Is Your Business at Cyber Risk?

Penrose Business Association - Cyber Risk Breakfast

April 2024

Agenda

- What does the cyber risk landscape look like in 2024
- What to do if the worst happens
- How to protect your business
- Learn about what insurers are looking for
- Easy wins
- Live demo of RubberDucky exploit
- Exclusive offers for PBA Members

About Lucidity

- Lucidity are a cloud first Managed Service Provider **established in 2003** in Auckland, New Zealand.
- Our mission is to deliver **high-quality security-focused solutions** that are **cost-effective for small and medium-sized businesses**.
- We are an **award-winning Microsoft Partner** specialising in Microsoft 365 and Azure, and the network and security needed to do so safely and efficiently.
- Lucidity works with over **150 customers across NZ** with staff in Auckland, Hamilton, Gisborne, Wellington and Christchurch.
- Lucidity's founders still actively work within the business; supported by a growing team of 20, with **strong subject matter expertise** within our specialties.

> Lucidity aspires to be your technology partner of choice that enables modern ways of working

Introduction

- Kiwi businesses have traditionally held the view that "**It'll never happen to us. We are small**" But it is happening and more and more.
- Small businesses are especially susceptible, as they **possess valuable information but may lack the robust security** measures of larger organisations.

Introduction

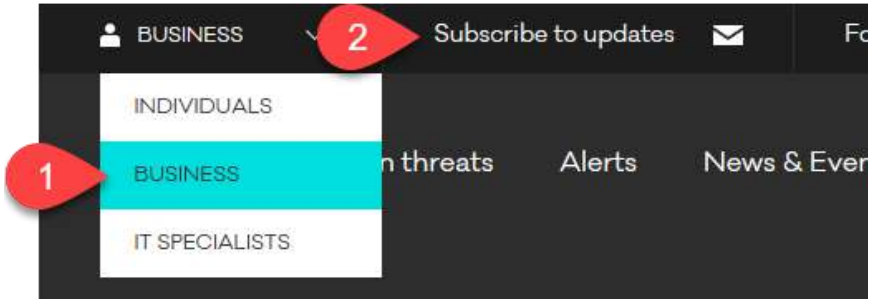
- The cost of a cyberbreach could be huge – not just financially:
  - **Financial** loss
  - **Reputational** loss may impact current and future business.
  - **Data Loss** could set your business back years and **intellectual property may be leaked.**
  - **Technical Damage** may leave your business crippled, affecting your ability to do business.
  - Operational Impact **diverts significant time and effort from normal business** operations.
  - **Stress** on business owners and staff can be enormous.

Introduction

- There are also privacy considerations:
  - Companies which “fail to take adequate care” could be penalised legally and financially – NZ have the Privacy Act 2020
  - Internationally, there are already strong laws such as GDRP that enforce this.
  - Australia has recently toughened laws including an increase to maximum fines from $2.22M to $50M!
  - NZ is likely to follow suit. Currently fines typically range from $10k to $50K.

The Statistics

- CERT NZ is the New Zealand government's dedicated team for cybersecurity incident response.
- Every quarter they publish statistics on *reported* cyber incidents
- They also report vulnerabilities, so its worth subscribing - > https://www.cert.govt.nz/

