THE 2025 CYBER SECURITY CHECKLIST

AN EASY-TO-UNDERSTAND GUIDE FOR BUSINESS OWNERS & EXECUTIVES

EXPERA INFORMATION TECHNOLOGY

PUBLISHED BY

Vince Fung

Founder & CEO

THE STATE OF CYBER SECURITY

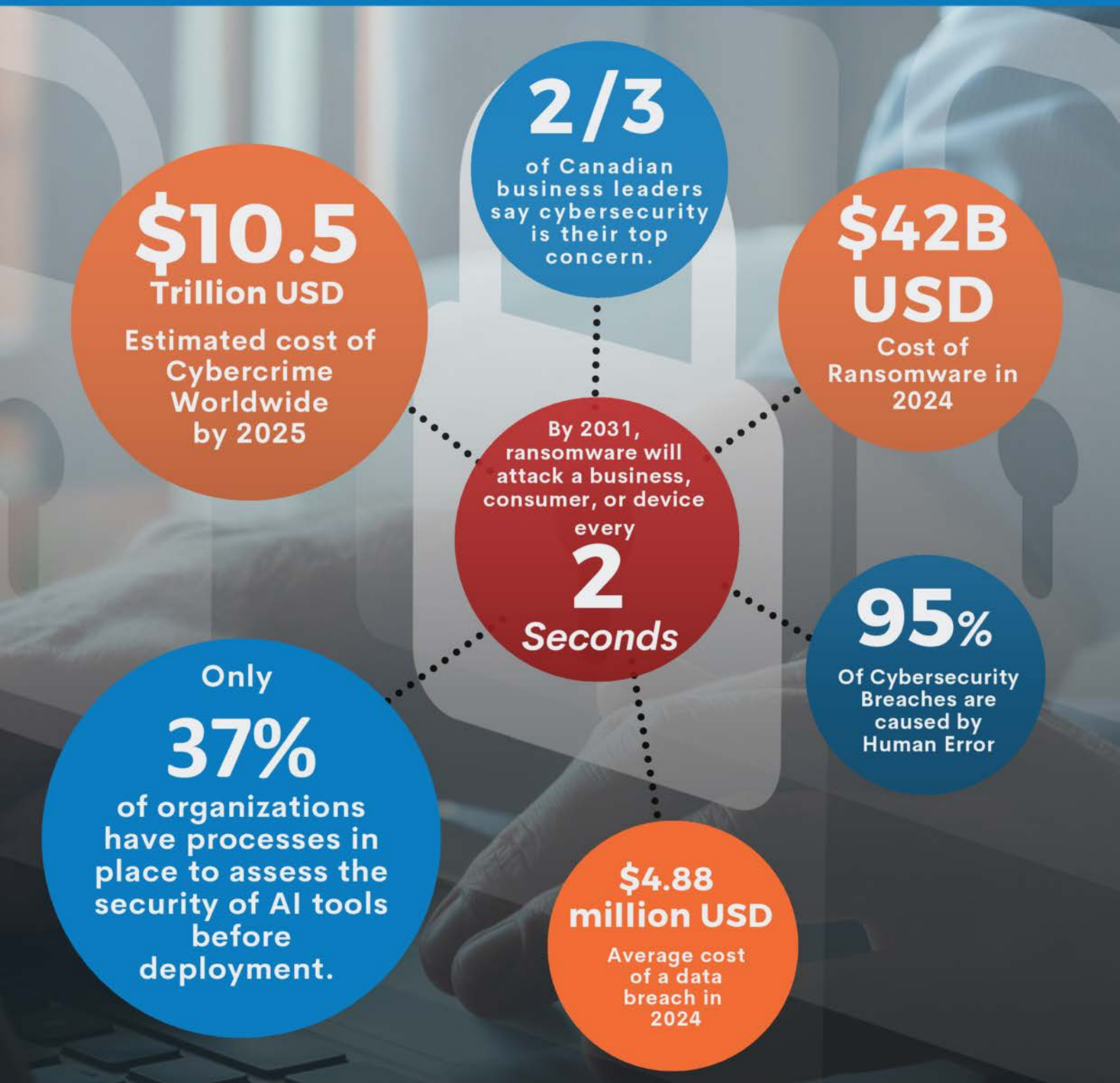
Thank you for downloading a copy of our "2025 Cyber Security Checklist" - You've just taken the first big step to ensuring that your business is protected against the latest cyber threats!

