CYBERSECURITY TOOLKIT

clearbridge

TOP 12 CYBERSECURITY TIPS TO REDUCE BUSINESS RISK

Learn the **TOP 12 WAYS** you can ensure your business is cyberready and aware.

203-2600 Gladys Ave
Abbotsford BC Canada V2S 0E9
support@clearbridge.ca
(778) 383-6726

Clearbridge helps businesses with more than just tips to best manage IT. We help by leading your digital strategy efforts through investments in technology. Connect with us to learn more about how Clearbridge can help your business. Talk soon!

Table of Contents

Introduction

Clearbridge Business Solutions is an operationally focused team of business and technology experts. We help businesses (and their people) focus on what they do best by delivering on their IT strategy, security, and support needs.

Our team strives to provide high-quality business-centric results through our under-promise and over-deliver model. We serve organizations local to our community and remote across Canada and the US.

We love technology and the optimization it can bring to a business. We leverage IT only in the best places, in the right ways, where it can create more value than the required investment.

As a team of business and technology enthusiasts, we show up each day to work on what we love. We strive to make this evident through our communication and results. We look for the #bestwayspossible, so our customers can do the best work they've ever done!

Our Promise

Cybersecurity is our top priority. We want to empower you and your business to get on the right path to cyberresilience, minimizing your risk of exposure to cyberthreats and attacks. That's why we've built our **Cybersecurity Toolkit** to provide you with valuable resources that will teach you how to protect and secure your data and information.

1 - Remember, It Can Happen to You!

The number one thing you need to keep in mind is that YOU ARE A TARGET.

Many businesses think their data is not valuable enough to worry about, but that is not the case!

You are an attractive victim to hackers because you may not have the same defences as larger companies.

So, cybersecurity should be your priority. If you have money and data that might be desirable to hackers (like passwords, your customers' information, or sensitive content) being complacent will not help.

Once you drop your guard, you will be more at risk! Take time to know and understand your assets and put practical protection measures in place.

2 - Practice Good Password Management

8	#	CAT	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Zz
USE NUMBERS	INCLUDE CHARACTERS	AVOID REAL WORDS	PRIORITIZE LENGTH	USE UPPER & LOWERCASE

Example: 8N#cl<ErS$W3&0mZ

Password security is critical for your business. Hackers continue to think of new and sophisticated ways to hack accounts and access your business' and employees' personal data.

Ensure your employees are using strong, lengthy, and random passwords as this will drastically reduce the likelihood of a hacker guessing their password.

Another big no-no? Using the same password for multiple accounts. Passwords should also not be shared with anyone, even family or a close friend.

A couple of ways to up your password security: consider using a password manager like LastPass and enable multi-factor authentication (MFA).

Learn more about creating strong passwords here.

3 - Educate Employees On Safe Email Practices

CONTACT THE SENDER

If a message seems to come from someone you know, contact that person via text message or phone call to confirm it.

>

REPORT THE MESSAGE

Contact the Fraud Reporting System (Canadian Anti-Fraud Centre) or call toll-free at 1-888-495-8501.

>

DELETE IT

Delete it to prevent yourself from accidentally opening the message. Do not download any attachments.

Be vigilant of 'spoofed' email addresses that appear to be coming from a trustworthy source. Hackers are very crafty.

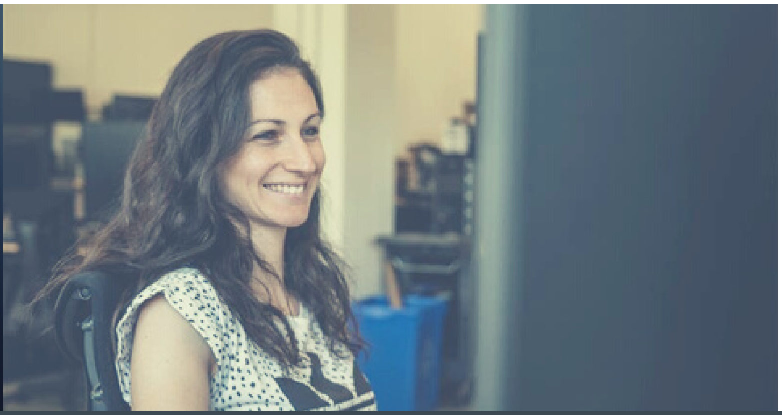
If the email address does not match the sender's name, you could be looking at a phishing email. Be wary!

Stop automatically opening emails or following their links. Look for spelling and grammar mistakes and lengthy URLs with odd or unfamiliar extensions.

