

6 Ways We Shield Your Business From Ransomware



Introduction

As your business becomes increasingly digital, the devices, back-end systems, and applications you're using generate an overwhelming amount of data — an attractive target for cybercriminals and ransomware.

Ransomware is a pernicious form of malicious software that encrypts data against access by your own business, only to be unlocked if you pay the ransom demand. In some cases it's possible to crack the code, but the cryptology specialists capable of such feats don't come cheap. As of 2021, the average cost to recover from a ransomware attack was estimated at \$1.85 million.¹

The increasing number of employees working remotely and on-the-go has created more risk. When your employees exchange critical business data using smartphones, tablets and personal laptops, your proprietary data, as well as financial information, may be exposed and, therefore, vulnerable. Attackers can gain a foothold with something as simple as tricking an employee into clicking on the wrong link or attachment in an email.

Hackers are discovering easy targets with the recent surge in work-from-home arrangements and the use of insecure employee-owned devices.²

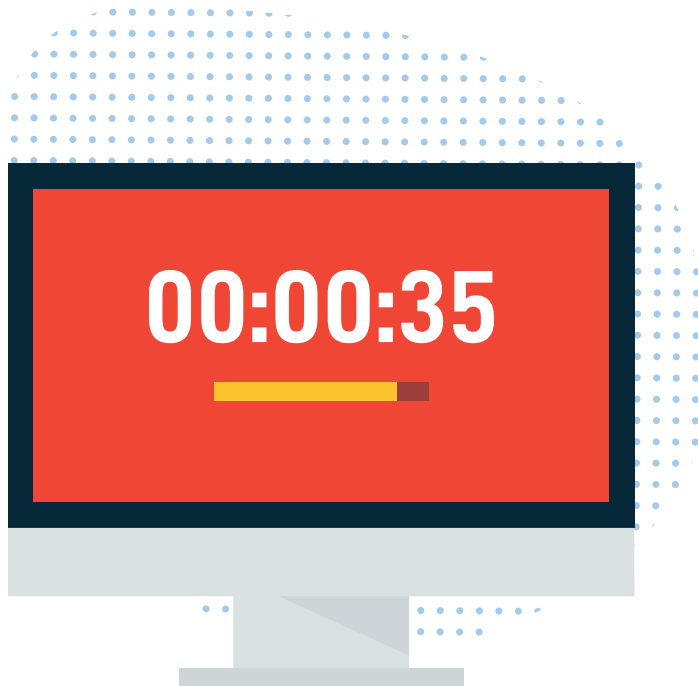
When Will You Be Attacked?

Callout for this section: When thinking about cybersecurity, the question is not “if” your business will be attacked but “when” — and how prepared you will be when it happens.

When thinking about cybersecurity, the question is not “if” your business will be attacked but “when” — and how prepared you will be when it happens. Infection methods are more sophisticated and phishing scams look more realistic. Fake emails with malicious payloads often appear to come from a trusted institution like a bank or a major technology company like Microsoft, Google, or PayPal, hijacking the trust consumers (and employees) place in those organisations.

For example, one scam that popped up in 2020 used Google Drive file sharing notifications. The email notifications people received legitimately were sent by Google, but the documents they pointed to contained harmful links.³ A 2021 scam impersonating Microsoft represented the company logo as an HTML table with coloured cells, rather than referencing an image file of the company logo that might have been detected by spam filters.⁴

The extortion carried out by ransomware attackers is a serious concern, but often not what does the most damage. In the 2021 attack on Colonial Pipeline, which caused fuel distribution disruptions across the northeastern U.S., law enforcement helped the company recover a portion of the \$4.4 million in ransom it paid. However, the company said it expected fully recovering from the attack to cost tens of millions of dollars.⁵



When thinking about cybersecurity, it's not just about “if” your business will be attacked; it's about “when” it will be attacked.

The trend is that cybercriminals are growing ever more devious, resourceful, and aggressive. No one can avoid being targeted, but you need not let yourself be an easy target.



Attacks on large companies and government organisations tend to be most in the news, but the U.S. Department of Homeland Security estimates that 50 to 70 percent of ransomware attacks are aimed at small and medium-sized companies.⁶ In addition to reporting similar numbers, the National Cybersecurity Alliance estimates that 60% of small businesses hit by a cyber attack go out of business within 6 months.⁷

Ransomware often gains a foothold in an organisation through a phishing email that tricks an employee into following a link or opening an attachment containing malicious code. The attachment might appear to be an invoice received by finance or a resume received by HR. Other attacks are embedded in web pages and exploit browser security flaws. Some of the most dangerous are network worms capable of replicating themselves across the Internet and corporate networks.⁸

One of the most notorious of these worms is WannaCry. Once WannaCry infects a device, it finds and encrypts files, displays a "ransom note" and demands bitcoin payment from infected users. Reports indicate that the ransomware strain has spread to 150 countries, impacting 10,000 organisations, 200,000 individuals and 400,000 machines. Many of these attacks appear to be sponsored by nation states — in 2017, the U.S. and U.K. formally accused North Korea of being behind WannaCry.⁹

The trend is that cybercriminals are growing ever more devious, resourceful, and aggressive. No one can avoid being targeted, but you need not let yourself be an easy target. With the right preparation, you can avoid being held at the mercy of ransomware attackers and prevent downtime for business-critical systems.