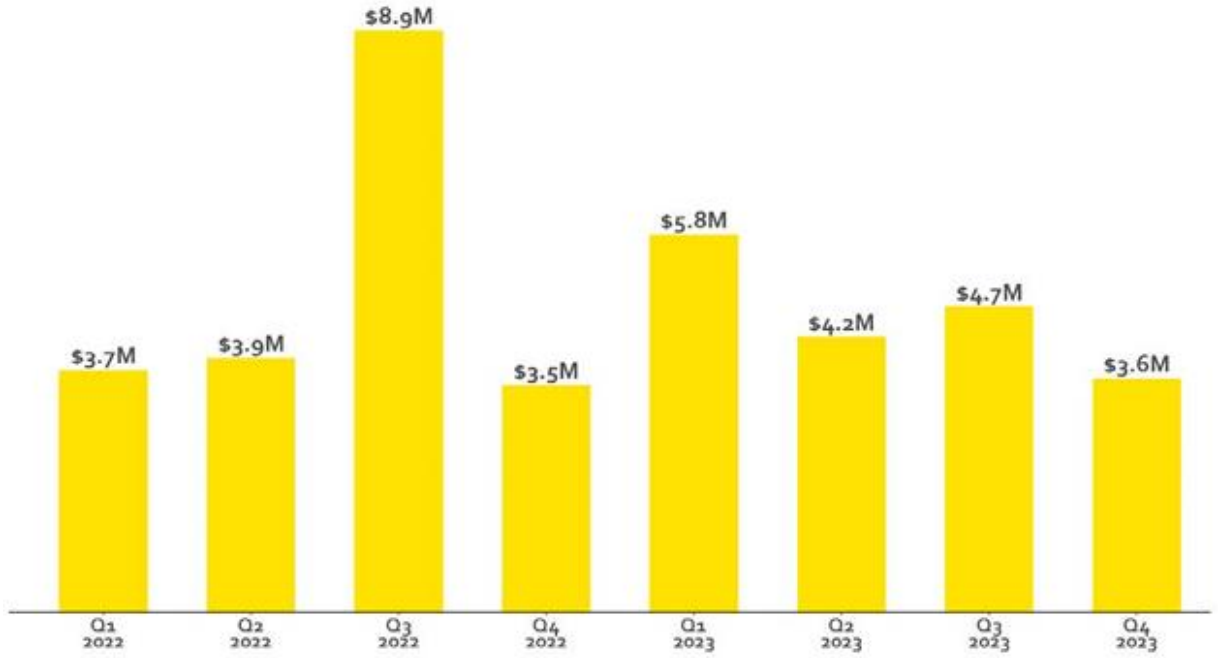


Reported losses in NZ

Q4 2023 - CERTNZ

- $3.6M in losses Q4
- $16M in losses over last 4 quarters

Figure 8: Direct financial losses per quarter

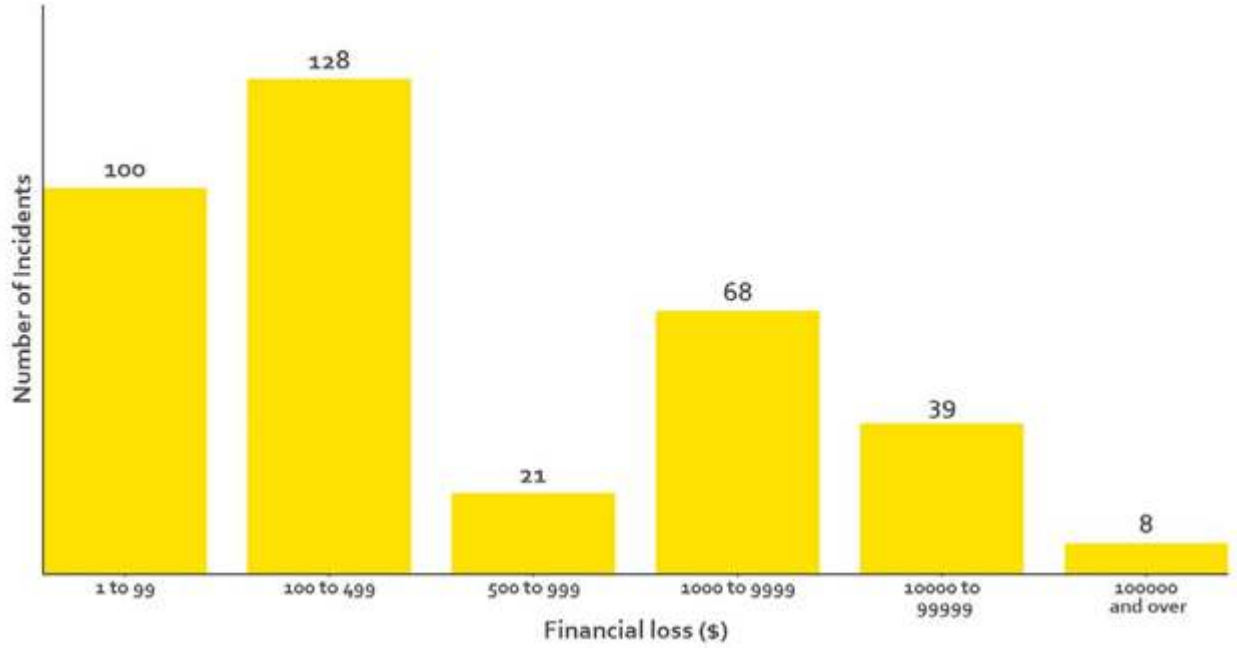


Size of losses

Q4 2023 - CERTNZ

- 39 losses over $10,000+
- 8 losses over $100,000+

Figure 9: Distribution of direct financial losses



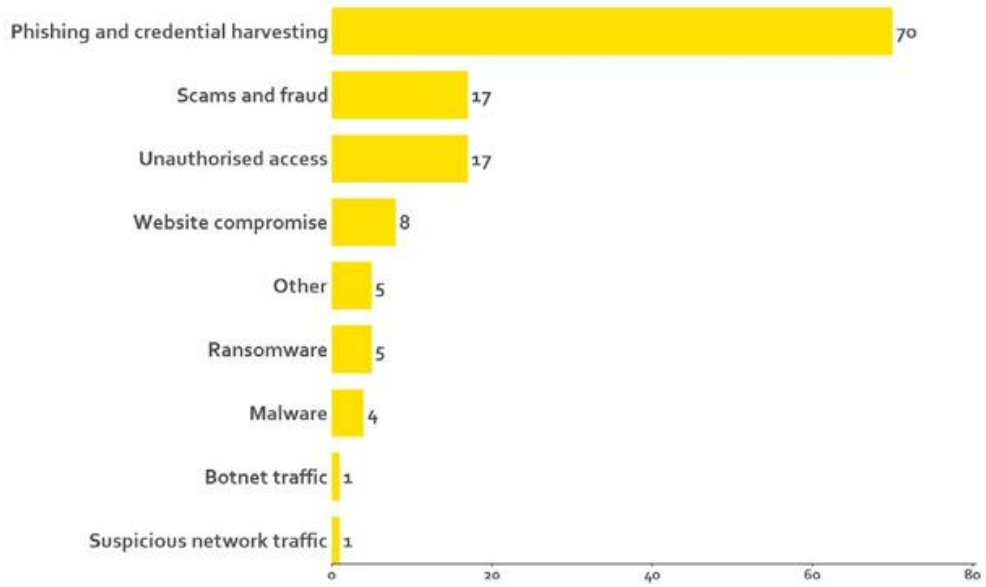
Top incidents affecting businesses

Q4 2023 - CERTNZ

128 incidents (7%) reported to CERT NZ specified that they **affected organisations**.

Phishing & credential harvesting far out in front.

Figure 5: Breakdown of incidents affecting organisations



1. Phishing and credential harvesting. Types of email, text or website attacks designed to convince users they are genuine, when they are not. They often use social engineering techniques to convince users of their authenticity and trick people into giving up information, credentials or money.
2. Scams and fraud. Computer-enabled fraud that is designed to trick users into giving up money. This includes phone calls or internet pop-up advertisements designed to trick users into installing fake software on their computers.
3. Unauthorised access. Successful unauthorised access can enable an attacker to conduct a wide range of malicious activities on a network, infrastructure or computer. These activities generally fall under one of the three impact categories: compromise of the confidentiality of information, improper modification affecting the integrity of a system, degradation or denial of access or service affecting its availability.
4. Website compromise. The compromise, defacement or exploitation of websites by attackers for malicious purposes, such as spreading malware to unsuspecting website visitors.
5. Other
6. Ransomware. A common malware variant with a specific purpose. If installed (usually by tricking a user into doing so, or by exploiting a vulnerability) ransomware encrypts the contents of the hard drive of the computer it is installed on, and demands the user pay a ransom to recover the files.
7. Malware. Short for malicious software. Malware is designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Commonly includes computer viruses, worms, Trojan horses, spyware and adware.
8. Botnet traffic. Botnets are networks of infected computers or devices that can be remotely controlled as a group without their owner's knowledge and are often used to perform malicious activities such as sending spam or launching Distributed Denial of Service attacks.
9. Suspicious network traffic. Detected attempts to find insecure points or vulnerabilities in networks, infrastructure or computers. Attackers typically conduct a range of reconnaissance activities before conducting an attack, which are sometimes detected by security systems and can provide early warning for defenders.

No city or sector is safe

Q4 2023 - CERTNZ

Of the 128 reports affecting organisations, the finance and insurance sector accounted for 38% - a considerable margin!

