



BUILT FOR
MEDIUM & LARGE
ORGANIZATIONS

250+
EMPLOYEES

MEDIUM & LARGE ORGANIZATION CYBER ROAD TRIP

Strengthen today's readines.
Prepare for tomorrow's **risks**.

A practical action guide to help organizations identify what matters, strengthen response, maintain operations, and build resilience.



PROTECT

People, Data
and Operations



PREPARE

Teams
and Leadership



STAY RESILIENT

Through Disruption
and Change



KNOW WHAT
MATTERS



CONTROL
ACCESS



PREPARE
YOUR PEOPLE



PRACTISE
YOUR RESPONSE



STAY READY



CYBERSECURITY IS A TEAM EFFORT.
TOGETHER, WE CAN BUILD A SAFER DIGITAL CANADA.

LET'S HIT THE ROAD.
A STRONGER, MORE RESILIENT
CANADA STARTS NOW.



1

START HERE

ARE YOU ACTUALLY READY?

A fast readiness check to see where your organization stands today. Use this to identify strengths and gaps across five key areas.



**CHECK YOUR READINESS.
SPOT THE GAPS, PLAN YOUR NEXT STEPS**



ORGANIZATIONAL READINESS CHECK

For each statement, choose the option that best describes your organization today.

THERE'S NO RIGHT OR WRONG ANSWER — THIS HELPS YOU SEE WHERE TO FOCUS.

AREAS TO CONSIDER



NO
Not in place
or just starting.



PARTLY
Some progress,
but gaps remain.



YES
In place and
working well.



PEOPLE

Our employees understand their role in cybersecurity and follow key security practices.

☐
☐
☐


PROCESS

We have clear policies, procedures, and response plans for cyber incidents.

☐
☐
☐


TECHNOLOGY

Our security tools, systems, and data are regularly updated, monitored, and protected.

☐
☐
☐


PARTNERS

We manage third-party and supplier risks, and have clear security expectations in place.

☐
☐
☐


LEADERSHIP

Our leadership prioritizes cybersecurity, provides the right resources, and supports a strong security culture.

☐
☐
☐


**EVERY JOURNEY STARTS
WITH A CLEAR VIEW.**

Use this assessment as your starting point. You'll revisit it at the end of the guide to see how far you've come!



YOUR ROAD TO READINESS

Every strong organization follows a path. Use this roadmap to guide your team through the key steps to strengthen your cyber readiness and build a more resilient future.

**SIX STOPS. A STRONGER ORGANIZATION.
LET'S HIT THE ROAD.**



**STOP
1**

KNOW WHAT MATTERS

Identify your critical assets, key risks, and what needs to be protected.

PAGE
3



**STOP
2**

PROTECT

Strengthen your people, processes, and technology to reduce risk.

PAGE
4



**STOP
3**

VERIFY

Detect threats early, validate information, and confirm what's real.

PAGE
5



**STOP
4**

EXTERNAL

Know Your Dependencies
Third-Party Detour — Who Are You Relying On?

PAGE
6



**STOP
5**

ADVANCED THREATS

Use AI Without Creating New Risk
AI Checkpoint — Know What's Going In

PAGE
7



**STOP
6**

IMPROVE

Turn lessons into lasting improvements and build a stronger future.

PAGES
8-9



**YOU'VE REACHED
YOUR DESTINATION.**
A more resilient organization.
A safer Canada.



YOUR PROGRESS TRACKER

Check off each stop as you go. Every step brings you closer to a stronger, more resilient organization.



**STOP 1
KNOW WHAT
MATTERS**

☐


**STOP 2
PROTECT**

☐


**STOP 3
VERIFY**

☐


**STOP 4
EXTERNAL**

☐


**STOP 5
ADVANCED THREATS**

☐


**STOP 6
IMPROVE**

☐


**FINISH STRONG.
STAY RESILIENT.**

Revisit this guide anytime to keep your organization on the right path.

IDENTIFY YOUR CRITICAL ASSETS

Critical Systems Checkpoint

Identify the systems, data, services and business processes you cannot operate without.

Ask: What has to stay running? How long can it be unavailable? Who owns it?



**KNOW
WHAT MATTERS.
PROTECT WHAT
KEEPS YOU MOVING.**



WHY IT MATTERS:

Cyber incidents can disrupt your most important systems, services and data. Knowing what matters helps you focus your efforts, prioritize resources, and make faster, better decisions when it counts.

