OneCollab

PROTECTING YOUR BUSINESS FROM RANSOMWARE ATTACKS

www.onecollab.co.uk

@onecollablimited
+44 20 8126 8620
info@onecollab.co.uk

Introduction

Ransomware Infections — a Daily Risk

The threat of ransomware looms larger than ever before. With news of ransomware attacks increasing in both numbers and scale, it's crucial to protect your business by treating this threat as any other external business threat.

Let's face it, unless you're a security professional, understanding and incorporating ransomware threat into your business operations planning can be daunting. At OneCollab, we recognise the critical importance of safeguarding your business against ransomware attacks. As your trusted IT partner, our primary goal is to ensure your organisation remains resilient in the face of evolving cyber security threats.

Our step-by-step guide outlines expert advice and guidance on protecting your business from ransomware attacks. We'll delve into how it operates, and crucial strategies to prevent its infiltration into your personal and business devices.

Statistics

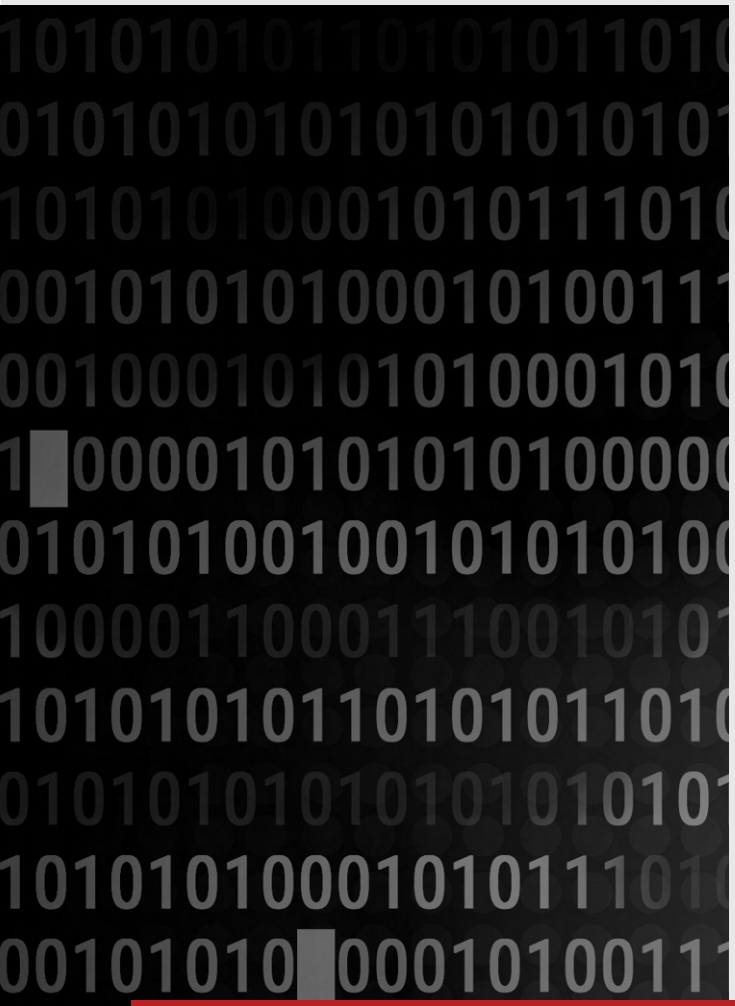
5,070 ransomware attacks were recorded in 2023, marking a 55% increase from 2022[1]...

20% of ransomware costs are attributed to reputation damage[2]...

$1 Billion in ransomware payments were surpassed in 2023[3].

With these statistics in mind, it's clear that vigilance against ransomware attacks is paramount for safeguarding your business's assets and reputation.

[1]Cyberint 'Ransomware Trends and Statistics Report 2023', [2]AAG IT 'The Latest Ransmware Statistics', [3]Chainalysis 'Ransomware 2024'.



What is a Ransomware Attack?

Ransomware is a type of malware which has been engineered to block access to your device and its data, often by encrypting files.

Attackers demand a ransom for decryption, threatening to leak stolen data if not paid.