We've created this to be an easy-to-understand guide for business owners and executives, written in plain English.

We've developed this guide from over two decades of our experience, being a member of an elite group of cybersecurity-focused IT providers, and through the work that our threat analysis team does every day, to keep the clients we serve secure.

This guide was put together to help leaders like you gain a better understanding of the threats you face and the questions you should ask your IT people to ensure that you have the right protections in place to secure your business in the rapidly evolving threat landscape.

Vince Fung
CEO and Founder
Expera IT



Cybersecurity has become a major struggle for busineses large and small. The stats above speak for themselves.

It's become more important than ever for businesses to take cybersecurity seriously. Building a culture of security in organizations must come from the top.

A HOLISTIC APPROACH

PROTECTING YOUR BUSINESS IN TODAY'S LANDSCAPE

A cyber attack is the biggest risk that a business faces today. The probability of being hit with a business-crippling attack is orders-of-magnitude higher than any other type of disaster, including fire, theft, flood or any other natural or man-made disaster.

In fact, virtually every business is guaranteed to be the target of a cyber attack. Cyber security experts now live by the mantra:

"It's not a matter of if, it's a matter of when."

As a business owner or executive, your leadership in driving and building a culture of security within your organization will be one of the most important indicators of success.

One of the stats on the previous page was that 95% of cybersecurity breaches are caused by human error. No matter how much technology is deployed to keep your business secure, all it takes is one employee getting tricked to do something they aren't supposed to and multiple safeguards that were put in place can be rendered useless.

The reality today is that:

Hackers Don't Hack Systems, Hackers Hack People!

A HOLISTIC APPROACH

BUSINESSES NEED 360 DEGREES OF PROTECTION

In order to maximize security, businesses need to take a layered approach. Gone are the days where you can just protect the systems by putting a simple fence around your network with a gatekeeper.

To be effective in protecting your assets, the approach that you need to take is very much like an onion, with your assets in the center. The onion has multiple layers and in the event that a layer get penetrated, there are other layers in place to keep your assets secured

With all of the hacks of major corporations and governments that seem to come out on the news almost daily, it's sometimes easy to think that there is nothing you can do to protect yourself. But understand that cybercrime is very much financially motivated. You'll see that protecting yourself is about putting enough roadblocks in place so the hackers move on to an easier victim.

Step #1

Only **10%** of Canadian businesses have a Cyber Insurance Policy

$1 Million average cost of a ransomware attack

Your first step and your last resort...

CYBER INSURANCE

Many business leaders look at insurance as a last resort. While this may be the case, it is absolutely essential that you have the right cyber insurance policy as part of your overall cyber security strategy.

According to Insurance Business Canada, only 10% of Canadian businesses have a cyberinsurance policy in place.

Add to that the fact that the average cost of a ransomware attack is $1 Million dollars, and you can quickly see the risk of not having a policy.

If you don't currently have a cyber insurance policy in place, now is the time to talk to you broker so that they can recommend the right coverage for your business.

Talk to your insurance broker today!

PRO TIP:

As you look into options for cyber insurance, you may discover that there are no standard policies, there are demanding processes, and broad coverage exclusions. Brokers who are experienced with cyber insurance policies are also rare and hard to find.

Here are some of the questions you should ask and what to look out for.

Things to Watch for in a Cyber Insurance Policy

- **What type of data is covered?**
- **Your obligations**
- **Disclaimer of warranties**
- **Definition of start and end of an event**
- **Limitation of liability**
- **Limits by type of loss**
- **Specific exclusions**
- **What losses are covered?**

(ie. forensic investigation, victim notification, financial monitoring, legal fees, fines, loss of business, insider events, physical data theft...)

KEY COMPONENTS OF YOUR CYBER SECURITY STRATEGY

DATA

Your data is one of your biggest and most important assets. In the connected world that we operate in today, data is the lifeblood of business. From sales to operations and finance to human resources, ensuring the integrity and availability of data is critical to the operation of every business.

SYSTEMS

Ensuring that you have the right security tools to protect you systems is an essential part of your cyber security strategy. Systems protection must happen at multiple layers to ensure that everything from your servers, cloud services, laptops, desktops, mobile devices, and network components are all secured and protected.