KEY QUESTIONS

Use the questions below to identify and assess your organization's critical systems, data, services and processes.



WHAT HAS TO STAY RUNNING?

Which systems, services and processes are essential to your operations?



HOW LONG CAN IT BE UNAVAILABLE?

What is the maximum acceptable downtime before it causes significant impact?



WHO OWNS IT?

Which team or individual is responsible for this system, data or process?



WHAT WOULD BE THE IMPACT?

What would be the operational, financial, reputational or safety impact if it were unavailable?

CRITICAL SYSTEMS CHECKLIST

List your organization's critical systems, data, services and business processes. Use the questions above to help you complete the table.

SYSTEM / SERVICE / PROCESS	DESCRIPTION	WHY IT'S CRITICAL	MAX DOWNTIME (hrs/days)	OWNER (team/individual)
1				
2				
3				
4				
5				



KNOW WHAT MATTERS TO STAY AHEAD.

Revisit this table regularly to ensure it stays up to date as your organization evolves.

LOCK DOWN ACCESS

Access Control — Who Can Get In?

Ensure the right people have the right access to the right systems, and remove any unnecessary or excessive access.

Focus on: MFA, privileged accounts, former employees, third parties and service accounts.



WHY IT MATTERS:

Excess or unmanaged access is one of the biggest cyber risks for organizations. Attackers often exploit valid accounts to gain access, move laterally, and cause damage. Strong access controls help prevent unauthorized access and reduce the impact of a potential breach.

KEY AREAS TO CHECK

Review the areas below to understand and strengthen your access controls.



MULTI-FACTOR AUTHENTICATION (MFA)

Is MFA enabled for all users, especially high-risk and privileged accounts?



PRIVILEGED ACCOUNTS

Who has elevated access? Is it limited to only those who need it?



FORMER EMPLOYEES

Are accounts disabled immediately when someone leaves?



THIRD PARTIES

Do vendors and partners only have the access they need? Is it regularly reviewed?



SERVICE ACCOUNTS

Are non-human accounts (e.g., applications, systems) properly managed and monitored?

ACCESS CONTROL CHECKLIST

Use this table to review and assess your current access controls. Identify any unnecessary or excessive access and plan for remediation.

ACCOUNT TYPE	WHO HAS ACCESS?	IS MFA ENABLED?	IS ACCESS REQUIRED?	ACTIONS NEEDED
1 User Accounts (employees)				
2 Privileged Accounts (admins)				
3 Former Employees				
4 Third Parties (vendors/partners)				
5 Service Accounts (applications/systems)				



**LESS ACCESS.
LESS RISK. A STRONGER,
MORE RESILIENT ORGANIZATION.**

Review access regularly and remove any unnecessary or excessive permissions. The fewer doors open, the harder it is for attackers to get in.

VERIFY BEFORE YOU TRUST

Verification Checkpoint

High-risk requests involving money, credentials, sensitive data, system changes and executive requests need a second channel of verification.



WHY IT MATTERS:

Attackers often impersonate trusted people to gain access, move money or make system changes. Verifying requests helps prevent costly mistakes and protect your organization.

HIGH-RISK REQUESTS

Always verify requests that involve:



Money transfers



Credentials or access requests



Sensitive data requests



System changes



Executive requests

DECISION FLOW — SHOULD YOU TRUST THIS REQUEST?

Follow the steps below for any high-risk request.



QUICK CHECKLIST

Use these questions to validate high-risk requests.



MONEY TRANSFERS

- ☐ Was this expected?
- ☐ Is the recipient correct?
- ☐ Have you confirmed with finance?



CREDENTIALS / ACCESS

- ☐ Is the request legitimate?
- ☐ Have you verified the requester?
- ☐ Is the level of access appropriate?



SENSITIVE DATA

- ☐ Is this data necessary?
- ☐ Is the requester authorized?
- ☐ Have you confirmed the purpose?



SYSTEM CHANGES

- ☐ Was this planned?
- ☐ Is it an approved change request?
- ☐ Have you verified with IT/security?



EXECUTIVE REQUESTS

- ☐ Is the request typical of this person?
- ☐ Have you confirmed via a second channel?
- ☐ Does it create urgency or pressure?



KNOW YOUR DEPENDENCIES

Third-Party Detour — Who Are You Relying On?

Your business depends on vendors, cloud platforms, MSPs, suppliers and AI services. If they go down or are compromised, what happens to us?