Figure 10: Reports by sector

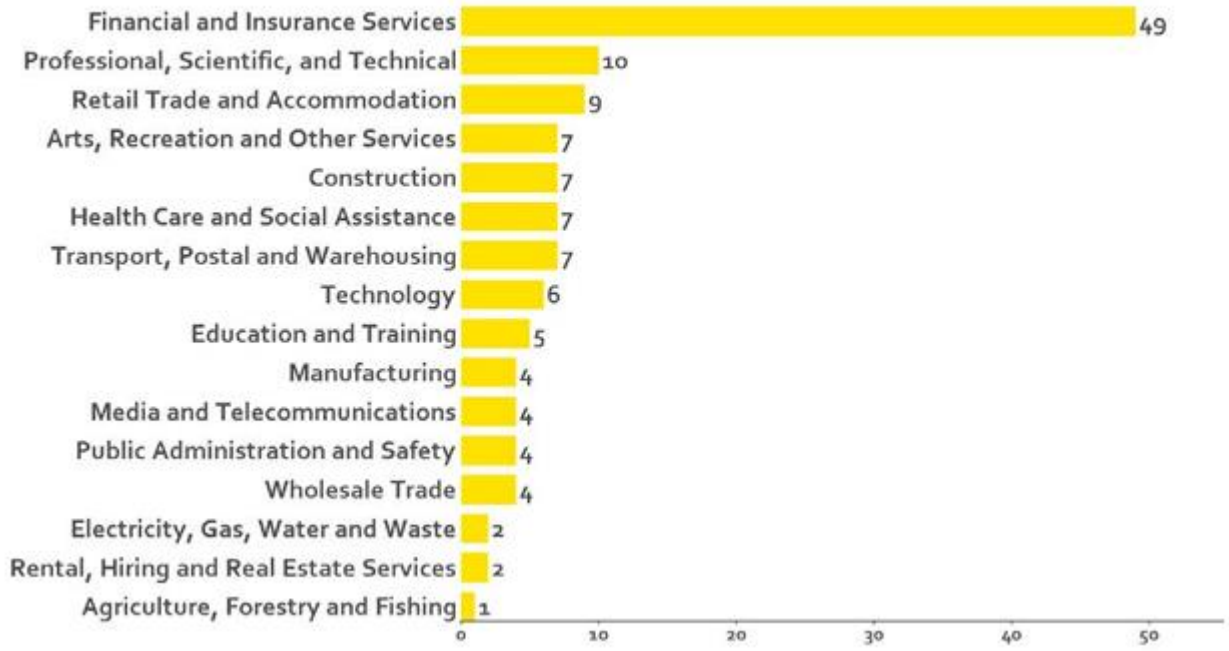


Figure 11: Breakdown of reports by region

If the worst happens

- If you suspect a cybercrime, **shutdown and call your IT provider/team immediately.** Quick reaction could reduce the damage.
- **Call your insurer –** your policy may include resources including technical, legal and ransom negotiators.
- If there is large scale impact, **create an incident response team** and include separate people for technical and comms, and assign a leader.

Protecting your business

Priority	Offensive or Defensive Strategy	Why
One	Backups	No backup = no recovery!
One	Multi-Factor Authentication	99.9% of compromised accounts don't have MFA!
Two	XDR (nextGen anti-virus)	Attacks start on devices and servers and can be detected and remediated automatically using XDR.
Two	Anti-Spam Filtering	Spam is a top way to infect or convince a user to give away their credentials **via Phishing/Credential Harvesting**
Two	Operating System Update Management	Updated operating systems have less vulnerabilities to exploit.
Two	Security awareness training	Most cyber attacks start by a user being tricked. Training helps to avoid this.
Two: Inbound connections Four: Outbound connections	Firewall (ideally w/ Advanced Threat Protection)	Firewalls are important to protect services that are exposed to the internet.

KEY: Red = MUST HAVE Blue = Included in Microsoft 365 Business Premium.

Defensive strategies build robust defences to deter threats. Offensive strategies uncover & address vulnerabilities before attackers do.