PEOPLE

The biggest challenge of your cyber security strategy will be ensuring your people don't do stupid things that leads to a security breach. Proactively, you'll need to ensure you have the right corporate policies in place, cyber awareness training programs, and easy-to-use tools that your people can utilize to help maximize security.

OVERSIGHT

Cybersecurity isn't something that you can just "set-and-forget." As the threat landscape evolves, you need to constantly refine the protection mechanisms you have in place to stay on top. It's also critical to ensure your systems are properly maintained to deploy security updates and verify that everything you have in place are actually working.

THE TOP 3 RISKS THAT BUSINESSES FACE ARE:

Stolen Credentials

When accessing systems and data, the only thing separating a legitimate user and someone gaining unauthorized access is their username and password. Stolen credentials and hacked passwords are one of the leading causes of a security breach.

Unpatched Software

Many software updates are not just to add features but to address security flaws that have been discovered. Hackers exploit these flaw and are often successful in gaining unauthorized access to systems. Ensuring software is up to date is essential to keeping your business secure.

Your People

From clicking on links or attachments that launch malware to giving up credentials to hackers, your people are one of the biggest threats. All it takes is one person getting tricked to do something they aren't supposed to and hackers can bypass layers of security.

WHAT LEVEL OF SECURITY DOES YOUR BUSINESS NEED?

Core Security

Your business utilizes technology to operate but an extended systems outage wouldn't cause a complete stoppage of work. The data in your business is valuable but doesn't contain anything that is of a highly sensitive nature. There is limited budget and appetite for investing in cyber security.

Security Conscious

Technology is essential to your business. A systems outage would have a significant impact and near complete stoppage of work. Your data is extremely valuable and may include items of a sensitive nature. Ensuring that systems and data are secured is essential to long term business success.

Compliance Driven

Your business operates in a highly regulated industry with compliance and reporting requirements. Technology is the backbone of your business and a strong compliance and cyber security program is critical to your reputation with clients, vendors, and regulatory authorities.

REQUIREMENT LEVELS

Each of the checklist items on the following pages can be categorized into one of the following requirement levels.

As it is impossible to use a "one size fits all" approach to cybersecurity, your business needs to evaluate the risks, costs, and benefits to determine the appropriate requirement levels of each security protection item based on your unique business needs.

Mandatory

Optional

Recommended

Low Value

Data Protection

Your data is one of your biggest and most important assets. In the connected world that we operate in today, data is the lifeblood of business. From sales to operations and finance to human resources, ensuring the integrity and availability of data is critical to the operation of every business.

Backup of Servers and Data

- How frequently are the servers backed up?
- Are the backups copied to an offsite location? Are they encrypted?
- Are the offsite backups stored in Canada?
- Is at least one regular backup set made offline?
- Are backups monitored and how often are backups tested?
- How long will it take to restore systems in the event of a disaster?
- Is just the data being backed up or the entire server including the operating system and the configuration?

Microsoft 365 Data Backup

- Is Office 365 being backed up?
- What data is being backed up? (Email, Teams, OneDrive, SharePoint, etc.)
- How frequently is it being backed up?
- How long would it take to recover lost data?
- Are backups monitored and how often are backups tested?
- Is email archiving in use? Is legal hold retention enabled?

Backup of Cloud Infrastructure

- Are there servers running on cloud providers? (Azure, AWS, etc...)
- How frequently are the servers backed up?
- Are backups performed within the same tenant as the servers?
- Are backups monitored and how often are backups tested?

Backup of Cloud Applications/Services

- What other cloud services are being backed up? (SalesForce, Quickbooks Online, Sage Online, ERP Systems, etc...)
- How frequently are they being backed up?
- How long would it take to recover lost data?
- Are backups monitored and how often are backups tested?

Backup of User Computers

- Is a policy in place to ensure data is not saved on the local computers?
- If not, are user computers backed up?
- How frequently are they being backed up?
- Are backups monitored and how often are backups tested?

Data Protection

Device Encryption

- Is data on laptops, desktops, and mobile devices encrypted?
- Is the encryption enforced and centrally managed?
- Are the encryption keys rotated?
- Is data on servers encrypted?

USB Lockdown and Encryption

- Is the use of USB flash drives and disks restricted?
- Is this centrally enforced and managed?
- If use is permitted, is encryption enforced on these devices?

