


RESISTING RANSOMWARE:

Strategies to protect your **business** and your **customers**





Here's a hard truth every business owner must face: if you use computers in any way, you're a target for ransomware, the sort of malware that encrypts files and demands a ransom for the decryption key. When this type of attack hits your system, your data – and your business – is in the hands of the hacker, and you're often powerless until you pay up.

The bad news is that ransomware-related crime is getting worse. Hackers are launching more sophisticated attacks more frequently, demanding higher ransoms with no guarantee of returned files. What would happen to your business if ransomware hijacked your sensitive data? The grim reality is that many companies would flounder.

When it comes to ransomware, prevention is the name of the game: whatever you're willing to pay in ransom is likely significantly more than an investment in preventative measures would require. With the help of this white paper and our tailored cyber programs, you can refine your strategy and lay out actionable steps to help defend your business against ransomware attack.

You may be vulnerable, but you're not powerless	4
Big profit, low risk: why cyber criminals love ransomware	6
The ransomware racket is evolving (and fast)	8
Strategies to sidestep ransomware attacks	10
Planning your response	12
How we can help	14





You may be vulnerable, but you're not powerless

Ransomware can be more damaging than you might imagine, since data is at the heart of your daily operations. Not sure how an attack would impact your business?

Ask yourself these questions:

- What would it cost your customer relationships if you had to request fresh copies of their data after a ransomware attack?
- How long could your business pay its operating costs without incoming revenue?
- Does your company know the best practices for preventing and recovering from ransomware?

There's a lot on the line when you store data – a single breach could have immediate and long-lasting consequences. Fortunately, a well-constructed plan can help get you up and running a few hours after the event.

The key is to create a comprehensive response, tailored to your company's unique needs and focusing on:

- **Employee training.** Empower your employees to detect and deny criminal efforts, even as they grow more sophisticated.
- **Process audit.** Ensure that your recovery plan and response team are prepared to act quickly.
- **Technology recommendations.** Optimize your IT architecture to detect and eliminate as many strains of ransomware as possible.
- **Regular backups.** Protect your data by backing up frequently and testing the integrity of those backups regularly.

Constant and widespread security threats in today's digital landscape mean you must stay focused in your planning, and vigilant with your research. Keeping on top of trends in cybercrime and learning how and why thieves choose the routes they choose can help you focus your attention where it needs to be – and escape financial disaster.



Keeping on top of trends in cybercrime and learning how and why thieves choose the routes they choose can help you focus your attention where it needs to be – and escape financial disaster.

Big profit, little risk: why cyber criminals love ransomware

Easy to perpetrate and instantly profitable, ransomware is the darling of the digital underworld. Ransomware attacks in the business arena have spiked in recent years, and now it seems to be the preferred revenue-generating mechanism for the dark web.

There are several reasons for this rise in ransomware's popularity.

1. Its Efficient.

Every organization has unique information that's vital to operations. An inability to access that data, the ensuing disruption to regular revenue-generating operations, and the potential harm to your reputation [make up a compelling reason to pay the ransom.](#)

2. It's low risk.

Most ransoms are extorted in cryptocurrencies, like Bitcoin, making them untraceable. Plus, the data doesn't need to be sold on the black market to turn a profit: the payout is derived directly and solely from the victim. Fewer steps and fewer interactions make it less likely that criminals will blow their cover.



3. It's easy to deliver.

[More than 97 per cent of phishing emails contain ransomware](#) – it's designed to move through emails with malicious links and malicious attachments.

4. It's profitable.

Perhaps the most motivating factor is also the simplest: ransomware requires little investment on the part of the criminal, but it can potentially return significant and consistent monetary rewards.