Protecting your business

Priority	Offensive or Defensive Strategy	Why
Three	Detection & Response Team (SIEM/SOC)	Real-time monitoring of potential threats ensures eyes are on the ball and attacks can be stopped quickly.
Three	Security Hardened Devices and Servers	Harden devices are less likely to be exploited.
Three	Dark Web monitoring & identity theft protection	By monitoring for leaked credentials, you can proactively reset users' passwords.
Three	App Control (black/white-listing)	Controlling what is allowed to run on a device or server will stop a threat actor running tools to facilitate an attack.
Three	Web content filtering & monitoring	Checks web destinations are safe based on a database thus stopping users accidently browsing to malicious sites.
Three	Vulnerability Scanning	Automated scanning of system vulnerabilities provides an opportunity to remediate before a cyber criminal attempts to exploit it.
Four	Automatic email signatures	Consistent signature branding helps recipients detect falsification.
Four	Password Manager	Password managers help your users maintain good password hygiene by making it easier to have unique passwords across all systems/apps.
Four	Penetration testing	Penetration testing proactively tests the security of systems to uncover & address vulnerabilities before attackers do

KEY: Red = MUST HAVE Blue = Included in Microsoft 365 Business Premium.

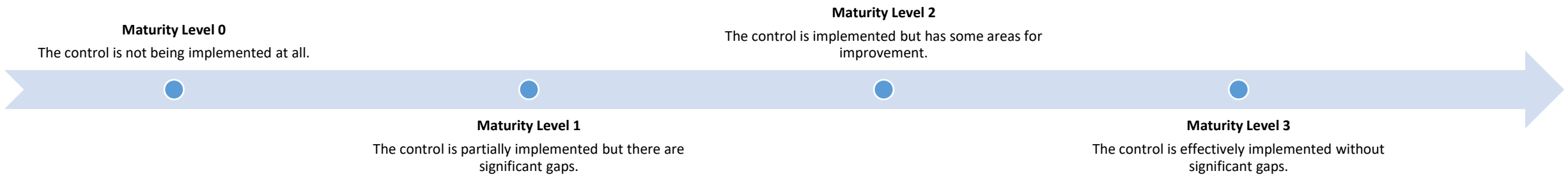
Defensive strategies build robust defences to deter threats. Offensive strategies uncover & address vulnerabilities before attackers do.

Using a framework to guide you – Essential Eight (AU)

Others Include: CERTNZ (basic guidance), CIS, NIST

- A framework can help guide your implementation and its priorities.
- Your goal should be to keep improving your security so your organisation through the maturity levels for each of the eight controls.

Essential Eight Controls	Purpose
1. Application control	To prevent unauthorised applications from running on your systems
2. Patch applications	To keep your apps up-to-date with the latest security patches
3. Configure Microsoft Office macro settings	To protect your systems from malicious macros hidden inside commonly used files
4. User application hardening	To make applications more secure against attacks
5. Restrict administrative privileges	To reduce the risk of unauthorised access to your systems
6. Patch operating systems	To keep your operating systems stable and secure against vulnerability exploitation
7. Multi-factor authentication	To add one or more layers of security before a user can log in
8. Regular backups	To ensure that you have a copy of your data in case it is lost or corrupted



Is cyber insurance worth considering?

- According to an Aviva Insurance survey, cyber events are:
  - 67% more likely than physical theft
  - 400% more likely than a fire
  - Yet most companies are not insured for the risk
- Cyber insurance not only helps with the financial impact, but also:
  - Response, recovery and legal
  - Greatly reducing stress on your business.
- What insurers are looking for at a minimum:
  - Multi-Factor Authentication
  - 3 copies of all backups – production data, backup set, offline backup set

Easy Wins

- Lock your machines when you get up and walk away – we'll show you why next...
- Make sure you have backup – including M365 backup
- Turn on MFA for ALL users
- Have a disaster recovery plan
- Look into cyber insurance
- Passphrases rather than passwords

Live Demo: Rubber Ducky

Lucidity Cloud Services

- What is a rubber ducky?
  - A rubber ducky is a USB key looking device that registers itself with your computer and pretends to be a keyboard. It can type incredibly fast, launching almost anything it wants to.
  - It uses a loophole that most end user devices (Android, iOS, Windows, Mac) all universally trust a keyboard / mouse device without prompting the user or triggering any kind of Antivirus software.

Exclusive Offers for PBA Members

- Free M365 Security Assessment and Recommendations

Questions?

Contact

Lucidity Cloud Services

Email: info@lucidity.co.nz

Web: www.lucidity.co.nz

Phone: +64 9 363 8888

+64 (0)800 HOSTED

References

- CERTNZ - https://www.cert.govt.nz/
- CERTNZ Q4 Report – CERT-NZ-Q3-2023-Data-Landscape-Report-V2-NON-EMBARGO.pdf
- Essential Eight - Essential Eight | Cyber.gov.au