Data Destruction

- Is a secure wipe performed on old disks when servers and computers are decommissioned?
- What is the process to ensure that this has been completed?
- Is this process also followed for old backup media?

Data Access Permissions Review

- Is a review of data access permissions performed regularly?
- How frequently is this performed?
- What processes are in place to ensure rights are granted properly?

Data Asset Management

- Is a regular review of where data is store performed regularly?
- Does the review include proper tagging and classification of data?
- Are steps taken to eliminate data sprawl and duplication?
- Are these performed in conjunction with data access permissions reviews?

Data Loss Prevention

- Are policies in place to prohibit the copying or sending of confidential data outside of the organization?
- Are documents and data files accurately tagged confidentiality levels?
- Are protocols in place to detect and block the sending of these files?

Storage Redundancy and Archive

- What systems are in place to ensure that there is high-availability for essential business data and systems?
- Is this data synchronized in real-time?
- How is it secured? How is it protected against ransomware?
- Is failover fully automated or does it require manual work to fail over?
- Is there an archival process for legacy data in place?
- Is the archive secured and backed up offsite regularly?

Systems Protection

Ensuring that you have the right security tools to protect you systems is an essential part of your cyber security strategy. Systems protection must happen at multiple layers to ensure that everything from your servers, cloud services, laptops, desktops, mobile devices, and network components are all secured and protected.

Firewalls at Office and Field Locations

- Are smart firewalls used to protect the perimeter at all office and field site locations?
- How frequently are these firewalls updated to the latest version?
- Are these firewalls equipped with an Intrusion Prevention System?
- Are these firewalls monitored to detect attacks and suspicious activity?
- Are both inbound and outbound traffic filtered to minimize breaches?
- Are all Remote Desktop and unnecessary inbound ports blocked?

Next Generation Antivirus Protection

- Does the software rely on signatures and can only detect known viruses?
- Is the Antivirus software powered by Artificial Intelligence?
- How frequently are virus definitions updated?
- Is the Antivirus software capable of recognizing malicious behavior?
- Does the software allow you to rollback to a state prior to infection?
- Is the Antivirus software monitored 24x7?
- What is the performance impact of the Antivirus software?

Threat Hunting and Hacker Foothold Detection

- Is advanced threat hunting and hacker foothold detection in place?
- Is this in place to protect both servers and user computers?
- Is threat hunting monitored 24x7?

Asset Inventory

- Is there an inventory of all current and retired IT assets?
- Is this inventory updated in real-time? If not, how often is it updated?
- What is included in the inventory? (Servers, computers, network devices, mobile devices, etc...)
- Is there an inventory of all installed software and licenses?

Management & Security of Network Devices

- Are managed network devices updated regularly to the latest version?
- Is the configuration of these devices backed up regularly?
- Do configuration changes to these devices go through an approval process?
- Are configuration changes documented and a history maintained?
- Are these devices monitored for performance and traffic anomalies?

Systems Protection

Wireless Networks

- Is the wireless segmented to isolate guests from the internal network?
- Is enterprise encryption enabled for all wireless networks?
- Do employees authenticate with their own username and password?
- Is the guest password changed regularly and not posted in an open area?

Network Access Restrictions

- Is network access locked down to only authorized devices?
- Are least access permissions assigned for access to resources by users?
- Is ZeroTrust implemented to restrict access by default unless granted?

Network Passwords

- Who has administrative access to server and infrastructure?
- Are daily use accounts restricted from special use admin accounts?
- Are different local admin passwords used across all devices?
- Is multi-factor authentication used on admin accounts?
- Are credentials for network devices stored in a secure password vault?
- Is admin access to devices and systems logged?

Remote Access Controls

- Which users are granted remote access?
- Is remote access secured with multi-factor authentication?
- Is remote access traffic encrypted?
- Is security enhanced using a broker service rather than exposed ports?
- Is remote access activity monitored and logged?

Patch and Security Update Management

- How often are security updates and patches deployed to systems?
- Is this process centrally managed and automated?
- Are third party applications also patched in addition to the operating system?
- Can systems that are missing patches be easily identified for remediation?
- What update policies and schedules apply to servers, workstations, mobile devices?
- Is there a testing process and test environment for major patches or upgrades?

