



# Is Your Organization Ransomware-Ready?




# Is Your Organization Ransomware-Ready?

Ransomware is a gold mine for cybercriminals. Most businesses aren't fully prepared to defend against it, and it can be monetized beyond the ransom by selling stolen data and using "name and shame" schemes. What's worse, the cost of ransomware downtime has nearly doubled and [can cost far more than the ransom](#).

**So what's a company to do? Be ransomware-ready.**

Running an [Endpoint Detection and Response \(EDR\)](#) tool can undo ransomware encryption by rewinding the chain of events — it's one of the best ways to be ready. Answer these 11 questions to learn what else you can do:

**What's worse, the cost of ransomware downtime for victims has nearly doubled in the past year and can cost far more than the ransom.**



## **1. Are your backups ransomware-resistant?**

Ransomware can encrypt backups that are connected to your network. And you can't restore from encrypted backups.

For your backups to be ransomware-resistant, they need to be offline, isolated from your networks, and in a different physical location from your servers. They also need to be inaccessible to devices that may be infected by ransomware, including computers and mobile devices. Switching to a third-party, cloud-based disaster recovery (DR) solution is a good way to reduce this risk and it might save you some money, too. It's typically less expensive and faster than traditional DR solutions.

**While ransomware-resistant backups save you from having to pay the ransom, keep in mind they don't prevent attackers from damaging your company in other ways if they can access your systems.**

## **2. Have you segmented your IT environment so there are boundaries between your systems?**

Part of making backups ransomware-resistant is to put them in another segment in your environment. Colonial Pipeline had not done this — nor had they segmented their network, which meant that the attackers had free access to jump from one system to another, including the

company's operational system. With access to both the IT systems (information or office systems) and OT systems (operational or factory-floor systems), the entire company was vulnerable due to one [leaked password for an old VPN account](#) that had been published on the dark web.

With firewalls between segmented systems, you can reduce your ransomware and hacking risks.

### 3. Is your incident response plan (IRP) ready to go?

Your IRP should include tested processes and procedures specifically for ransomware. They should not only ensure that you can restore from backup effectively but assign specific roles and responsibilities in case of a ransomware attack.

All employees need to know what to do and how to do it, including isolating any affected device immediately and powering off any device that may have been affected but is not yet completely corrupted. Management needs to know how to handle an attack once it's occurred, including escalating the incident, filing a cyber insurance claim, activating legal counsel and forensic specialists, and conducting tabletop exercises beforehand.

### 4. Do you require multi-factor authentication (MFA) for every login?

[MFA](#) makes it much harder to get into your systems. The extra layers of authentication force attackers to exploit a vulnerability within your systems rather than exploit a person or use stolen login credentials available on the dark web.

Even the most highly trained and diligent employees can't guard against ransomware if their passwords get cracked. Once criminals can access an employee's computer, they can easily download ransomware. [Password best practices](#) protect against ransomware by making passwords hard to crack.

Using [single sign-on](#), in addition to MFA, is better yet. It authenticates access privileges in real-time and reduces the required number of passwords employees must remember down to one, thereby reducing the risk of compromised passwords.

**Even the most highly trained and diligent employees can't guard against ransomware if their passwords get cracked. Once criminals can access an employee's computer, they can easily download ransomware.**

## 5. Does your email gateway include advanced features?

Email gateways that include reputation screening and protect against impersonation also protect against ransomware. Infected emails are much less likely to make it through.

Reputation screening looks at the reputation of the sender — has your company received email from this sender before? Is the sender on a blacklist? How many recipients of emails from this sender have opened, replied to, or forwarded the emails? Impersonation screening uses granular-level techniques to ensure that senders are who they say they are, including your CEO. Phishing employees using spoofed leadership email addresses is especially effective because employees are highly likely to click on a link from the boss. Make sure to remove all executive email addresses from your website and other nonessential public-facing platforms.

Next-gen email protections effectively guard against man-in-the-middle attacks in addition to ransomware.

## 6. Are your employees fully trained on ransomware prevention?

Vigilant employees are your organization's first line of defense. Every employee should be aware that mistakenly clicking on a malicious link can download ransomware into your organization's IT environment. How can employees distinguish between links that are safe and ones that aren't? That's what the training is for.

While scams evolve and get more sophisticated, phishing emails and links in social media are still the most common ransomware delivery mechanisms. Compromised websites continue to be a risk, too.