Pay attention to the details. For example, if the email contains characters in place of regular letters, this could be a hacker working their magic.

Recognize the other signs of phishing emails—does it seem too good to be true? Is it claiming that you've won a large sum of money? Is it promoting unprompted offers or opportunities?

Learn more about safe email practices here.



4 - Enable System Access Only as Required

An organization should avoid implicit trust and continuously validate every stage of a digital interaction. Every access request should be fully authenticated, authorized, and encrypted before granting access.

VERIFY THE USER

VALIDATE THE DEVICE

LIMIT ACCESS

Begin with the end in mind.

Staff should only have access to the data and systems required to do their jobs. No exceptions.

When an employee leaves the company, ensure that their access is removed and enable multi-factor authentication (MFA) for any accounts they previously had access to.

Never allow blanket access across teams or departments unless every member needs access to do their jobs.

User accounts with these privileges are attractive targets for cybercrime, as they hold a high level of system access.

It becomes more difficult for a hacker to access your sensitive information by minimizing privileges.

4 - Be Wary of External Devices

In our BYOD world, it's crucial to screen all devices before they connect to your network.

Many devices may carry malware, from computers and laptops to mobile devices and thumb drives.

Consider mobile device management (MDM) or mobile application management (MAM) to ensure that your company data can only be accessed by the right people.

In addition, this will allow you to remotely wipe devices, thus limiting their ability to become compromised.

Just remember that any device containing sensitive data connected to the company's internal network through VPNs and workspace browsers can be susceptible to an attack.

"We are a company of problem solvers. We create solutions to real business problems—often using technology as our tool—and we support those solutions inside of our customers' businesses in a fully integrated manner."

- Ryan Kononoff, CEO

6 - Back Everything Up

A basic cybersecurity rule: backup ALL your networks and systems regularly (both cloud-based and physical servers).

This practice should be standard but also outlined in your incident response plan (IRP). Always be sure to store the backup data away from the main server.

When faced with a cyberattack, you may need to completely wipe a device or server. By backing up and storing your data across multiple locations and offline, any infected systems won't be able to access it.

Also, ensure you regularly test that backups are being done correctly and that your data restoration procedures are effective.

7 - Make Sure Your Systems are Patched and Up to Date

Always keep your systems updated. Device and software manufacturers will release software patches to correct any flaws in the previous version.

You should also install the latest software updates as leaving your system on older versions may increase the chances of being exploited due to weaknesses and vulnerabilities.

It's a matter of getting into the proper habit.

You can reduce the possibility of becoming a target for malicious activity. Schedule routine update checks, turn on automatic updates, and use web browsers that receive regular and frequent security updates.

8 - Monitor and Test Your Networks

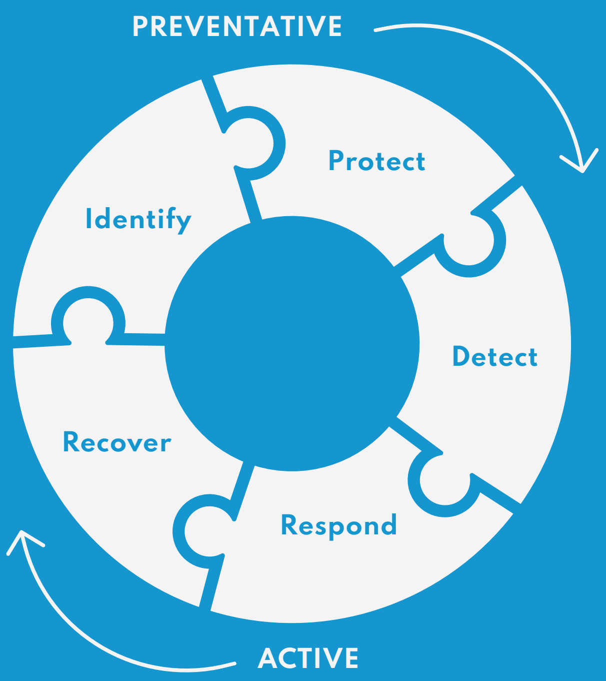
Your chances of avoiding a cyberattack increase when you persistently monitor and test your networks and devices.

If you notice suspicious activity or something that seems out of the ordinary, this could signal that one of your systems has been compromised.

As a rule of thumb - be involved and understand how distinct types of activity should normally look so you immediately notice red flags that identify potential attacks.

Penetration tests and vulnerability assessments can help detect any infrastructure weaknesses that could result in system vulnerabilities. This will determine your detection and response capabilities.