Mobile Device Management

- Do you have a Mobile Device Policy and a Bring Your Own Device (BYOD) Policy in place?
- Is a Mobile Device Management tool used to manage devices?
- Are both company owned and BYOD devices managed in an appropriate manner?
- Do you have the ability to enforce encryption and other security policies?
- Do you have the ability to remotely wipe a lost or stolen device?
- Do you have the ability to selectively wipe a BYOD device when an employee leaves?
- Do you have a way to manage updates of mobile operating systems?
- Do you have a way to restrict what applications are permitted on mobile devices?

Securing Your People

The biggest challenge of your cyber security strategy will be ensuring your people don't do stupid things that leads to a security breach. Proactively, you'll need to ensure you have the right corporate policies in place, cyber awareness training programs, and easy-to-use tools that your people can utilize to help maximize security.

Executive Buy-In

- Is your entire leadership team onboard with your cyber security directives?
- Does this include ownership, board of directors, and executives?
- Is everyone on the same page and agrees to the security level needed for your business?
- Is there a willingness to spend the time implementing these cyber security directives?
- Has an appropriate budget been allocated?
- Are all of the executives themselves willing to follow the new rules and guidelines?
- Is the executive team willing to participate in driving the required adoption and change?

Cyber Awareness Training

- Is there a Cyber Awareness Training program in place?
- Are these training programs live or pre-recorded video sessions?
- Is there a quiz to verify that your people have completed the training?
- Is there a central dashboard to track who has completed the training?
- When new threats emerge, is new content made available to users and tracked for viewing?
- Is the content entertaining and engaging or extremely dry and painful to watch?
- How often is the content updated?

Threat Susceptibility Testing

- Is phishing testing performed regularly to test which employees are vulnerable?
- Is additional training required when they fail a test and click on the links?
- Is there a company policy for a certain number of strikes that results in termination?
- Is external social engineering testing performed?
- How frequently are phishing and social engineering tests performed?

Insider Threat Protection

- Are reference checks specifically with previous mangers performed for all new hires?
- Are background checks performed with local and national authorities for new hires?
- Do employees have access to distress and support programs?
- Is there an open door policy with employees that encourages them to safely and openly share issues that they may be facing in their personal lives so that they can seek help?
- Are programs in place to encourage employees to report suspicious behaviors or risks?

Password Management Vault

- Do your employees utilize a centrally maintained password management system?
- Are all password vaults encrypted and can only be unlocked with the user's master password?
- Does this vault sync across all devices and browswers?
- Does this vault recognize and generate warnings for at-risk passwords?

Securing Your People

Acceptable Use and Security Policies

- Is there a IT Acceptable Use Policy in place in your organization?
- What other policies are in place? (BYOD, Remote Work, Social Media, etc...)
- Are employees required to read and sign off on these policies?
- How is the acceptance of these policies tracked and recorded?
- When policy changes are made, are all employees require to re-accept the new policy?

ZeroTrust Application Whitelisting

- Are only administrator-authorized applications, scripts, and code allowed to run on servers and computers?
- Is application whitelisting centrally managed and in real-time?
- Can commonly used applications be pre-approved for execution?
- Are updates to commonly used applications pre-approved?
- Can unwanted applications/cloud services be blocked? (DropBox, Google Drive, etc...)
- Can approved applications be ringfenced to restrict what it can do on the system?

Administrative Rights Lockdown

- Are all users restricted from having local administrative rights on their computers?
- Is there a central way for users to request admin rights to perform required tasks?
- Is all admin access logged and recorded?
- Can admin access to automatically granted for common requests such as printer installs?
- When admin access is granted, is the application be blocked from running another program?

Self Service Credentials Management

- Do users have a way to manage and reset passwords without calling the helpdesk?
- Are users warned of password expiry or account lockouts?
- Does the self-service password reset tool work even outside the office?
- Can administrators use the password management tool to authenticate users for support?

Multi-Factor Authentication and Single Sign-On

- Is Multi-Factor Authentication (MFA) Enabled for all Microsoft 365 Services?
- Is MFA or Single Sign-On Enabled used to secure other cloud services?
- Is MFA configured with the Microsoft Authenticator App or with text messages (less secure)?
- Is MFA enforced for ALL users in your organization?

Screen Savers and Privacy Screens

- Is automatic screen saver with screen lock enforced on all devices?
- Are users required to enter their password when their screen locks?
- Is this enforced on both computers and mobile devices (mobile phone and tablets)?
- Do you employ privacy screens for users that work in public areas outside of the office?

