CYBERSECURITY TOOLKIT

clearbridge

CYBERSECURITY AUDIT

25 STEPS to determine if your business is equipped to handle a cyberattack.

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

clearbridge

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!

Is Your Business Properly Equipped to Take On a Cyberattack?

This extensive **25-step Cybersecurity Audit** will help you determine if your business is set up to handle a cyberthreat of any size. Each step allows you to see if you are protecting your information, preventing data breaches and simply put, looking both ways before crossing the street!

1 - Have you implemented multi-factor authentication (MFA)?

☐

MFA can protect your business from up to **100%** of automated attacks. Since hackers do not have access to your device, they cannot complete the login process even if they get ahold of your username and password.

One effective way to add another layer of security to your procedures is to add Multi-Factor Authentication (MFA). Some system examples to focus on when implementing MFA include:

- Any system where you are storing important and confidential information, such as servers or cloud-based storage solutions.
- CRM (customer relationship management) and ERP (enterprise resource planning).
- Internet banking.
- Accounting and payroll systems.
- Email platforms (Office 365 and Google Workspace).

2 - Do you restrict certain administrative privileges?

Administrative privileges are the ability to make **major changes to a system**, typically an operating system. It can also mean large software programs such as a database management system.

Your administrative accounts should be used solely for functions and applications required for work purposes. If someone gains unauthorized access, this could result in your data being significantly compromised. Consider restricting administrative accounts from internet access and emails and change your admin privileges if you have not done so already.

Top 4 dangers:

- Higher risk of virus/malware infections.
- Computers becoming critically "messed up".
- Allowing hackers to create new user accounts.
- Attacking other devices on your network.

3 - Are you patching your operating systems?

A **patch** or **fix** is a quick-repair job for a piece of programming designed to resolve functionality issues, improve security or add new features. A patch is particularly important because it addresses known vulnerabilities.

All operating systems must be patched. Devices on the network or cloud should also be patched as unexpected vulnerabilities may not be discovered until after release.

- **Windows Updates**
- **macOS Updates**

Best practices:

- Set clear expectations and hold teams accountable.
- Work collaboratively with technical teams to ensure a common language.
- Establish a disaster recovery plan (DRP).

4 - Are you 'whitelisting' your approved applications?

Whitelisting is a type of access control useful for financial or personnel records, where a business might have only **2-5 employees** who access these files, software or websites.

Whitelisting is a list of approved applications that a computer or mobile device can access. It ensures that no new or malicious software can be executed or installed. Essentially, any software not on your whitelist could potentially be infected with malware. Learn more about implementing application control here:

- How to Whitelist Applications in Windows
- How to Whitelist Applications in macOS

Best practices:

- Document and categorize all whitelisted applications.
- perform regular reviews of whitelisted applications, and keep the list up to date.
- Place users into access groups and apply specific whitelists to each group based on job function.

5 - Are you performing daily backups?

In recent years, **millions** of sensitive business records have been compromised in backup-related gaffes. People realized after they needed a backup that their backups weren't being done, weren't being done off-site, or weren't working.

If your data is compromised, corrupted, or destroyed, you will need to access that information quickly. So, you must schedule daily backups of your most critical data.

- Windows Backups
- macOS Backups

Data backup guidelines:

- Play by the 3-2-1 backup rule:
  - Create three copies of your data.
  - On at least two storage solutions.
  - Store one of them in a remote location.
- Follow best practices:
  - Backup regularly.
  - Opt for more storage.
  - Do not underestimate physical copies.

6 - Are you taking advantage of a password manager?

Over **80%** of data breaches are due to poor password security.
A data breach can cost companies and individuals **millions of dollars,**
yet the measures employees take to prevent this are minimal.

You need to create long complex, and random passwords to keep your accounts secure. How will you remember them all? That is where a password manager comes in handy! Store all your passwords securely (they will be encrypted), then share them with your team safely. A great option is LastPass.

Pros of using a password manager:

- One password for everything.
- Automatically generated passwords.
- More security than other options.
- Works across your devices.
- Can be shared with a trusted person
- Increase productivity.
- Secure company credit cards.
- Usage report & activity logs.
- Never get locked out if someone leaves.

7 - Are you restricting access to your data?

One article cites data showing that **60%** of all attacks were carried out by insiders. Of these attacks, **three-quarters** involved malicious intent, and **one-quarter** involved inadvertent actors.

It is critical to regularly check your system and ensure your employees only have access to the data and networks they need to do their jobs. Plus, having fewer people with access to sensitive data will help ensure that data is less likely to be compromised.

- Learn About Control Permissions in Windows
- Learn About Control Permissions on MacOS

Reasons why you should restrict data access:

- Unrestricted user access can lead to accidental data exposure.
- User access can lead to intentional privilege misuse and abuse.
- Hackers can use compromised user credentials.