Our Six-Step Approach to Keeping Your Data Safe

Much like biological viruses, there are many ransomware threats circulating the web. With every occurrence, the sophistication of these viruses is increasing in a multitude of ways, including how they spread and how they encrypt data. As your IT service provider, we know that protecting your business from ransomware is not a single-prong approach. Being able to mitigate or prevent attacks is our top priority. We have put in place an agile, multi-layered approach that can adapt as new and increasingly hostile threats emerge.


Our best-in-class approach consists of six layers:

1. Patching

The most basic layer of protection is to monitor and patch all computers and applications. With the latest patches, we can address all known OS Security vulnerabilities. Patching provides the most basic layer of protection to operating systems, especially once a security flaw is uncovered. We provide the latest patches to ensure your operating systems are running at peak performance and that all system vulnerabilities are addressed.

2. Antivirus and Network Monitoring

People are being targeted through more sources than ever — email, ad networks, mobile applications and devices. Anti-virus and network monitoring examines all files and traffic, and filters them against all known threats. We keep virus definition files updated to protect these systems.



Much like biological viruses, there are many ransomware threats circulating the web.

There is sometimes a gap between when a threat is first introduced and when we receive notification and can develop a remedy.



3. Backup and Disaster Recovery

There is sometimes a gap between when a threat is first introduced and when we receive notification and can develop a remedy. We do a full-system backup to protect your back-office systems. This enables us to stay on top of things when an attack occurs and provide a recovery option for unknown threats and even the most catastrophic failures.

“The most important defence for any organisation against ransomware is a robust system of backups,” the FBI’s computer crime division states in a public advisory.¹⁰ Part of making backups “robust” is ensuring that they are not also hacked. “The time to invest in backups and other cyber defences is before an attacker strikes, not afterward when it may be too late,” the FBI warns.

4. Endpoint Backup

Although there's a layer of protection on your back-office systems, you still need to have backup and recovery of data for devices. These devices create, share and store business data, and if a cybercriminal captures this proprietary and sensitive information, it can have a significant impact on business productivity and profitability. We do real-time data backup on these endpoints to prevent business critical information from being compromised.



The most important step in our process is to create awareness about these threats.

5. Secure File Sync and Share

We want to allow your employees to collaborate securely from any location and using any device — even their smartphones and tablets. Using our enterprise-grade, secure file sync and share solution, you can grant access and editing controls for specific documents, such as Word documents, Excel spreadsheets and PowerPoint presentations, and we can help employees to recover documents that are maliciously or accidentally deleted.

6. Education and Awareness

The most important step in our process is to create awareness about these threats. We offer training and educational materials to help you educate your employees about cybersecurity risks, new ransomware strains and best practices for spotting phishing attempts, suspicious emails and other security risks. Empowering them to be proactive and encouraging them to report questionable content using rewards and incentives will help increase awareness and decrease overall risk.

We Protect Your Business With A Comprehensive Solution

New ransomware threats are constantly emerging and evolving. To learn how we can protect your business and provide a secure and collaborative environment for all your employees, contact us today.

Zubair Syed | Solutions Architect | Phone: 1300 754 711 | Email:
zubair.s@ampmit.com.au | AMPM IT Solutions | <https://ampmit.com.au>

SOURCES

- ¹"Ransomware Recovery Costs More Than Double in a Year, Now Average \$1.85 Million," CSO Online, 7 May 2021 <https://www.cpomagazine.com/cyber-security/ransomware-recovery-costs-more-than-double-in-a-year-now-average-1-85-million/>
- ²"Russian Criminal Group Finds New Target: Americans Working at Home," New York Times, 25 June 2020 <https://www.nytimes.com/2020/06/25/us/politics/russia-ransomware-coronavirus-work-home.html>
- ³"A new scam uses Google Drive to send out a deluge of dodgy links," Wired, 29 October 2020 <https://www.wired.co.uk/article/google-drive-spam-comments-phishing>
- ⁴"How phishing attacks spoofing Microsoft are evading security detection," TechRepublic, 28 April 2021 <https://www.techrepublic.com/article/how-phishing-attacks-spoofing-microsoft-are-evading-security-detection/>
- ⁵"How a major oil pipeline got held for ransom," Recode, 8 June 2021 <https://www.vox.com/recode/22428774/ransomware-pipeline-colonial-darkside-gas-prices>
- ⁶"6 Things Every Small Business Needs to Know About Ransomware Attacks," Inc., 25 June 2021 <https://www.inc.com/amrita-khalid/ransomware-hackers-crime-cybersecurity-tips.html>
- ⁷"60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)," Inc., 11 May 2017 <https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html>
- ⁸"CSO's guide to the worst and most notable ransomware," CSO Online, 10 June 2021 <https://www.csoonline.com/article/3607649/csos-guide-to-the-worst-and-most-notable-ransomware.html>
- ⁹"Cyber-attack: US and UK blame North Korea for WannaCry," BBC, 19 December 2017 <https://www.bbc.com/news/world-us-canada-42407488>

