Maverick Gardner Information Technologies & Solutions Inc.
1260 Journey's End Circle, Unit 11
Newmarket, Ontario
L3Y 8Z7

Cybersecurity for Canadian SMBs

Protecting.Your.Business.in.a.Connected.World

Prepared by Maverick Gardner Information Technology & Solutions

1. Introduction

In an era where digital operations drive business success, Canadian small and medium-sized businesses (SMBs) are increasingly targeted by cybercriminals.
Limited resources, remote work, and reliance on cloud systems make SMBs a prime target — yet many remain underprepared.

This whitepaper outlines current cybersecurity challenges facing Canadian organizations, explores the latest threat landscape, and provides actionable strategies to strengthen resilience.

2. The Canadian Cyber Threat Landscape

According to the **Canadian Centre for Cyber Security (CCCS)**, over **60% of cyberattacks in 2024** targeted SMBs.
The impacts include data loss, reputational harm, financial penalties, and operational downtime — often devastating for smaller enterprises.

Common Threats Facing SMBs

- **Phishing & Business Email Compromise (BEC):**
  Deceptive emails trick users into revealing credentials or approving fraudulent payments.
- **Ransomware:**
  Attackers encrypt business data, demanding payment for recovery.
- **Supply Chain Attacks:**
  Breaches through vendors or managed service providers (MSPs).
- **Insider Threats:**
  Accidental or malicious employee actions exposing sensitive information.
- **Cloud Misconfiguration:**
  Unsecured cloud storage or permissions leading to data leaks.

3. Why SMBs Are Targeted

Cybercriminals exploit SMBs for several reasons:

- Smaller budgets for cybersecurity tools and training
- Outdated systems and weak patch management
- Fewer dedicated IT or compliance staff
- Access to larger organizations through vendor relationships

Fact: 1 in 5 SMBs in Canada experiences a cybersecurity incident every year.
(Source: CyberSecure Canada, 2025)

4. The Cost of a Breach

Even a single breach can be crippling:

- **Average cost per incident:** $300,000+ (IBM 2024)
- **Average downtime:** 23 days
- **Permanent customer loss:** up to 40% after a publicized incident

The indirect costs — brand damage, lost productivity, and regulatory noncompliance — often exceed the immediate financial loss.

5. A Framework for SMB Cyber Resilience

The path to cybersecurity maturity begins with a framework built around **five key principles** inspired by ISO 27001 and the **NIST Cybersecurity Framework**.

Principle	Description	Key Activities
Identify	Understand what assets you need to protect	Inventory systems, classify data, assess risk
Protect	Implement safeguards and access controls	MFA, encryption, patching, awareness training
Detect	Monitor for abnormal activity	Endpoint protection, SIEM alerts, threat intel
Respond	Establish clear response protocols	Incident response plan, playbooks, containment
Recover	Ensure continuity and resilience	Backups, disaster recovery, business continuity plans

6. Top 10 Cybersecurity Best Practices for Canadian SMBs

1. **Adopt Multi-Factor Authentication (MFA)** across all accounts and systems.
2. **Encrypt sensitive data** at rest and in transit.
3. **Maintain regular, tested backups** offline or in immutable storage.
4. **Apply updates and patches** promptly for all software and firmware.
5. **Train employees regularly** on phishing and cyber hygiene.
6. **Segment your network** to contain potential breaches.
7. **Implement endpoint protection** and advanced threat detection.
8. **Secure cloud services** through configuration reviews and logging.
9. **Create an incident response plan** and practice tabletop exercises.
10. **Engage a trusted Managed Security Partner** (like Maverick Gardner ITS).

7. Canadian Compliance and Standards

Aligning with security frameworks improves resilience and regulatory compliance:

Framework	Purpose	Key Relevance
ISO 27001:2022	International information security standard	Structured ISMS implementation
CyberSecure Canada	Federal SMB certification program	Recognized baseline cybersecurity controls
NIST CSF	US-based, risk management framework	Strong model for control maturity
PIPEDA	Canadian privacy law	Governs personal data handling

Achieving alignment not only protects your data — it also increases credibility with clients and partners.

8. The Role of a Managed Security Partner

For most SMBs, hiring full-time cybersecurity specialists isn't feasible.
A **Managed Security Partner (MSP)** provides scalable protection through continuous monitoring, threat response, and compliance management.

Maverick Gardner ITS offers:

- 24/7 monitoring and incident response
- Policy and compliance management (ISO, NIST, CGP)
- Endpoint and network defense
- Cloud and data security optimization
- Employee awareness and training programs

9. Building a Culture of Cyber Awareness

Technology alone can't stop every threat — your people are the first and last line of defense. Encourage a security-first mindset through:

- Regular phishing simulations
- Monthly awareness micro-trainings
- Leadership-driven communication on security priorities

10. Conclusion

Cybersecurity is no longer optional — it's foundational to business survival.
By adopting proven frameworks, implementing layered defenses, and partnering with experts, Canadian SMBs can reduce risk and strengthen trust with customers and stakeholders.

11. About Maverick Gardner ITS

Maverick Gardner Information Technology & Solutions provides **Managed IT Services**, **Compliance-as-a-Service**, and **Cybersecurity Solutions** that help organizations remain secure, compliant, and operationally resilient.

We serve clients across Canada in critical industries — including nuclear, defense, manufacturing, and professional services — with technology built for trust.

info@maverickgardner.com
647-484-6045
www.maverickgardner.com