Oversight

Cybersecurity isn't something that you can just "set-and-forget." As the threat landscape evolves, you need to constantly refine the protection mechanisms you have in place to stay on top. It's also critical to ensure your systems are properly maintained to deploy security updates and verify that everything you have in place are actually working.

High Level IT Oversight

- Is there someone in charge of the high level strategic direction of IT in your organization?
- Is this person regularly involved in senior leadership level discussions on you business?
- Does this person have a deep understanding of how your business operates?
- Does this person help identify areas where technology can drive efficiencies?
- Does this person help identify areas where technology can help elevate client experience?
- Does this person help identify areas where technology can drive additional revenues?

Responsive and Knowledgeable IT Support

- Do you have access to responsive IT support for end users to ask questions if they are uncertain whether something is malicious or now before they click a link or open a file?
- Do you have rapid access to IT support in the event of a potential security incident?
- Do your users have the confidence to contact IT support whenever they need it without worrying about incurring costs?

Network Operations Center

- Are all of your systems centrally monitored to proactively identify issues?
- Does the monitor check to ensure systems are kept up-to-date?
- Does it check for potential performance issues such as disk, CPU, and memory?
- Does it ensure that security patches and critical updates are in place?
- Does it track compliance with network policies such as screen lock and encryption?

Security Operations Center

- Are your security tools monitored 24x7 by a security operations team?
- Are all of your tools working in conjunction with each other to aggregate security signals?
- When an issue is detected, does the security team have the ability to quickly isolate threats?
- Are threats remediated quickly to minimize risks to other users and systems?
- Is a threat analysis team constantly working to identify new threats and risks?
- Are security policies consistently updated based on new threat intelligence?

Change Control and Management

- Are changes to system settings and software centrally managed and reviewed?
- Is a change management process in place to ensure changes are documented and approved?
- Does the change management process include a risk analysis?
- Does the change management process include a back out plan in case of issues?
- Does the change management process ensure that documentation is properly updated?

Oversight

IT Service Request and Ticketing System

- Are IT service requests submitted through a centralized ticketing system?
- Does the system track response times and resolution times?
- Does the system capture all communication and action items for future analysis?
- Does the system categorize different types of issues according to ITIL standards?
- Are incidents, service requests, and problems all tracked properly?
- Does the ticketing system provide robust reporting and analysis functionality?

Secure IT Documentation Platform

- Is a secure IT documentation portal in place to manage and track all IT documentation?
- Does the portal track both hardware and software assets?
- Is a detailed knowledge-base available to both technicians and users?
- Is documentation well organized and easily searchable?
- Does the documentation platform have a secure way to encrypt system passwords?
- Does the platform support centralized multi-factor authentication in a secure manner?

IT Runbook Standards and Best Practices

- Are IT management and support processes well documented in a Run Book?
- Are technicians trained on and religiously follow these standards and best practices?
- Are standards and best practices reviewed regularly and updated?
- When major incidents or projects are completed, are look-backs done to improve processes?
- Do your IT leaders belong to industry organizations and peer groups to keep up with trends?

Security Information and Event Management

- Is a centralized system in place to aggregate all logs and security signals from IT devices?
- Does this system automatically correlate events to identify security threats?
- Does the system have external threat intelligence feeds?
- Does the system leverage artificial intelligence and machine learning?
- Does the system meet compliance requirements for your business?
- How are security alerts and reports generated and actioned?

Microsoft 365 Admin and Management

- Is your Microsoft 365 tenant and Azure Active Directory regularly maintained?
- Are alerts and warnings actioned and remediated?
- Are the most current standards and best practices implemented in your 365 configuration?
- Is your Microsoft 365 Security Score reviewed and plans put in place to elevate the score?
- Is your M365 tenant monitored by a 24x7 Security Operations Center for security anomalies?

Risk Assessments

- Is an IT security risk assessment performed on an annual basis?
- What framework is the risk assessment based on? (NIST, ISO, PCI DSS, etc...)
- Are the risks identified in these assessments ranked and placed on the IT roadmap?
- Is immediate action taken to remediate any major high risk issues?

