Building strong defenses against evolving cyber threats

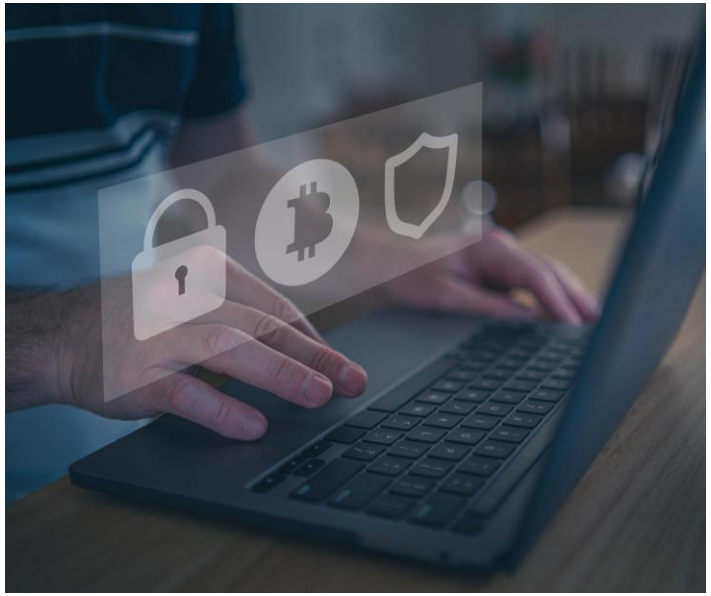
Cybersecurity 101: From Reactive to Resilient

Why Cybersecurity Matters for NZ SMBs

Rising Cyber Threats

The National Cyber Security Centre has reported that there were:

- **Over 7,000 incidents** were reported, mostly affecting individuals & SMBs.
- **32% of serious cases** involved suspected state-sponsored actors.
- **$21.6 million** in financial losses were reported, mostly by SMBs.



Gaps in Security Awareness

Many SMBs rely on basic antivirus but lack training, causing vulnerabilities like phishing scams.