In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever, relseased or the ransom increases.

Examples of Ransomware Attacks

LockBit Attack on Royal Mail, January 2023[4]

In January 2023, the LockBit group targeted Royal Mail, causing chaos in international mail delivery. The attack crippled crucial services like the parcel tracking website and online payment system. Printers at the Royal Mail distribution centre in Northern Ireland churned out copies of LockBit's orange ransom note.

Despite threats to post stolen data online, Royal Mail refused to pay the ransom, leading to the publication of the data.

Clop Group Attack Through Vulnerability in MOVEit Transfer, June 2023[5]

In June, the notorious Clop group, known for its February attacks on Fortra GoAnywhere MFT, exploited a vulnerability in Progress Software's MOVEit Transfer. Despite Progress fixing the vulnerability (CVE-2023-34362) by May's end, not all clients applied the patches promptly.

This attack, one of the year's largest incidents, targeted various organisations, including oil giant Shell and the BBC.

[4] The Record 'LockBit Ransomware Group Threatens Royal Mail Data Leak Deadline'

[5] Kaspersky 'MOVEit Transfer Attack Protection'.

Am I Target for Ransomware Attacks?

No sector or business size is immune to the reach of ransomware, with vulnerabilities lurking even in the most fortified environments. The likelihood of successful attacks varies, influenced by factors such as technological infrastructure, security measures, and overall cyber security maturity.

News headlines underscore the indiscriminate nature of these assaults, targeting organisations across diverse sectors, from healthcare and finance to aviation. Yet, attackers often select their targets based on two key factors: **opportunity** and potential **financial gain.**

Organisations with limited security resources and file-sharing user bases may present attractive opportunities, while those with urgent file access needs or sensitive data may be more inclined to pay ransoms swiftly to mitigate damage and preserve reputation.

Furthermore, proactive measures are essential in mitigating the risk of ransomware attacks. By adopting a comprehensive cyber security strategy, organisations can bolster their resilience and minimise the impact of potential ransomware attacks.

Should I Pay The Ransom?

At the forefront of business risks looms the ominous threat of ransomware attacks. These insidious assaults wield the power to encrypt critical data, paralysing entire computer systems and, in extreme cases, sealing the fate of businesses indefinitely.

Amidst the weight of such perilous circumstances, businesses grapple with a daunting decision: whether to succumb to hackers' demands and offer a ransom payment in exchange for data decryption.

Yet, in the vast majority of scenarios, the resounding answer remains a steadfast **"no."**

Businesses are strongly urged to resist the temptation of ransom payments unless they find themselves devoid of any viable lifelines for survival.

How Do Ransomware Attacks Work?

Understanding how attackers breached your network is crucial for preventing future ransomware attacks.

01

Access

Cyber attackers infiltrate your network, seizing control and implanting malicious encryption software.

They may also pilfer copies of your data, leveraging it as leverage for extortion.

02

Activation

The malware springs into action, locking devices and encrypting data across the network, rendering it inaccessible.

03

Ransom Demand

You'll typically receive an on-screen notification from the cybercriminal, detailing the ransom and instructions for payment to regain access to your data or unlock your computer.

Payments are usually demanded through anonymous web pages and in cryptocurrencies like Bitcoin.

How Is Ransomware Delivered?

Ransomware attacks persist as a pervasive cyber threat, underscoring the need to understand how to defend against them. Here are six of the most common delivery methods for ransomware:

Phishing

Phishing emails serve as a prevalent avenue for ransomware infections, tricking victims into disclosing sensitive information or clicking on malicious links or attachments.

Once clicked, ransomware swiftly infiltrates the victim's device.

Drive-by Downloads

Malicious software can be unwittingly installed on a victim's device through drive-by downloads, requiring no action from the victim beyond visiting a compromised website. Exploiting unpatched security vulnerabilities, these downloads infect devices silently.

Exploit Kits

Cybercriminals utilise exploit kits, seeking out unpatched security vulnerabilities to streamline malware distribution.

By luring users to their landing pages through malvertisements or spoofed websites, exploit kits identify and exploit vulnerabilities to infect devices.