Oversight

Incident Response Plan

- Do you have a detailed incident response plan that outlines likely cyber threat scenarios?
- Are changes to your IT infrastructure captured so that the it can be updated in the plan?
- How often is this incident response plan updated?
- Are different systems assigned appropriate levels of priority for recovery?
- Are there recovery time and recovery point objectives defined?
- After the plan is updated, are the changes highlighted and disseminated to all stakeholders?
- Is this response plan in a place where it is still accessible in the event of a systems outage?
- Is there a process to do trial runs of the different scenarios for practice?
- How often are components of this plan reviewed and tested?
- Does you plan include notification and updates to all stakeholders (including clients, vendors, staff members, shareholders, regulatory agencies etc...)?
- Are the contact details of all key stakeholders and their roles outlined in the plan?

Incident Response Team

- Have you assembled your incident response team?
- Are they all aware of their responsibilities?
- Have they participated in the creation of and reviewed the Incident Response Plan?
- Are the contact details of all members of this team documented?
- Are contact number outside of your IT infrastructure included in case of a major systems outage?
- Does your incident response team include members outside of our your organization (consultants, insurance providers, service providers, etc...)?

Virtual Muster Point

- Do you have a communication point where key stake holders can securely communicate ?
- Is this communication outside of your IT infrastructure in case your systems are down?
- Who is authorized to post and share updates at this location?
- Are all stakeholders aware of when and how to access this virtual muster point?
- Do you have a updated contact list of all stakeholders that is securely stored outside of your regular systems in case your systems are down or compromised?

Regulatory Compliance

- Is your business subject to any regulatory compliance requirements?
- How frequently does compliance need to be audited?
- Are there any special reporting requirements?
- Are there any special logging requirements?
- How do you stay on top of any changes or updates to the requirements?
- Do you have an Artificial Intelligence Responsible and Acceptable Use Policy in place?

Reporting

- Do you have access to reporting that shows how your security layers are functioning?
- How frequently do you get these reports?
- Is the data in these reports in real-time?
- Does the report give you a measure of your security posture?

ARE YOUR SECURITY LAYERS ACTUALLY WORKING?

A recent survey by AttackIQ indicates that 53% of organizations don't know if their security tools that they have in place are actually working to protect them from data breaches.

53%

Of Enterprises Have No Idea If Their Security Tools Are Actually Working

Having a solution deployed and having a solution that actually protects you are two very different things.

Threats are ever-evolving, tools fail, and people make mistakes. Ensuring your security layers are actually protecting you can be a major challenge.

If you'd like to know if what you currently have in place is actually working, **find out today!**

IMPLEMENTATION HELP

Implementing all the pieces of your cyber security stack can seem overwhelming. There are a lot of moving pieces, a lot of different technologies, there's the people aspect of it, and the threat landscape is evolving on a daily basis.

EXPERA
INFORMATION TECHNOLOGY

For over 25 years, Expera has delivered world class I.T. Services and Cybersecurity solutions to help businesses gain a competitive edge while keeping them secure against the latest threats so that they can thrive.

If you'd like assistance implementing the security layers you need to keep your business protected, we're here to help!

References:

1. Cybersecurity Facts and Stats
2. What is Cybersecurity, IBM
3. Cyber threats top concern for Canadian business leaders: survey
4. Ransomware Will Strike Every 2 Seconds by 2031
5. Cost of a Data Breach Report 2024
6. Global Cybersecurity Outlook 2025
7. Every 14 seconds, a business is falling victim to a Ransomware attack
8. Ransomware still uses social engineering as its main infection vector
9. Just 10% of Canadian businesses have purchased a Cyber Insurance Policy
10. 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked
11. 53% of enterprises have no idea if their security tools are working - Help Net Security

Thank you for downloading our 2025 Cyber Security Checklist!

If you found this guide helpful, we'd love to hear from you!
Please also feel free to share this with other business leaders who would benefit from this.

EXPERA
INFORMATION TECHNOLOGY

GetIT@experaIT.com | experaIT.com | 888.749.0098

2020 WINNER MSP 501 Channel Futures. | THE GLOBE AND MAIL 2020 REPORT ON BUSINESS CANADA'S TOP GROWING COMPANIES | GROWTH 2020 CANADA'S FASTEST-GROWING COMPANIES | IT COMPANIES 50 BEST MANAGED | Canada's 50 Best Managed IT Companies

Notes:

EXPERA
INFORMATION TECHNOLOGY