**Working with a reputable cybersecurity awareness training company to train all of your employees is the single most cost-effective investment you can make in preventing ransomware attacks.**

## 7. Are all of your computers patched and up to date?

Ransomware is not a virus. It's malware that locates vulnerabilities in your system. If any of your computers are running an operating system (OS) that's not been patched with the latest security updates, those computers likely have exploitable vulnerabilities. Computers running

Windows 7 (or any outdated operating system) are at much higher risk — as many as [100 million or more computers](#) are still running Windows 7. A single unpatched computer can bring your entire organization to a standstill.

## 8. Is your antivirus and antimalware software sophisticated enough?

The most effective antivirus software adds layers of protection. Before downloading a file, it automatically opens it in a sandbox, or a safe zone, that allows for checking for malicious content. This creates a protective two-step process that blocks suspicious downloads.


Your software should also include [zero-day threat detection](#) and, if possible, an [endpoint detection and response](#) (EDR) solution. Zero-day threats are software or hardware vulnerabilities that do not yet have patches available. When hackers discover the existence of a zero-day vulnerability, they quickly write code to exploit it then include that code in the ransomware package. To block zero-day attacks, next-gen antivirus uses threat intelligence, behavioral analytics, and machine-learning code analysis. EDR helps you locate, contain, and remove sophisticated threats that less sophisticated software may miss.

## 9. Do you have a verifiable smartphone policy that protects your network?

Having a Bring Your Own Device (BYOD) policy is critical to protecting against ransomware, as is training your employees on how to adhere to it. Malware on smartphones can make its way onto your network if your employees don't keep personal data separate from business data. And if a phone that's not locked down is lost or stolen, criminals can steal sensitive data to use in ransomware scams and bypass MFA, because MFA usually sends authentication codes by text, a phone call, or an app that's on the phone.

Modern platforms can automatically verify proper phone configurations — for example, Office365 and newer versions of Exchange can verify if a passcode is present or if biometric security is enabled — and continually monitor your network activity for any breaches. When you find improper BYOD use, be sure to enforce your policy.

**Some insurers are conducting penetration tests on your company to see if their experts can get into your system.**



## 10. Do you block the use of unauthorized USB drives?

USB drives can lead to all sorts of problems, including ransomware. If an employee plugs in an infected USB drive to their computer or clicks on an infected file on the drive, they just inadvertently opened the door to ransomware. Some ransomware strains may propagate themselves by hiding on a computer, then infecting other USB drives when they're connected.

Banning the use of USB drives has become a common practice for some companies. Just make sure to offer an efficient alternative to moving files around, such as using a secure cloud platform. Otherwise, employees will be tempted to use a workaround that may be equally or more susceptible to ransomware. Allowing only authorized USB drives may be a good option.

## 11. Do you have visibility into your network and are you continually monitoring activity?

To protect against ransomware, you need to be on the offensive. You can't contain a threat that you don't know exists.


By implementing good visibility tools, there is a strong possibility you will be able to see suspicious activity. Suspicious activity can include two identical logins simultaneously, activity from unusual locations or at unusual times, or views or modifications to files that have been untouched for years. There may be a good reason for these anomalies, or they could indicate an impending ransomware attack. Without visibility tools and monitoring, you're flying blind.

## Did you answer YES to all of these questions?

If you answered YES, your organization is successfully protecting itself against ransomware — you are ransomware-ready. If you didn't, start tackling your vulnerabilities in priority order.

While it's important to note that no organization is ever 100% safe from a ransomware attack, following these best practices adds layers of protection that can significantly reduce your odds of being attacked. The first two items on the list — ransomware-resistant backups and segmented systems — will determine how quickly you can recover if you are attacked and at what cost.

**By implementing good visibility tools, there is a strong possibility you will be able to see suspicious activity.**



## Why you shouldn't pay the ransom

If you get attacked, paying the ransom should be your last recovery option. You don't know if the attackers will give you the decryption key after you pay up or if they'll demand even more ransom or attack you again later. In a recent report, Sophos found that of companies that paid the ransom, only [8% got all of their data back](#) and 29% got half or less of their data.

Paying ransoms also encourages more ransomware attacks.

**The best way to avoid having to decide whether or not to pay a ransom — and having to deal with the rest of the [fallout from a ransomware attack](#) — is to go on offense by planning in advance. Due diligence pays off.**

**Leapfrog Services** is an IT Security, Network, and Infrastructure Managed Service Provider (MSP/MSSP) that's been helping organizations meet their business goals and protect their data since 1998. Our team designs and operates outsourced solutions based on our proven methodology that includes matching your level of threat protection to your business needs and adhering to the highest cybersecurity standards (we are SSAE 18 SOC 2 compliant). Guarding against risks systematically and consistently reduces the likelihood your organization will be attacked and helps you to remain productive and successful. You can reach us at 404-870-2122 or [leapfrogservices.com](http://leapfrogservices.com).