Remote Desktop Protocol (RDP) Exploits

While RDP facilitates remote computer connections, it becomes a vulnerability when weak credentials are employed.

Cybercriminals exploit such weaknesses to manipulate systems, encrypt files, and demand ransom payments for access restoration.

Malicious Software and Downloads

Cybercriminals often host websites offering free downloads of software, apps, and movies, enticing users to unknowingly infect their devices with malware, including ransomware.

Caution should be exercised, and downloads should be sourced from reputable platforms.

USBs and Removable Media

Ransomware can also infiltrate devices through removable media like USBs and external hard drives. Users should exercise caution, keeping removable media secure and refraining from plugging potentially compromised devices into their systems.

Top 3 Ransomware Families[6]

LockBit3
LockBit3 operates under a Ransomware-as-a-Service (RaaS) model and appeared around September 2019. This ransomware primarily targets large enterprises and government entities across multiple countries. Interestingly, it avoids targeting individuals in Russia and nearby countries.

8Base
The 8Base group has been around since at least March 2022 but became more famous in mid-2023 for being extra active. They use different kinds of ransomware, with one called Phobos being quite popular. What's notable about them is how they use advanced techniques and double extortion tactics.

Akira
Akira Ransomware showed up at the start of 2023 and doesn't pick sides between Windows and Linux computers. It spreads through things like infected emails or flaws in virtual private networks (VPNs). When it infects a computer, it scrambles up files and adds a ".akira" tag to their names. Then it asks for money to unscramble them.

[6] Checkpoint 'January 2024 Most Wanted Malware'

Consequences of A Successful Ransomware Attack

Ransomware attacks have far-reaching consequences that extend beyond the immediate loss of data or system. The ramifications of these attacks are profound and wide-ranging, impacting individuals, businesses, and even entire communities.

Here are some common consequences of ransomware attacks:

Ransom Payments

Ransom demands can be exorbitant, with no guarantee of receiving the decryption key even if paid.

Data Breach

The exposure of personal or sensitive information could result in privacy breaches and potential legal consequences.

Downtime Costs

Businesses face significant downtime during and after ransomware attacks, resulting in lost productivity, revenue, and potential contractual penalties.

Recovery Costs

Restoring operations post-attack requires more than ransom payment; businesses must invest in rebuilding and enhancing cyber security, incurring substantial costs.

Reputational Damage

Ransomware attacks have lasting impacts, damaging businesses' reputation and trust among stakeholders.

Legal Consequences

Data breaches from ransomware attacks can lead to legal action and fines under data protection laws for businesses that fail to safeguard sensitive information.

Best Practices for Preventing Ransomware Attacks

Thankfully, numerous strategies exist to prevent against ransomware attacks. As technology evolves, adhering to fundamental cyber security practices and maintaining vigilance is key to safeguarding yourself and your business.

Backups

Follow the 3-2-1 backup rule: keep three copies of data in two locations, with one copy stored off-site for disaster recovery.

Employee Training

Educate employees on spotting phishing emails, suspicious links, and avoiding unknown attachments.

Software Updates

Regularly update software to install the latest patches, preventing exploitation of system vulnerabilities by cyber attackers.

Access Control

Employ robust access management to limit unauthorised access, thereby reducing potential entry points for ransomware.

Email Security

Use email security measures to block malicious executables, spam, phishing, and other common email-based ransomware attacks.

Anti-Virus

Deploy comprehensive anti-virus and anti-malware software to scan for, detect, and respond to cyber threats effectively.

Firewalls

Utilise firewalls as the first line of defence against external attacks, protecting against both software and hardware-based threats.