9 - Be Preventative



*Based on NIST Cybersecurity Framework

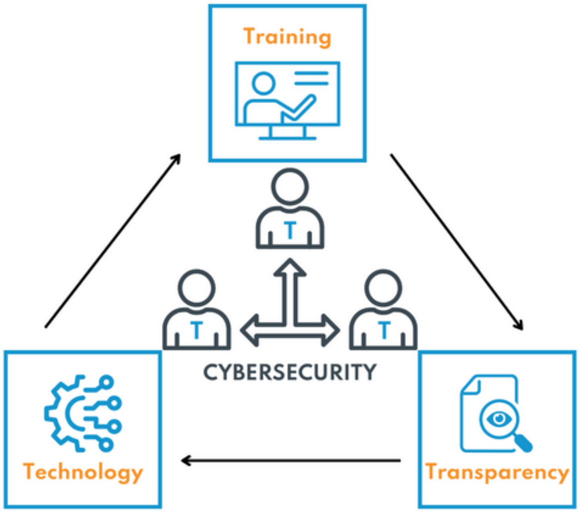
We always say, being PROACTIVE + ACTIVE is your best line of defence against cyberthreats. Altogether, it can save your company time, resources, and ultimately, money.

There are many different forms of precautions you can take. Email security can block malicious senders and attachments. A firewall can prevent attacks from various types of malware, like ransomware and hackers trying to steal your valuable data and information.

Another critical way to protect you and your business is to provide employees with cybersecurity training and education. We provide cybersecurity content on multiple topics that will help you gain more confidence in your ability to ward off cyberattacks. Check out our blog, Tech Tips page, and E-Books page for a ton of valuable resources!

10 - Follow the Three Ts

Employees should understand and be trained on company policies about software use, and data ownership.



Technology should support employees and employers in detecting, investigating, and responding to data breaches.

Employees should be transparent about what activities the company is monitoring on work-issued laptops.

The three Ts is a simple framework that businesses can consider prior to implementing a cybersecurity strategy and should be the first step to mitigating cyberthreats.

More comprehensive frameworks exist, such as The NIST Cyber Security Framework (CSF), which consists of standards, guidelines, and best practices for managing cybersecurity risks through a cost-effective approach.

The CSF is applicable to many different industries. Learn more here.

The Government of Canada's version of NIST, ITSG-33 provides baseline advice and guidance for IT security risk management. If your organization is looking for foundational enterprise security guidance, you should consider this framework.

11 - Train and Educate Your Employees

Security-related risks are reduced by 70% when businesses invest in cybersecurity training and awareness.

INCREASE AWARENESS

REDUCE THREATS

IMPROVE SECURITY

When it comes to your cybersecurity, humans are the weakest link. No matter how costly or effective your defensive technology is, one person lacking the knowledge to recognize and respond to an attack can cause horrible repercussions.

Fortunately, the power is in your hands to develop and implement cybersecurity training within your organization that will help arm your employees with what we like to call cyberreadiness and awareness.

Here are some extra tips:

- Keep up to date with Clearbridge training content, Tech Tips, and E-Books.
- Enforce a security mindset from day one.
- Review breaking news together and talk about the latest security vulnerabilities.
- Offer an incentive if they demonstrate outstanding cybersecurity awareness.
- Run drills to simulate an attack, such as phishing or ransomware.

12 - Be Prepared and Have an Incident Response Plan Ready

You're never fully safe from threats. Plus, they are always morphing and evolving. Hackers also have many tricks up their sleeves that can put them one step ahead of you.

We can help you create an incident response plan (IRP) that will act as a supportive document should you be faced with any serious challenges.

Some of the things that an IRP covers includes:

- Responsibilities for incident response team members.
- A business continuity plan (BCP).
- An outline of the tools, technology, and resources that should be in place.
- Network/data recovery processes
- An outline of the internal and external communications that should take place.

Use our template to get started!

"The absolute best way to protect yourself and your business from data breaches is to stay vigilant. Secondly, hiring a technology company to provide your business with cybersecurity audits and monitoring may help to identify weaknesses and ensure your network has robust security configurations in place."

- Ryan Kononoff, CEO

Thank you for reading our e-book!

Cybersecurity isn’t a single, one-size-fits-all solution. Instead, it’s a series of best practices you must implement and maintain. We're dedicated to equipping our customers with the tools they need to be cybersecure through managed IT services and educational resources. To learn more, reach out to us!

For support, contact us.

✉ www.clearbridge.ca

🌐 support@clearbridge.ca

☎ (778) 383-6726