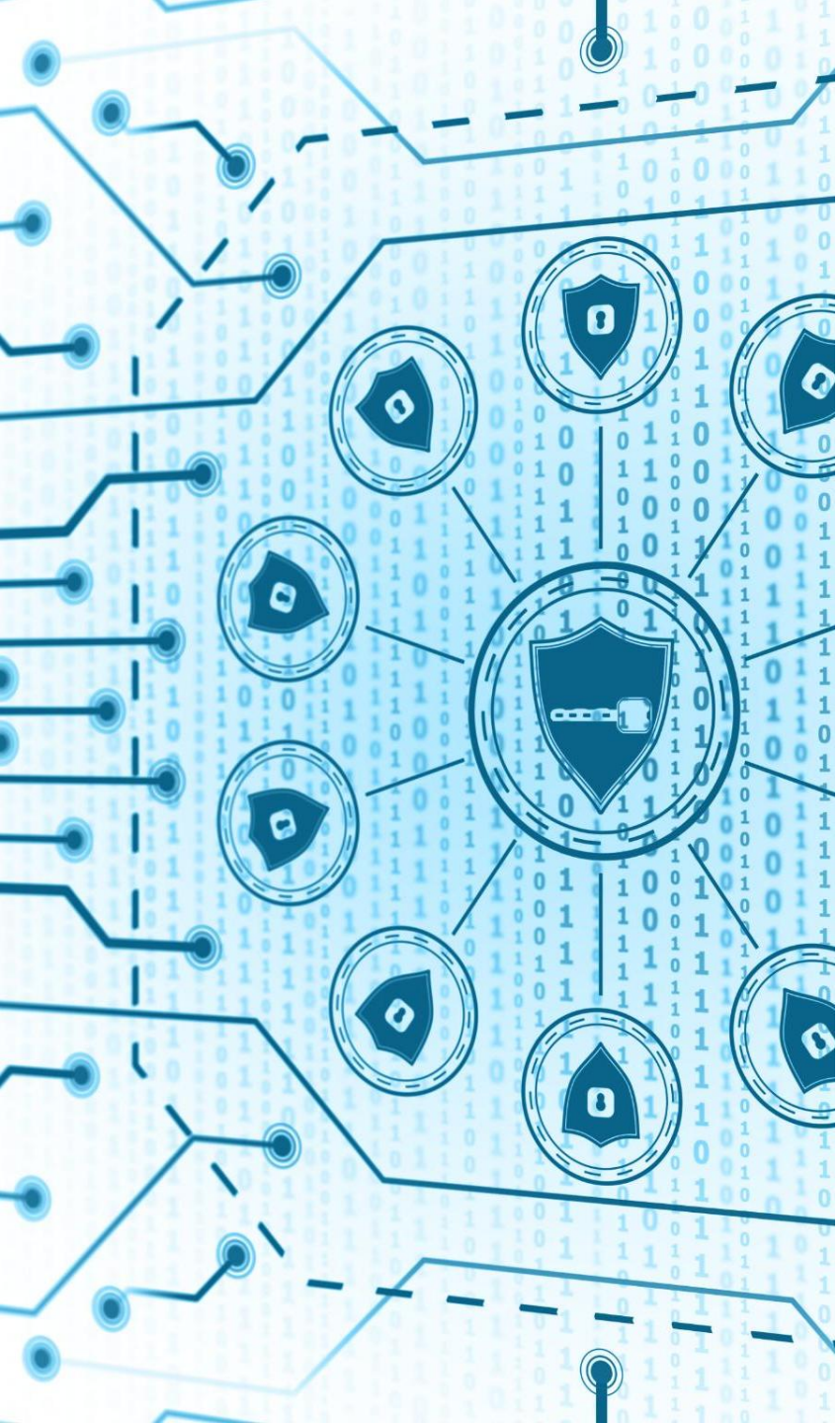
Business Impact

Cyber-attacks threaten business continuity, customer trust, and lead to financial instability.

Need for Proactive Security

SMBs must adopt resilient cybersecurity practices to protect and thrive in a digital world.

focus technology group



Reactive vs. Resilient Mindset

Reactive Mindset Challenges

Reactive cybersecurity waits for threats, often causing panic, financial loss, and reputational damage.

Resilient Mindset Benefits

Resilient cybersecurity anticipates threats, blocks early, and recovers quickly, ensuring business continuity.

Smart Protection Strategies

Smarter layered defenses with real-time monitoring and AI-driven detection improve threat management.

Business Priority and Culture

Viewing cybersecurity as a business priority empowers teams and fosters continuous improvement culture.

focus technology group

Be Proactive

Preventing Cyber Threats

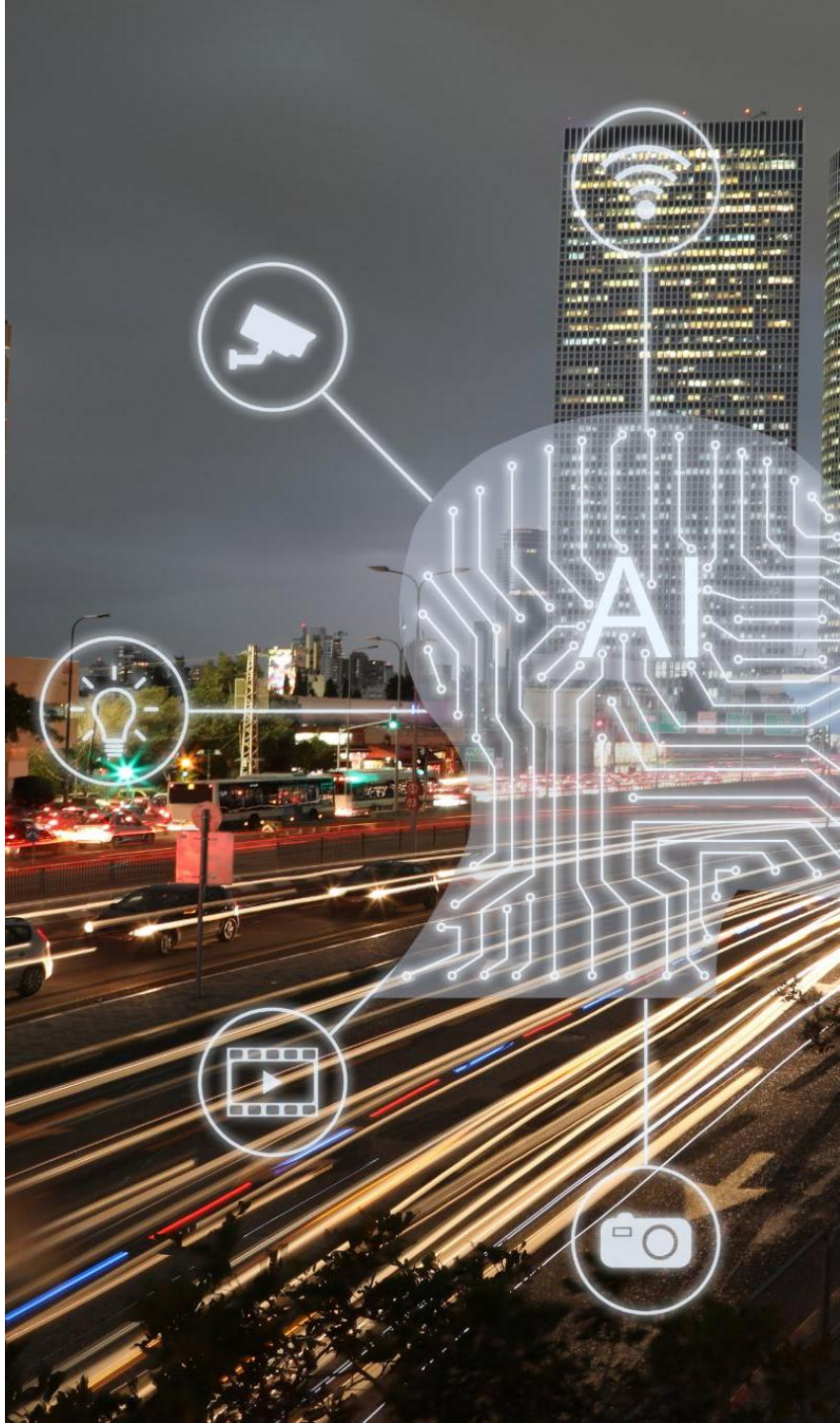
Proactive cybersecurity involves preventing cyber threats before they cause harm, using tools like AI, real-time monitoring, and threat intelligence to detect and respond to risks early.