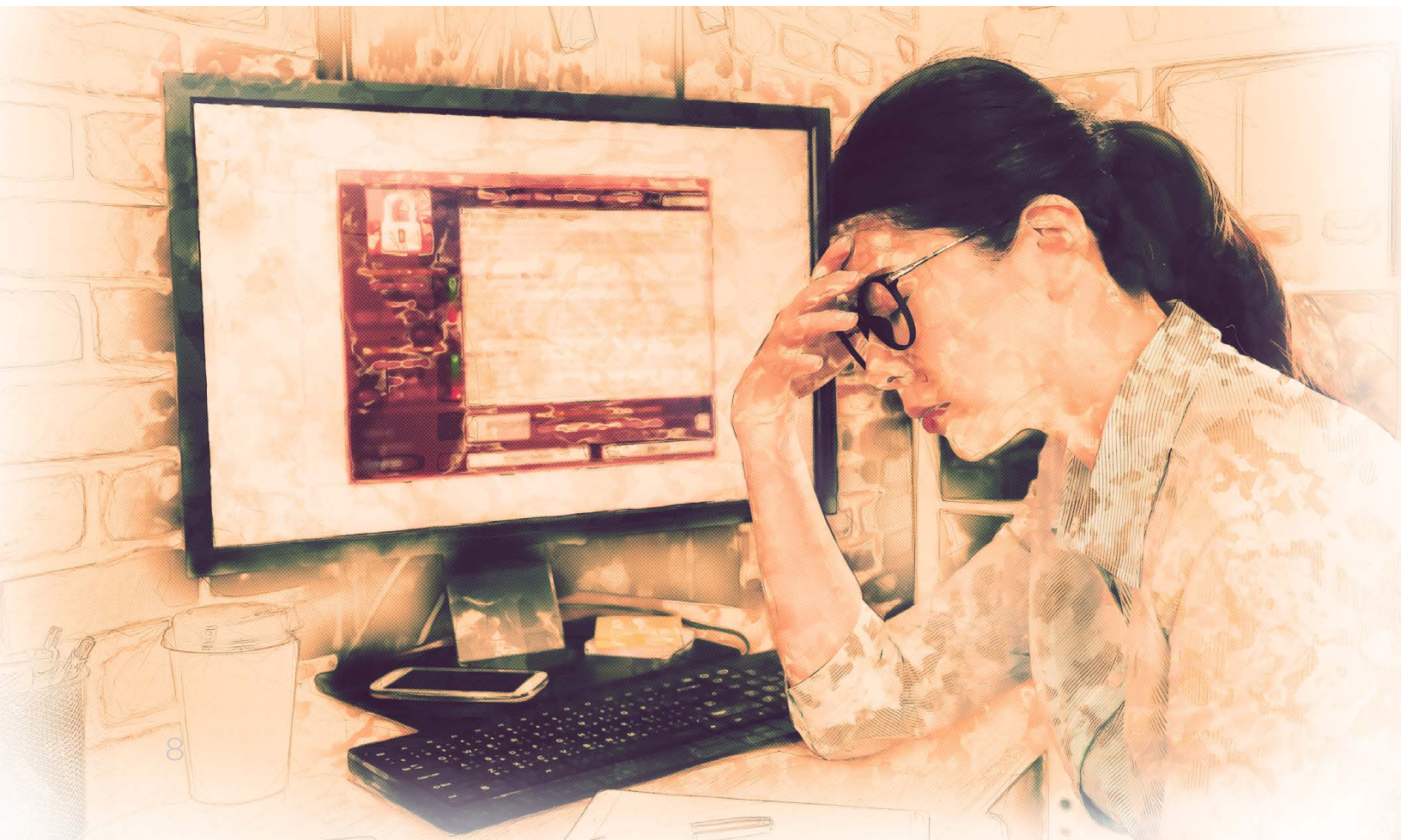


More than 97% of phishing emails contain ransomware – it's designed to move through emails with malicious links and malicious attachments.

The ransomware racket is evolving (and fast)

Ransomware profits can differ according to the breadth and depth of the attack, but recent events have returned startling results. The WannaCry attack of 2017 was globally devastating; some experts estimate [financial losses could reach up to \\$4 billion US](#).