WHY IT MATTERS:

Third parties can be a major source of cyber risk. A disruption or breach at a vendor, cloud provider or supplier can impact your systems, data, and ability to operate. Understanding and managing these dependencies helps reduce risk and improves your resilience.

KEY AREAS TO CHECK

Review the key third-party dependencies below and consider their impact on your organization.



CRITICAL VENDORS

Who are your essential vendors and what do they provide?



CLOUD PLATFORMS

Which cloud services do you rely on (e.g., email, storage, applications)?



MSPs & IT PROVIDERS

What services do they manage and how critical are they to operations?



SUPPLIERS

Which suppliers are essential to your products or services?



AI SERVICES

What AI tools or platforms do you use and what data or systems do they access?

DEPENDENCY CHECKLIST

Use this table to identify and assess your key third-party dependencies. Consider the potential impact if they are disrupted or compromised.

THIRD PARTY / VENDOR	SERVICE PROVIDED	HOW CRITICAL IS IT?	WHAT HAPPENS IF THEY GO DOWN?	RISK MITIGATION IN PLACE?
1				
2				
3				
4				
5				



KNOW YOUR DEPENDENCIES.
MANAGE THE RISKS.
KEEP YOUR BUSINESS MOVING.

Review your third-party relationships regularly, understand the risks, and have a plan in place. The more you know, the better prepared you are for disruptions.



USE AI WITHOUT CREATING NEW RISK

AI Checkpoint — Know What's Going In

Be mindful of what you enter into AI tools. Understand approved tools, protect sensitive data, and verify AI-generated output before using it.

Focus on: what employees can/cannot enter, approved tools, sensitive data, AI-generated output verification and ownership.



WHY IT MATTERS:

AI tools can be powerful, but they can also introduce new risks. Sensitive information entered into AI tools may be stored, used to train models, or exposed. Understanding how to use AI safely helps protect your data, your organization and your reputation.

KEY AREAS TO CHECK

Review the key areas below to understand how to use AI safely at work.



APPROVED TOOLS

Are you using company-approved AI tools?



SENSITIVE DATA

Are you entering confidential, personal or proprietary information?



WHAT CAN YOU ENTER?

Do you know what you can and cannot input into AI tools?



VERIFY OUTPUT

Is the AI-generated output accurate, appropriate and free of bias?



OWNERSHIP & USAGE RIGHTS

Do you understand who owns the output and how it can be used?

AI USAGE CHECKLIST

Use this table to review your AI practices and identify areas for improvement.

PRACTICE	YES	NO	ACTIONS NEEDED
1 I use only approved AI tools.	☐	☐	
2 I do not enter confidential, personal or proprietary information.	☐	☐	
3 I understand what I can and cannot input into AI tools.	☐	☐	
4 I verify AI-generated output before using it.	☐	☐	
5 I understand ownership and usage rights for AI-generated content.	☐	☐	



**USE AI SMARTLY.
KEEP INFORMATION SAFE.
GET THE BENEFITS WITHOUT THE RISK.**

Follow your organization's AI policies, use approved tools, avoid entering sensitive data, and always verify AI-generated output. Using AI responsibly helps you work smarter while keeping your information and organization safe.

MAKE THE CALL

Incident Decision Point — Who Does What?

When something goes wrong, clear roles and escalation triggers help you respond faster and reduce the impact.

**MAKE THE CALL
EARLY.
LIMIT THE IMPACT.**



WHY IT MATTERS:

A fast and coordinated response helps contain the issue, reduce disruption, meet legal and regulatory obligations, and protect your organization's reputation.

KEY ROLES DURING AN INCIDENT

Different teams have different responsibilities.



IT / SECURITY

Investigate, contain and restore.



LEADERSHIP

Make key decisions and escalate when needed.



LEGAL / PRIVACY

Assess legal and regulatory requirements.



COMMUNICATIONS

Manage internal and external messaging.



BUSINESS OPERATIONS

Keep critical functions running and coordinate workarounds.

ESCALATION TRIGGERS

If any of the following happen, escalate to the appropriate teams immediately.



Data breach or suspected compromise



Significant service outage



Financial impact (e.g., fraud, ransom)



Legal or regulatory notification required



Media attention or public interest

QUICK ACTION CHECKLIST

Use this checklist to confirm initial actions and who needs to be involved.