Affordable SMB Solutions

Cloud-based threat intelligence tools offer cost-effective protection options tailored for small and medium businesses.

Building Confidence

- Proactive security measures help **build trust** among employees and customers.
- By safeguarding digital assets, businesses demonstrate a commitment to data protection - enhancing their reputation and stakeholder confidence.



Layer Your Protection

Multiple Security Layers

Layered protection secures devices, emails, networks, and cloud services, forming barriers against attacks.

Essential Security Tools

Firewalls, antivirus software, and VPNs are critical tools for implementing layered cybersecurity defenses.

Zero-Trust Approach

Zero-trust means always checking who’s trying to access company systems to keep data safe.

SMB Cybersecurity Planning

Small businesses can achieve layered protection by assessing systems, identifying gaps, and integrating solutions.

focus technology group

Train Your Team

Employee Cybersecurity Awareness

Employees serve as the first defense line, making awareness essential to prevent cyberattacks.

Key Training Topics

Training includes spotting phishing, using strong passwords, enabling 2FA, and avoiding risky behaviors.

Reinforcing Training

Regular workshops, simulations, and reminders help embed good cybersecurity habits in staff.

Building Security Culture

Empowering employees with responsibility fosters a resilient and secure business environment.

focus technology group

Plan for Recovery

Importance of Recovery Planning

A recovery plan minimises damage during cyber incidents and reduces downtime and financial loss. Regular testing and updates keep the plan effective.

Backup Strategies

Maintaining regular backups offline and in the cloud ensures data can be quickly restored after an incident, protecting business operations.

Cyber Incident Response Plan

CIRP defines roles and actions during an attack, including IT support contact, customer communication, and system restoration, ensuring swift response.

Building Trust and Professionalism

A well-executed recovery plan protects data, maintains operations, and builds stakeholder trust by demonstrating professionalism.

focus technology group

Keep Improving

Ongoing Cybersecurity Effort

Cybersecurity requires continuous attention and regular audits to identify and fix vulnerabilities promptly.

Proactive Risk Management

Scheduling periodic reviews of policies and training helps businesses stay ahead of evolving cyber threats.

Learning and Adaptation

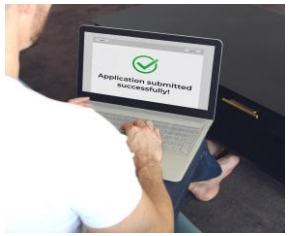
Continuous improvement involves learning from incidents and updating response plans to build resilience.

Building Security Culture

Embedding cybersecurity into operations fosters a culture of security and maintains customer trust.

focus technology group

Simple Security Wins



Basic Cybersecurity Actions

Keeping software updated and using two-step login significantly reduces cybersecurity risks for SMBs.

Strong Passwords and Backup

Using strong, unique passwords together with regular data backups protects against common breaches.

Employee Security Awareness

Encouraging staff to follow best practices and use security tools fosters a safer business environment.

focus technology group

Cybersecurity Myths

1. Antivirus is enough

Reality: AV only catches known threats. Modern attacks often bypass traditional antivirus, requiring layered security like threat detection and response.

2. I'm in the cloud now I don't have to worry about backups.

Reality: Being in the cloud doesn't eliminate the need for backups – you're still responsible for protecting your data from deletion, corruption, or ransomware.

3. Cloud backup means I'm safe

Reality: Cloud backups help recover lost data, but they don't stop cyberattacks. If malware hits, it can infect your backups too – unless they're properly protected.

4. I have a firewall, so I'm protected

Reality: Firewalls block unauthorised access, but they don't stop insider threats, phishing, or advanced attacks. You need continuous monitoring and user awareness.

focus technology group

Final Takeaway

Building Cyber Resilience

Strengthen security by investing in proactive tools, training, audits, and recovery planning.

Shared Responsibility

Cybersecurity impacts all teams, not just IT; everyone must understand and support security efforts.

Future Outlook

Advances in smarter, affordable cybersecurity tools and greater education make staying prepared easier.

Call to Action

Starting now with resilience-building and integrating cybersecurity into business strategy is essential.

focus technology group