In fact, 35 per cent of business executives who have encountered workplace ransomware attacks said their companies paid that ransom, and [20% of them paid more than \\$40,000](#). Due to the relatively low entry barrier and the potential profits, the ransomware model has been used against corporate entities more and more – [attacks increased 600 per cent between 2014 and 2016](#).

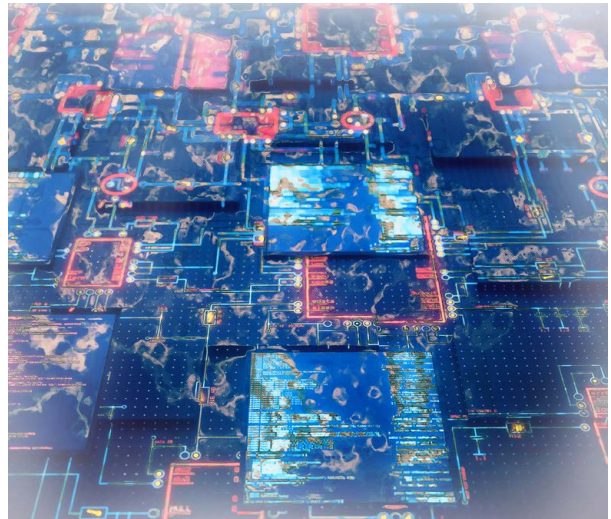


The high profits of early versions of ransomware have encouraged hackers to invest in more sophisticated methods, and they're encouraging others to hop on board, too. Today, criminals without programming resources can turn to [Ransomware-as-a-service \(RaaS\)](#) platforms to rent malware for a flat fee.

Some versions of RaaS are easily decrypted, but others are more robust, and aging IT networks may not measure up to the newest malware.

Your best defense? Updating your system, as well as your data protection practices to better shield your business from the growing ransomware threat.

How vulnerable is your company? The ransomware threat is widespread and severe – take a look at the statistics for a better idea of your risk.



Some versions of RaaS are easily decrypted, but others are more robust, and aging IT networks may not measure up to the newest malware.

Strategies to sidestep ransomware attacks

The threat is frightening, but there are some trusted methods you can use to help defend your data.

Your prevention measures should include three complementary strategies:

1. Empowering employees to detect and deny attempted ransomware infections
2. Optimizing your information technology (IT) architecture to detect and eliminate ransomware threats automatically
3. Auditing and practicing your planned response to a successful attack

With these key goals in mind, the following best practices will help you build out a stronger digital defense plan.



Back up files regularly

If your data is encrypted, a backup may be the only way to recover it. Decide on the longest stretch of time you're comfortable going without a backup, then back up your data accordingly. So, if you don't want to lose more than a day's worth of data, back up every 24 hours – it's that straightforward.

Secure your backups by ensuring they're not connected to the computers and networks they're in charge of backing up. The cloud or a data center works just fine. Note that some ransomware can lock cloud-based backups when the system is configured to back up continuously, so check with your provider about how they mitigate that threat.

Not only do you need to back up your data, you need to be able to trust those backups will work as expected. Be sure you test and monitor the integrity of your backups to ensure you can count on them when you need them.

Focus on awareness and training

The majority of ransomware succeeds by tricking users into clicking malicious email attachments and links. Teach employees how to spot phishing emails; to avoid clicking on banners or links without knowing exactly what they are, where they go, and who they're from; and to only visit trusted sites. It's crucial that your team is aligned when it comes to digital best practices.

If you have an internal or client-facing newsletter, share summaries of the latest permutations of ransomware. Even if a fraction of your workforce is made aware of the current threats, that could be enough to avoid a devastating attack.

Maintain next-generation anti-malware software

In some cases, these applications can catch the ransomware packages on their way in. Ensure that these solutions are set to update automatically and conduct regular scans.

Keep all software current

The fewer bugs you have, the harder it becomes to infect your system. Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered, including Adobe

Flash, Java, and web browsers. This precaution can be made easier through a centralized patch management system.