8 - Are you training your team about cybersecurity?

According to statistics, **90%** of "data leakage" is caused by human error, highlighting the need to train and educate employees on proper security practices.

Employees need to understand the diverse types of risks that are out there, how to mitigate a cyberthreat, and what steps to take should they encounter a cyberattack. Your team will be the ultimate defender if they are alert and aware. Here are some ways to engage your team:

- Keep up to date with Clearbridge Tech Tips, videos, e-books, and other security-focused training content.
- Start their cyberawareness from day one to enforce a security mindset.
- 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.

9 - Are you managing your mobile devices?

Mobility supports **communication**, **collaboration**, and greater overall **productivity**. Strong mobile security allows employees to access critical data while decreasing the risk of a security breach.

A mobile device management (MDM) plan protects your company data and employees' personal information. That way, you can provide staff access to business apps or data on mobile devices without individual device enrollment.

Benefits of MDM:

- The IT team can track and has full control over the device including applications.
- The IT team can remotely wipe, enforce password resets, encrypt the device, and take control over the device.
- Great for businesses that issue company-owned devices to employees.

10 - Are you managing your mobile applications?

87% of businesses allow employees to use personal devices to access business apps. The use of public and private apps is surging making it imperative for businesses to implement tools to streamline application use.

A mobile application management (MAM) plan supports a bring your own device (BYOD) workplace culture. Rather than managing an entire device, you can control required apps, along with their permissions and security overall.

Benefits of MAM:

- The IT team has control over company applications only and not over the user's device.
- The IT team can enforce policies so that the user can't access data if the device is not safe, encrypted, updated, or patched.
- Great for companies that allow for BYOD.

11 - Are your devices encrypted?

☐

Encrypting your phone makes your data **unreadable without a password.** Until that password is entered, all the data on your phone —including your text messages, emails, documents, and photos—is unreadable.

This is a necessity. Every device, including computers, hard drives, mobile devices, and storage, should be encrypted. This ensures that your data is incomprehensible without a key. Check out this specific information on encryption here:

- Device Encryption for Windows
- Data Encryption for macOS
- Encrypt your Android device
- Encrypt iPhone backups

2 types of data you should encrypt:

- Personally identifiable information:
  - Any kind of information another person can use to uniquely identify you (DL, SIN # etc.).
- Confidential business intellectual property:
  - Customer information, financial reports, product release documents, research & development data.

12 - Are you enforcing strong passwords?

90% of passwords are vulnerable to attack. The good news? Multi-factor authentication (MFA) blocks **99%** of all password safety issues. Check out our How to Create Secure Passwords blog post!

This is the key to your account's security. Do not create passwords that are easy to guess or hack; create a strong password policy in your workplace and be sure to enforce it. Your employees should create complex, random passwords as this will help boost security. Also, ensure they update them regularly.

Here are some extra tips:

- Use a mix of characters like capitalization, symbols, and numbers.
- Use a different password for every account.
- Use multi-factor authentication (MFA).
- Create passphrases that include at least four words you can remember.
- Never include personal information or meaningful dates.
- Review the Government of Canada's password etiquette.

13 - Is your email secure?

Approximately **15 billion** spam emails are sent daily; **45%** of all email is spam (and some researchers believe that number to be closer to **75%**.) making it easier for malicious phishing attacks to slip through.

Many organizations are threatened by malicious activities, so your employees should be wary of every email they come across. Follow the steps here to identify and handle malicious messages. Various measures can protect you by verifying senders and recipients to prevent malicious emails from coming in or out.

Top 5 ways to protect employees from phishing scams:

- Conduct company-wide cybersecurity training.
- Teach employees how to identify a phishing email (and quiz them).
- Show real-life examples of data breaches caused by phishing.
- Use trusted antivirus software and ensure it's routinely updated.
- Make sure executives are involved in your security initiative.

14 - Are your physical assets protected?

Remember that network security starts at the **physical level**. All the firewalls in the world won't stop an intruder who is able to gain physical access to your network and computers, so **lock up** as well as **lock down**.

Protect your physical assets by restricting access to your critical equipment as data can be compromised. Here are some quick tips:

- **Lock your dedicated server room when it is not being used.**
- **Have a clear policy on who can access the key or code to your server room.**
- **Have a proper surveillance system in place.**
- **Lock away any portable or vulnerable devices.**
- **Always shred or destroy sensitive documents.**

Examples of physical threats include:

- Natural events (floods, earthquakes, and tornados).
- Intentional acts of destruction (theft, vandalism, and arson).
- Unintentionally destructive acts (spilled drinks, overloaded electrical outlets, and bad plumbing).

15 - Are you controlling how removable storage devices are being used?