Network Segmentation

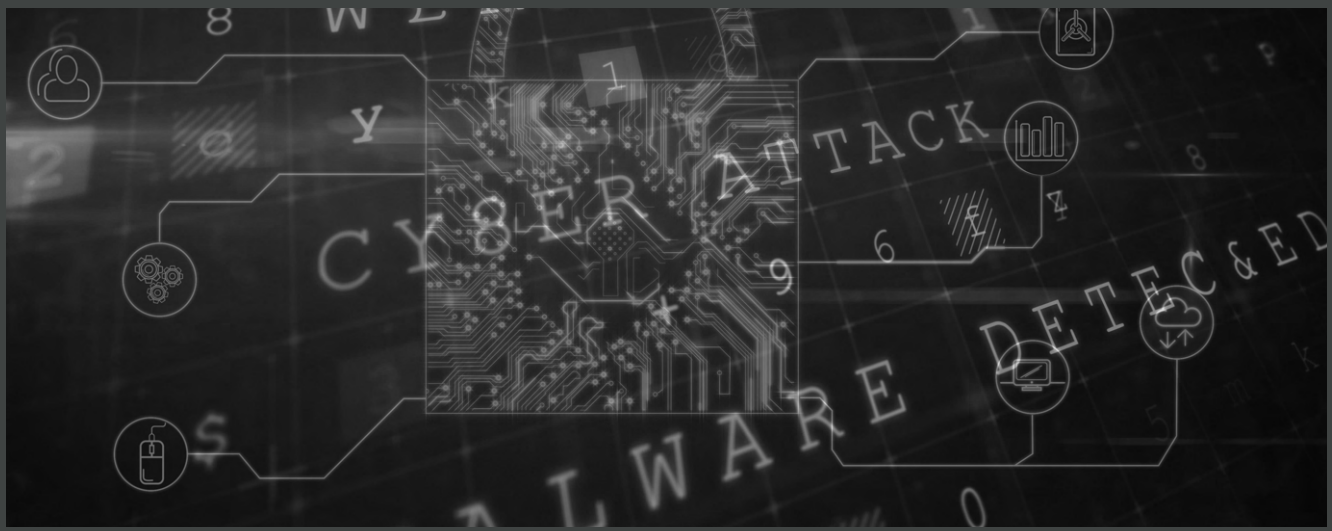
Divide your network into logical segments to enable isolation in the event of a ransomware attack.

Dark Web Monitoring

Stay ahead of potential threats by monitoring the dark web for any signs of compromised credentials belonging to your organisation.

Security Testing

Regularly conduct cyber security vulnerability assessments to adapt to evolving ransomware tactics and enhance security measures.



Working with a Cyber Security Firm To Protect Ransomware Attacks

Protecting against ransomware attacks is increasingly challenging due to the surge in sophisticated techniques. In-house IT teams often lack the expertise and resources to effectively address all threats. A reputable cyber security firm offers invaluable assistance in mitigating threats and defending against ransomware attacks.

How We Can Help

Expertise

Our specialised cyber expertise bridges your skills gap and remains ahead of evolving threats and new ransomware techniques.

Bespoke Solutions

We offer tailored security solutions to minimise data exposure and maximise protection against evolving cyber threats.

Proactive Threat Prevention and Detection

Our cutting-edge tech anticipates and neutralises ransomware threats, ensuring continuous network security.

24/7 Monitoring and Support

Our solutions continuously monitor your network activities, promptly isolating any attacks to swiftly contain damage.

Recovery Plans

We offer comprehensive backup and recovery plans to minimise the impact of data loss and downtime.

Employee Training

Our training ensures all staff adhere to your security policy and understand how to prevent ransomware attacks.

Conclusion

Businesses may dismiss cyber security, thinking, “No one wants my data, so why bother hacking me?” However, this overlooks the ransomware threat. It’s crucial to be proactive! While you may underestimate your data's value, ransomware attackers don’t.

Ultimately, prevention is crucial against ransomware attacks. With an average cost of $4.54 million and recovery expenses circ. $1.85 million[7], investing in proactive measures is vital. Isn’t it worth safeguarding your business from potential downtime, reputation damage, and customer dissatisfaction caused by hackers and ransomware?

Ready to enhance your company’s cyber security and protect against ransomware attacks? Book a consultation at **info@onecollab.co.uk** for tailored advice and minimise vulnerabilities.

[7] Express VPN ‘The True Cost of Cyber Attacks in 2024 and Beyond.’

OneCollab

Find Out More:
www.onecollab.co.uk

@onecollablimited

+44 20 8126 8620

info@onecollab.co.uk