Implement protective IT policies

Your IT team is an important first line of defense. Here are some things your IT experts can do to help:

- Only allow systems to execute programs known and permitted by security policy.
- Prevent programs from executing in common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs, including those located in the AppData/LocalAppData folder.
- Disable macro scripts from files sent via email. When possible, use Microsoft Office.
- Use viewer software to open Office files sent via email instead of the full Office Suite applications.
- Categorize and segment data based on its value and utility. For example, sensitive research or business data should not reside on the same server or network segment as an email environment. Configure firewalls to block access to known malicious IP addresses.
- Disable Remote Desktop Protocol (RDP) if it's not being used.
- Make sure there are no mapped drives that a virus can easily access. Some ransomware families like VirLock and Locky can access and encrypt shared network drives, spreading the ransomware infection across an entire organization.
- Tighten email policy. Strengthen spam filters to prevent phishing emails from reaching end users, to authenticate inbound email to prevent email spoofing, and to filter executable files from reaching end users.
- Establish a phishing testing program. Periodically send fake phishing emails to employees with a safe landing spot. See how many people fall for it and use the results as teachable moments and gentle reminders.

Planning your response

Sometimes ransomware can sneak through a company's defenses, but it's possible to shut down and contain an attack if you act right away.

You'll want to have a response plan in place to help limit the damage done and forge a clear path to swift recovery. The first 48 hours are particularly crucial; we've laid out some steps you can take to stay on top of the problem in another whitepaper - [find it here!](#)

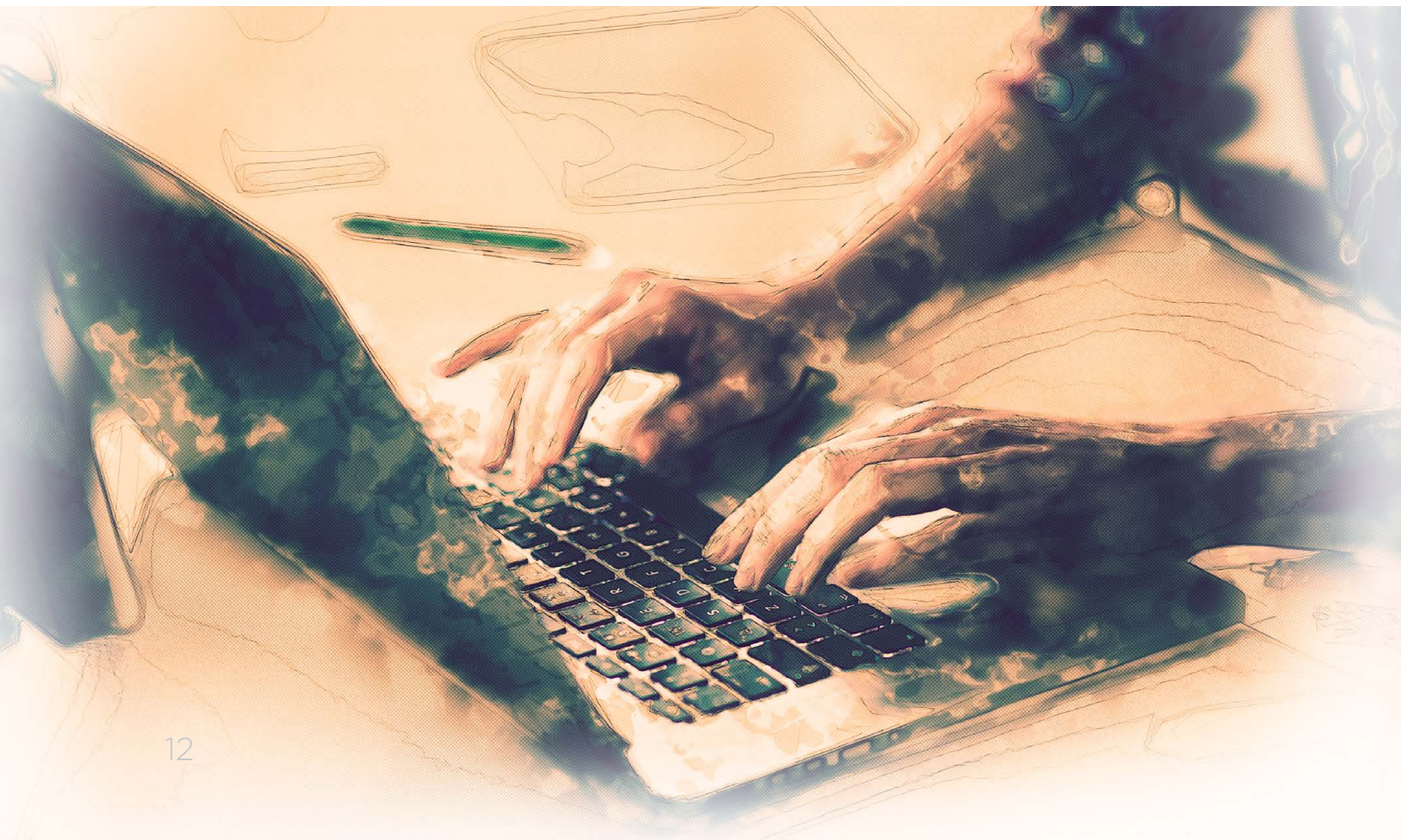
How will you regain control?