ACTION	IT / SECURITY	LEADERSHIP	LEGAL / PRIVACY	COMMUNICATIONS	BUSINESS OPS
1 Confirm what is happening.	☐	☐	☐	☐	☐
2 Contain the issue.	☐	☐	☐	☐	☐
3 Notify leadership.	☐	☐	☐	☐	☐
4 Assess legal or regulatory impact.	☐	☐	☐	☐	☐
5 Communicate internally or externally.	☐	☐	☐	☐	☐



**MAKE THE CALL. ACT TOGETHER.
REDUCE THE IMPACT.
KEEP YOUR BUSINESS MOVING.**

Know your roles, watch for escalation triggers, and communicate early.

KEEP THE BUSINESS MOVING

Recovery Route — What If Systems Go Down?

Be prepared to keep essential operations running if systems are unavailable. Plan for backups, manual workarounds and alternate communications.



**PLAN AHEAD.
KEEP OPERATIONS
MOVING.**



WHY IT MATTERS:

Systems can go down. Having backup plans and clear priorities helps you continue critical operations, reduce disruption and recover faster.

KEY AREAS TO CHECK

Review the key areas below to strengthen your recovery plans.



BACKUPS

Are your backups current and tested?



MANUAL WORKAROUNDS

Can critical work continue manually if needed?



ALTERNATE COMMUNICATIONS

Do you have backup ways to communicate with staff, customers and partners?



CRITICAL CONTACTS

Do you have an up-to-date list of essential contacts?



RECOVERY PRIORITIES

Have you identified what must be restored first?

RECOVERY READINESS CHECKLIST

Use this checklist to identify any gaps and plan next steps.

QUESTION	YES	NO	ACTIONS NEEDED
1 Do we have recent, tested backups?	☐	☐	
2 Can we continue essential functions manually?	☐	☐	
3 Do we have alternate communication methods?	☐	☐	
4 Do we have a list of critical contacts?	☐	☐	
5 Have we identified and prioritized what to restore first?	☐	☐	



**BE PREPARED.
STAY OPERATIONAL.
RECOVER FASTER.**

Test your backups, plan manual workarounds, keep critical contacts updated, and know your recovery priorities so your organization can keep moving.



TURN READINESS INTO ACTION

Your 30-Day Action Plan

Choose 3 things to fix, 1 process to test, 1 dependency to review and 1 exercise to run.



**TURN PLANS
INTO PROGRESS.**



WHY IT MATTERS:

Small, consistent steps today can make a big difference. Turning readiness into action helps you reduce risk, strengthen resilience and keep your organization moving.

YOUR 30-DAY PLAN

Fill in your action items below.



3 THINGS TO FIX

Identify and address your top 3 gaps.

1	
2	
3	



1 PROCESS TO TEST

Choose one key process to test (e.g., backup restore, incident response).

1	
---	--



1 DEPENDENCY TO REVIEW

Review one critical vendor, cloud platform or third party.

1	
---	--



1 EXERCISE TO RUN

Run one tabletop, drill or practical exercise.

1	
---	--

READINESS CHECKLIST

Use this checklist to track your progress over the next 30 days.

ACTION		COMPLETED
1	We have identified 3 key gaps to fix.	☐
2	We have selected 1 process to test.	☐
3	We have reviewed 1 critical dependency.	☐
4	We have planned or run 1 exercise.	☐
5	We have assigned owners and set timelines.	☐



**OUR ORGANIZATION
IS PREPARED WITH
READYSETCYBER.**

Take action, build stronger habits and keep progressing. A more secure and resilient organization starts with the steps you take today.

11

FINAL CHECKPOINT

TURN READINESS INTO ACTION

BE SMART. BE SAFE. BE READY.

You've completed the road map. Now it's time to turn awareness into action. Take simple, practical steps to strengthen your organization and keep the business moving.

YOUR 30-DAY ACTION PLAN

1



3 THINGS TO FIX

Identify and address your top 3 gaps.

2



1 PROCESS TO TEST

Choose one key process to test (e.g., backup restore, incident response).

3



1 DEPENDENCY TO REVIEW

Review one critical vendor, cloud platform or third party.

4



1 EXERCISE TO RUN

Run one tabletop, drill or practical exercise.



**OUR ORGANIZATION
IS PREPARED WITH
READYSETCYBER.**



STRONGER PEOPLE

More aware and empowered.



CLEARER PROCESSES

Practised and continuously improved.



A MORE RESILIENT ORGANIZATION

Ready for what's next.