Only about **10%** of companies have policies dealing with removable storage devices. It's a big problem as the threat of data theft or loss from downloading information on a thumb drive is growing **exponentially**, according to analysts.

Devices like removable storage media (thumb drives) or connected devices (your smartphone) can easily carry and transmit malware to your computer. If anything, thumb drives should not be used. On your end, drives can be disabled to prevent employees from putting information or removable media into your computers.

- Monitor Removable Storage in Windows
- Restrict Media Access on macOS

How to prevent the spread of malware:

- Don't plug in a device if you're unsure of its content.
- Never plug a device that you have found into a computer, either at home or work.
- Always have up-to-date antivirus software enabled on your devices.
- Enforce an encryption mandate on your devices,

16 - Do you have a Business Continuity Plan (BCP)?

Without a BCP, businesses may face **financial loss**; the longer a business goes without delivering its products and services, the greater its financial losses. But there can also be **technological consequences**, including the loss of important or sensitive data.

It is imperative to equip your team with a Business Continuity Plan (BCP). In the event of a disaster (for example outages, natural disasters or cyberattacks), they can adequately prepare and take action without hesitation. Do not forget to keep a physical copy somewhere safe as well.

Contact us to get started on our 5-step BCP Plan:

- Assignment of BCP Coordination Team.
- Assignment of BCP Response Team.
- Review Business Impact Analysis.
- Review the process and deliverables for the DRP - Disaster Recovery Plan.
- Schedule a BCP exercise - Clearbridge will lead it.

17 - Are you avoiding using public Wi-Fi?

Attacking an open Wi-Fi network takes less than **2 seconds**. Therefore, it's smart to keep your Wi-Fi network **password-protected** to help prevent hackers from accessing your network.

If your team works remotely (or while travelling etc.), avoid using public Wi-Fi wherever possible. It puts your secure information and data at risk. As an alternative, offer them portable connectivity. To learn more, check out our blogs on Remote Working Security Risks and Tips and How to Stay Safe on Public Wi-Fi.

The best thing you can do to protect yourself is to not use public/open Wi-Fi networks in the first place. You have alternatives:

- Your data/5G/LTE
- If you're on a device, using the hotspot function of your phone

Otherwise, make sure your connection is secure (HTTPS and the lock icon in the address bar) and avoid accessing sites that contain sensitive information.

18 - Do you have guest Wi-Fi set up?

☐

If you offer secure guest Wi-Fi access, users will be protected from **malware**, **ransomware**, and **phishing attacks**. That can be a good selling point for your business. It also shows you care about your customers.

You want to ensure that visitors or guests use a separate network from the one you use for work. This will protect your internal networks giving them access to the internet but not your secure data. Check out this resource:

- Guest Wi-Fi by Google

4 best practices when offering guest Wi-Fi at your office:

- Keep it separate from the internal network.
- Enforce appropriate use rules.
- Make it easily accessible.
- Encrypt the guest Wi-Fi network and change the password regularly.

19 - Are you using your email's security features?

42% of workers self-reported having taken a dangerous action (clicked on an unknown link, downloaded a file, or exposed personal data) while online, failing to follow **phishing prevention** best practices.

Most email platforms have built-in security features that you should take advantage of! Because email is often targeted by cybercriminals, they could gain access to your emails or other systems. Use these resources to ensure you are keeping your emails safe:

- Encrypt emails on Mac
- Gmail Security Tips

Best practices to keep your email safe:

- Don't open emails from someone you don't know or trust.
- Avoid sending any sensitive information over email.
- Never open an attachment within an email from a company or person you don't know

20 - Do you have an Incident Response Plan (IRP)?

☐

An IRP protects your company's reputation. Research found that **80%** of consumers would take their business elsewhere if directly affected by a data breach. If a security breach is not handled quickly and properly, your company **risks losing business.**

This invaluable set of instructions will help you detect, respond to, and limit the consequences of a malicious cyberattack against your organization's information systems(s). It also gives your team clear steps to follow to manage and mitigate a data breach or other incidents. Use this template to get started:

- Security Incident Response Plan - Template

Top 5 benefits of an IRP:

- Minimizes operational downtime.
- Provides a clear, methodical plan of action to rely on in critical times.
- Strengthens overall security.
- Builds trust with stakeholders.
- Ensures compliance.

21 - Are you using a VPN?

☐

A virtual private network (VPN) provides an encrypted server, hides your IP address, and **protects your identity** even if you are using public or shared Wi-Fi. Your data will be kept private from any prying internet eyes.

A VPN is a simple yet reliable security measure that protects your network by encrypting your information and providing a secure communication network. Follow these steps to set up a VPN software on Windows or macOS:

- Connect to a VPN in Windows
- Set up a VPN Connection on macOS

Advantages of using a VPN:

- Secures your data.
- Protects your online privacy.
- Changes your IP address.
- Offers protection in a hostile environment.
- Secures connection for remote working.
- Helps companies encrypt data and scan devices for malware to prevent hacking threats.