You'll need to take control of your system as soon as possible. Wipe hard drives, restore your systems, and download clean versions of your files from an uninfected functioning backup. Run a scan.

Who should you contact?

Depending on the severity of the attack and the size of your internal team of experts, you may need to reach out to:

- **Law enforcement.** if law enforcement needs to conduct a forensic investigation on your computers or servers, you may also need to obtain temporary server space to restore your systems



- **Service providers.** Contact your providers of IT services and cyber security monitoring, if you have them.
- **Legal counsel.** Legal specialists can help determine if a data breach has occurred and take the appropriate steps to inform the affected parties and remediate the situation.
- **Your insurer.** Your insurance contact can do more than sort out a claim. You should be able to count on them to connect you with breach coaching, legal counsel, specialized IT professionals, and other experts to help you respond and recover.

Make your response plan more than a technical exercise. Remember that it isn't the responsibility of network administrators or software engineers to resolve the expensive, sticky issues that follow a technical resolution, like notifying clients and staff in accordance with legal mandates or interfacing with the media and law enforcement. Be sure you have experts in every corner.



Remember that it isn't the responsibility of network administrators or software engineers to resolve the expensive, sticky issues that follow a technical resolution, like notifying clients and staff in accordance with legal mandates or interfacing with the media and law enforcement.

How we can help

Now that you know how much havoc ransomware can wreak, and that the threat is likely to continue, you can apply focused guidance to stay resilient. But while it's important to protect your business as well as you can, the right insurance can come to your rescue if your efforts fall short.

Not all cyber risk insurance is created equal. Without the right partnership, legal fees and fines, repair costs, and business interruption expenses that come with a ransomware attack could fall on your shoulders. And as ransomware becomes more sophisticated and far-reaching, a single attack can bring on serious financial trouble.

Together with CyberScout, Northbridge Insurance has developed a versatile and comprehensive [cyber risk insurance](#) program: your policy can protect your bottom line if you suffer a breach, but it also grants you access to extensive cyber resources to help you protect, assistance to help you react, and personalized guidance to make sure the same thing doesn't happen again. After all, risk management is an ongoing responsibility, and Northbridge takes that seriously with comprehensive policies that keep your company's long-term success in mind.





This whitepaper is provided for information only and is not a substitute for professional advice. We make no representations or warranties regarding the accuracy or completeness of the information and will not be responsible for any loss arising out of reliance on the information.

Northbridge Insurance and Northbridge Insurance Logo are trademarks of Northbridge Financial Corporation, licensed by **Northbridge General Insurance Corporation** (insurer of Northbridge Insurance policies). [3808-003 ed01E]