



CG Technologies

White Paper

The Small Business Guide to Ransomware Protection



What is Ransomware?

Ransomware is a type of software code or malware designed to disrupt your business, and it aims to hold your company hostage until you pay the attacker a fee to release you from their clutches. What separates ransomware attacks from other attacks is the sole intent of hijacking your systems and your business for monetary gain by the perpetrators.

Technology-focused roles should focus on the technical ransomware definition, while business leaders should focus on protecting the business from external ransomware as a Service business threat. The goal of ransomware is to profit at your expense.

How Does Ransomware Work?

Before a ransomware attack can even begin, the attacker must first find a way into your business systems and then encrypt your data, leaving you locked out of your files, even if just temporarily. The attacker then threatens you that if you don't pay, they will make it permanent. Their goal is to make it cheaper or easier for you to pay than to recreate the systems your business runs on.

The business decision to be made is a cost vs benefit strategic choice; pay early for ransomware prevention or pay later after the ransomware attack brings your business to its knees.

Types of Ransomware

There are three main ways that hackers extort money from your business:

Locker ransomware:

This type of malware deprives your business of access to its vital hardware systems. Every business has desktops, laptops, servers, routers, NAS systems, and other hardware systems with one form of operating system. The goal of locker ransomware is to deny the use of this hardware unless you pay to get it back.

Crypto ransomware:

This type of malware deprives your business of access to its data. Typically, the ransomware virus will encrypt all or just part of your data, making it completely unavailable to you. Partial encryption makes it more difficult for your ransomware removal tools to discover the ransomware attack.

Data Exfiltration Attack:

This type of attack occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft.

In all cases, the extortion racket is the same. If you pay, they promise to restore your systems or not share your data, but it is not guaranteed.



Types of data that is targeted includes:

- Usernames, associated passwords, and other system authentication related information
- Intellectual property
- Personal financial information
- Social security numbers and other personally identifiable information

The Ransomware Threat is Real

News about ransomware seems to be increasing in numbers and scale. However, you can protect your business by treating the threat as any other external business threat that needs to be understood and incorporated into your business operations planning.

Peace of Mind Starts with a Plan

The 5 Steps to Protection for Small Businesses

Your company and the systems it relies on to run your business are a critical part of your operations. Without your technology running reliably, your business will soon cease to exist. Imagine trying to run your business on paper or relying on snail mail to communicate with your clients and potential customers. Just like this advisory guide, your audience, customers and employees are digital natives.

Your business runs on technology and data, and the attackers know this.

There are 5 important steps to securing your businesses future.

1. Identify the Risks
2. Evaluate and Consider Possible Vulnerabilities
3. Evaluate the risk level and your tolerance for that risk
4. Risk Mitigation Requirements and documentation
5. Continuous Monitoring and Reporting

*Let's face it, you don't know what you don't know,
and unless you are a security professional, it is only
a matter of time before you could be the next victim of
a ransomware attack.*



Here are some helpful tips to guide you to a safer business and avoid a ransomware attack.

Prevention is the Best Medicine

The best ransomware protection begins with preventing the ransomware attack from penetrating your business. This requires technology solutions like firewalls and virus protection that places a strong technology boundary between your business systems and the external threats. Edge protection also has a human element. The most common way for ransomware attacks to harm your business is for your employees to let a ransomware virus in inadvertently. Train your staff to recognize and defeat human phishing attacks and how to identify and avoid other ransomware risks.

Edge Protection

It isn't enough to rely on your edge protection being foolproof. Trust but validate your internal systems communications and integrations. Segment internal systems and increase edge protection and harden endpoints so that if a ransomware attack is successful, it doesn't bring your system down completely.

We have all seen movies where the bad guy gets away by wearing a police or fire department uniform after creating confusion. Train staff to trust, but verify, internal human interactions as well as trusted vendor interactions, especially when in the midst of chaos.

Invest in anti-ransomware solutions such as:

- **Anti-Virus software which incorporates behaviour detection**
- **Firewall protection**
- **Monitoring, security, and event management systems**
- **Ransomware detection systems**
- **Ransomware removal systems**
- **Ransomware decryption tools**
- **Ransomware recovery systems**
- **Patch management systems**
- **Data management systems**
- **Backup systems**

1. Detecting Ransomware

The ransomware threat is real enough that business resources should be allocated to detecting ransomware in all business systems. Ransomware detection should be built into technology systems from edge systems all the way to your most core systems.

Detect ransomware attacks to your “human systems” as well. Continuously train your staff to look out for, recognize, and respond to any suspicious activity. Have a simple, easy way for employees to report suspicious emails, log activity, interactions with vendors, and innocent-sounding phone calls. The goal is not to create paranoia but to create awareness and an easy programmed response that works. The response should be as easy as, *“If you get a suspicious email, forward it to suspicious_email@mybusiness.com.”*

2. Protecting Your Data

Be comprehensive with your data protection; eight digits may be all it takes. All data from your hardware systems configurations, their passwords, your accounting data, and your customer data are potentially essential to the success of your business. One early famous ransomware attack came down to only one disgruntled employee having the eight simple digits that granted access to all of the city’s routers (default admin passwords). When he scrambled the routing tables, the city’s systems came to a standstill.

