Don’t Pay the Price:
A Checklist of Proactive Measures to Protect Against Ransomware

LeapFrog®

Don’t Pay the Price: A Checklist of Proactive Measures to Protect Against Ransomware

Modern day ransomware has evolved into sophisticated software that can cause an insurmountable amount of damage to companies. They face financial loss, data loss, data breaches, downtime during rebuilding, and devastating reputational damages. This type of cybercrime is popular among criminals due to the easily obtainable toolkits and even Ransom-As-A-Service that allow cyberattacks to be launched with minimal effort. Not to mention it pays well.

The global annual cost in damages from ransomware is estimated to reach $42 billion by the end of this year, and $265 billion by 2031, predicts Cybersecurity Ventures.

While it’s important to note that no organization is ever 100% safe from a ransomware attack, following this checklist of 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.

Keep 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.

Segment your network

Segment your network to minimize the attacker's ability to jump from one system to another in the same environment and limit the spread of ransomware. Further reduce your ransomware and hacking risks by installing firewalls between the segments.

Have an Incident Response Plan (IRP) ready to go

Response time is vital in minimizing the damages of an attack. Develop and regularly update an IRP in case fast action is required. 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.

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.

Secure all emails

Use email filters and scanners to detect and block potential threats. 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.

Train all employees often on ransomware prevention

9 out of 10 data breaches are caused by user error, according to Stanford University research.

Vigilant employees are your organization's first line of defense. Ransomware is always being reinvented into more sophisticated scams, making it imperative to conduct regular training sessions covering the risks of ransomware and how to recognize threats, including various phishing attempts and deceiving links.

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.

Ensure your computers and software are 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. Keep all software, operating systems and applications (apps) up to date.

Install sophisticated Antivirus and Anti-malware software

Use reputable antivirus and anti-malware software to scan for potential threats. 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 and 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.

Implement and Enforce a Bring Your Own Device policy

Smartphones and other devices that connect to the network can easily pass along ransomware. Enforcing 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 and continually monitor your network activity for any breaches.

Control the use of USB drives

USB drives can lead to all sorts of problems, including ransomware. If an employee plugs an infected USB drive into their computer or clicks on an infected file on the drive, they inadvertently open the door to ransomware. Some ransomware strains may propagate themselves by hiding on a computer and 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.

Monitor your IT environment constantly

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

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.

Ransomware can be devastating, but with the right precautions, you can defend your company and maintain your peace of mind.

Ransomware has evolved into a global threat and is becoming more sophisticated, more targeted, and causing longer recovery times. The best defense is prevention.

Leapfrog offers outsourced managed IT and cybersecurity services that fit easily into your business model. With over 25 years of MSP, MSSP, and CyberRisk Management experience, we help a broad array of companies simplify their IT operations while improving their security and resiliency. Our services are scalable, aligned, and built on a proven methodology, and our culture (we call it "Frogma") is built on Integrity, Service, and People so you get personalized, best-in-class support.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you want help managing and monitoring your organization against ransomware and other cyber threats, Leapfrog is here for you. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329