22 - Are you focused on cybersecurity awareness?

Cybercrime isn't just a broad category, but a growing one. These threats cost the world **$6 trillion** in 2021 and experts say that figure will rise by **15%** annually for the next five years.

Once you understand what you are up against and the risks and symptoms involved, you will be better equipped to recognize a cyberattack and take the appropriate steps to manage and mitigate it. Use these resources to assess your cyberreadiness and awareness:

- 10-Point Cybersecurity Inspection Checklist
- **Top 12 Cybersecurity Tips to Reduce Business Risk E-Book**

How to identify cybersecurity risks:

- Identify assets.
- Identify threats.
- Identify what could go wrong.
- Analyze risks and determine the potential impact.
- Determine and prioritize risks.
- Document all risks.

23 - Have you implemented a framework?

A framework is a a powerful asset for cybersecurity practitioners. Given its **flexibility** and **adaptability**, it is a **cost-effective way** for organizations to approach cybersecurity and foster an enterprise-wide conversation around cyberrisk and compliance.

While there are many different frameworks out there (depending on your type of business and security needs), they are often extremely technical. This is the perfect opportunity to reach out to Clearbridge for help! For more information, look here:

- NIST Cybersecurity Framework
- The Government of Canada's version of NIST, ITSG-33

Top 5 benefits of following a framework:

- Support risk management activities.
- Fosters trust among stakeholders.
- Enhances communication between technical and financial leaders.
- Provides flexibility (can be used by any sized business in any industry)
- Helps your business prepare for future compliance

24 - Are you always assuming there is a vulnerability?

A security vulnerability is a **weakness, flaw, or error** found within a security system that has the potential to be leveraged by a hacker to compromise a secure network.

Avoid complacency as it leads to weaknesses. For IT, it is very much about the proactive journey—you should constantly be evaluating, revising, and updating your policies, software, and permissions. Never assume that someone would not be able to find a loophole and target you in an attack. Wondering how to understand your vulnerabilities? Check out this resource.

Top 5 cybersecurity vulnerabilities:

1. Poor security defences.
2. Poor data backup and recovery.
3. Poor network segmentation and monitoring.
4. Weak authentication and credential management.
5. Poor security awareness.

25 - Have you partnered with a cybersecurity expert?

We know businesses have options when it comes to IT services and support. So, what makes Clearbridge the best choice? We offer **comprehensive, productivity-focused cybersecurity training and resources** that allow you to focus on your job, rather than IT.

There is a lot of information on the internet. However, dealing with experts is worth the investment. We gather our knowledge and expertise from the experience we've had working with other businesses that have faced the daunting reality of cyberthreats and attacks. Let's partner together! Here's why:

- We have relevant work experience and can provide examples of our previous work.
- We don't just want to sell you a one-size-fits-all software solution.
- We take pride in our communication skills and will always be transparent with you.
- We offer cybersecurity training—cybersecurity content, and other resources like our Cybersecurity Toolkit.
- We are here to create a tailored plan (BCP, DRP, IRP) for your business.

- [x] Introduction
- [ ] Have you implemented multi-factor authentication (MFA)?
- [ ] Do you restrict certain administrative privileges?
- [ ] Are you patching your operating systems?
- [ ] Are you 'whitelisting' your approved applications?
- [ ] Are you performing daily backups?
- [ ] Are you taking advantage of a password manager?
- [ ] Are you restricting access to your data?
- [ ] Are you training your team about cybersecurity?
- [ ] Are you managing your mobile devices?
- [ ] Are you managing your mobile applications?
- [ ] Are your devices encrypted?
- [ ] Are you enforcing strong passwords?
- [ ] Is your email secure?
- [ ] Is your physical hardware protected?
- [ ] Are you controlling how removable storage devices are being used?
- [ ] Do you have a Business Continuity Plan (BCP)?
- [ ] Are you avoiding using public Wi-Fi?
- [ ] Do you have guest Wi-Fi set up?
- [ ] Are you using your email's security features?
- [ ] Do you have an Incident Response Plan (IRP)?
- [ ] Are you using a VPN?
- [ ] Are you focused on understanding and assessing your risk?
- [ ] Have you implemented a framework?
- [ ] Are you always assuming there is a vulnerability?
- [ ] Have you partnered with a cybersecurity expert?

Thank you for using our Cybersecurity Audit!

Total: /25

We know that this was a big list to go through...BUT if you've made it all this way—you're now equipped with some information security tips that will get you on the right track. Reach out to us to determine the next steps you should take to ensure you and your business are safe!

To book your consultation, contact us.

Don't Wait, Get Started

www.clearbridge.ca

support@clearbridge.ca

(778) 383-6726