3. You need a data plan that includes protection against ransomware attacks.

Strong measures should be taken to separate operational working data from trusted online source data. Data should be separated and segmented by systems, services, and business organization. Most importantly, physical backups that ransomware viruses cannot alter must be available as a trusted source from which to restore.

4. Every vital system should be rapidly replaceable or restorable.

Maintaining precise knowledge of key hardware configurations and making it available to incident response teams allows for rapid replacement of compromised hardware, significantly reducing the business damage an attack can cause.



5. Know your Systems Weaknesses

Don't wait for a ransomware hack to expose your single points of failure. Know what they are in advance. Comprehensive knowledge of your technology systems and how they integrate to deliver business value is essential both in preventing attacks and recovering from attacks.

You need to understand how things are connected to better understand what and where your vulnerabilities are.



Single Points of Failure:

- Harden the most obvious points of failure as best you can
- Eliminate single points of failure wherever you can
- Where is your data stored or does it come from?
- Do you understand the flow of data in your organization?
- Data may allow malware to piggyback on it and access your systems and wreak havoc
- What other key areas leverage essential data from these systems?
- How integrated are your internal systems with external vendor systems?
- And, what is their vulnerability?

6. Consider Cloud Options

Small and medium-sized businesses often lack the specialized resources to implement advanced ransomware prevention measures. When you add the real threat of ransomware attacks into your cloud vs on-premises decision-making criteria, the cloud may become a more enticing alternative.

The better decision for a smaller business is often to use technology services such as cloud services to ensure a level of protection and certainty of service that is difficult to achieve for businesses operating at a smaller scale, especially where the external threats are new, novel, and unpredictable.

While cloud services may not be completely immune from malicious attacks, they have the specialized resources required to provide much greater protection than most small and medium-sized businesses can afford on their own. Just keep in mind that nobody is absolutely immune. Using cloud services is not an excuse to ignore planning; they just reduce the risk that a response will be necessary.

7. Train your Employees – Knowledge is Power

Having knowledgeable staff on security and how to protect your business is one simple way of securing your business. Phishing emails is a very common method or technique used by cybercriminals to access your systems or data.

They use emails that look genuine but contain malicious links and sometimes even code that gives them access. When your employee innocently clicks on a link, the criminal can launch an attack on the user's system or the IT systems they are connected to.

By having a well-informed staff, your organization is one simple step away from preventing a ransomware attack. Remember, the attackers need access to your systems to hold you and your business hostage. Without that access, your systems and your business are much safer.

8. Find a Partner

Businesses of all sizes have gaps in their ability to run IT. Even large organizations with full staffing of IT professionals rely on external experts to support their business from a technology standpoint. Finding a trusted IT partner is important to helping your business become more secure, informed and prepared when IT systems fail or there is a breach.

9. Plan for the Worst, Hope for the Best

Hoping you are never a target for a ransomware attack is not a replacement for planning how to prevent and respond to ransomware attacks. If all preventative measures fail and you are successfully hacked, having a ransomware attack response plan is essential; your advanced planning can mean the difference between a business inconvenience or a business failure.

Please don't wait until it happens to start deciding how to respond. If you can rapidly and successfully restore your systems without resorting to paying ransomware extortion, then you demonstrate that your business is not a profitable target, and you gain credibility in the marketplace.




Conclusion

The threat of ransomware is real and a growing external threat to your business. It is a particularly scary external threat because of the hostile intent involved in a ransomware hack versus the indiscriminate actions of mother nature. Risk is risk, don't be lead astray because the nature of one risk is scarier than another.

The best way to protect yourself is to have a layered approach to security that includes staff education if your network is replicated to an offsite datacentre, a full image-level backup. This acts as an insurance policy in the event you are the target of a ransomware attack.

The most important thing you can do to create peace of mind is to have a solid business availability and reliability plan designed to address all external threats that uses risk analysis techniques to determine how to and how much to prepare. Don't panic based on the latest media scare. It will have you in a constant state of anxiety and cause you to overspend on the wrong things and underspend on the important things.

Planning is critical and continuous updates to your plan that incorporate new threats and new technologies will help you maintain a solid security posture. While it is true that no plan survives the first contact with an enemy, the act of planning itself remains essential to your businesses ability to successfully prepare for and respond to whatever external threats may come its way. And, should you be hit with a successful ransomware attack, you will be prepared and have the confidence that your business will survive and that you will not be at the mercy of the criminals who launched it.



Be More Secure! Call Us Today.
(416) 244-4357

About CG Technologies

To learn more about all the services CG Technology has to offer, call us at: (416) 244-4357; email a Solutions Expert at: sales@CGTechnologies.co; or visit: www.CGTechnologies.com