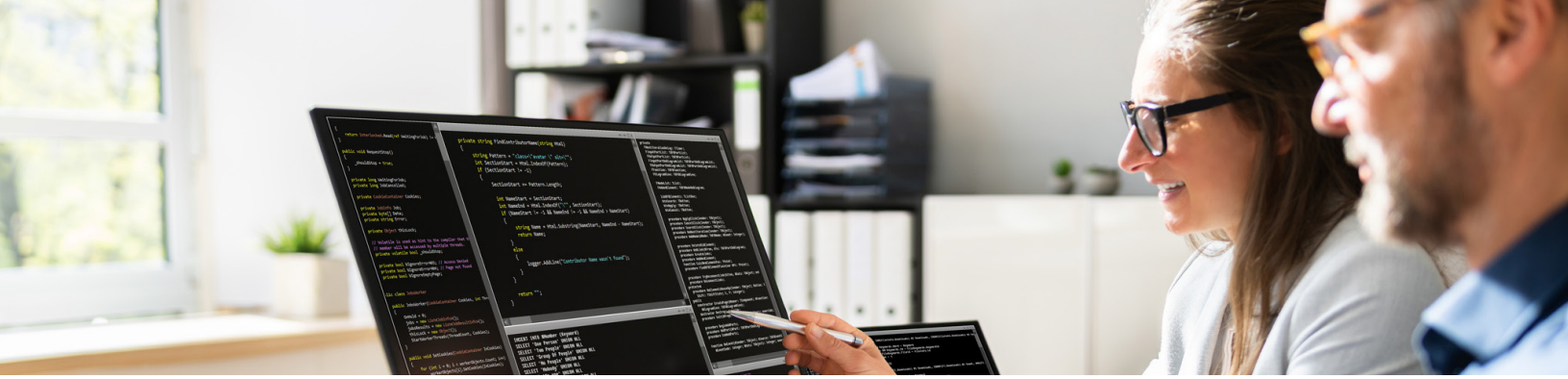
***Note:*** *This guide is intended to provide generalized guidance in preventing and recovering from a malware attack. Businesses should seek expert guidance from IT professionals or the cybersecurity team at Microsoft to secure their cyber real estate.*


# How Cyber Liability Insurance can help

Although it's nothing new, the insidious threat of ransomware is ever present and expanding its reach through Ransomware as a Service schemes. But as we've seen, there is no reason to panic and pay ransoms. Instead, businesses can limit their potential exposure to ransomware by following the steps outlined in this guide, investing in cyber security best practices, and seeking expert IT advice.

But no battle plan is perfect. The reality is that most profitable companies across all sectors will suffer a cyberattack at some point in their lifetime. McGowanPRO's expert advisors are well-versed in helping their clients mitigate their cyber liability risk. Our Information Security & Data Privacy Liability Insurance provides industry-leading coverage to protect businesses in the event of a cyberattack.

To learn more, contact us today.



# List of resources

Accountants Professional Liability Cyber and Data Security
What to do if you have a Data Breach
Protect Client Data from Identity Theft - Best Practices
FBI Field Offices
Microsoft
- Malware and ransomware protection in Microsoft 365 - Microsoft Service Assurance
- Recover from a ransomware attack - Office 365
- Ransomware detection and recovering your files
- Quickly configure for ransomware prevention in your organization to help stop ransomware cybercriminals.
- Deploy ransomware protection for your Microsoft 365 tenant
- The growing threat of ransomware - Microsoft On the Issues
- What is ransomware? | Microsoft Security
- What Is Malware? | Microsoft Security
- Understanding malware & other threats
- How Microsoft identifies malware and potentially unwanted applications

McGowanPRO
*Professional Liability Insurance*

**Contact us:**

L Squared Insurance Agency LLC
2430 Camelot Ct Grand Rapids MI 49546
Phone: +1 616-940-1101 | Fax: +1 616-940-1196

Info@l2InsurnaceAgency.com

https://mcgowanprofessional.com/