KINETICS GROUP
making IT work for you

CYBER THREAT UPDATE

10 minute read for Directors, CEOs & Operations Managers

Q2 2023

www.kinetics.co.nz

Are you Feeling **Lucky**?

> **" A cybercriminal only has to be lucky once, while a defender has to be lucky every minute of every day. "**

From Combatting Ransomware – A Comprehensive Framework for Action, Key Recommendations from the US Dept of Justice Ransomware Task Force.

The question governance boards are increasingly asking is '**can we prevent hackers from stealing our data?**'

Cyber-crime is a mega-business worth billions of dollars. The cost and effort to combat attacks is increasing. Nothing is guaranteed and the work required to reduce your risk is rapidly evolving.

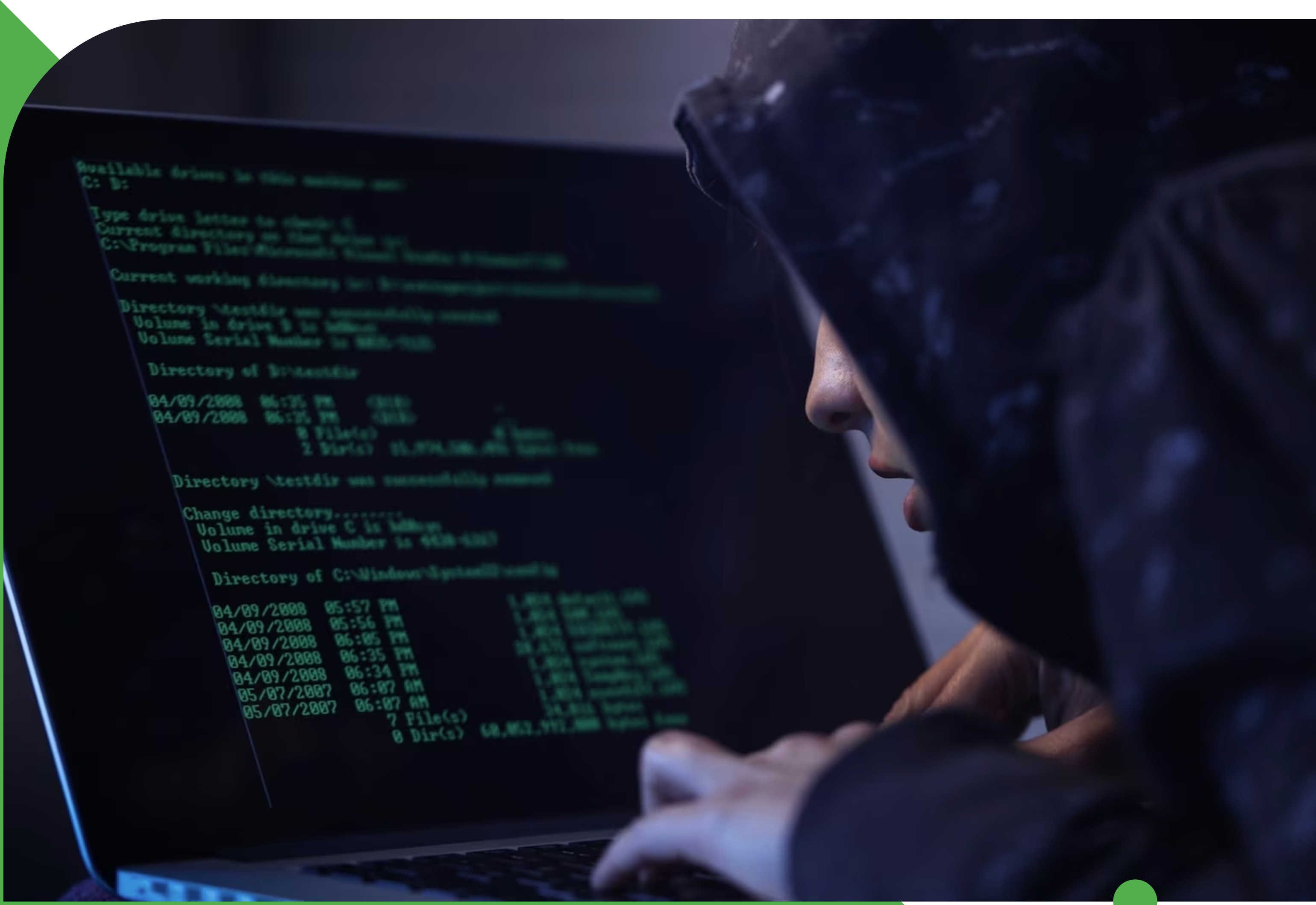
Attacks are getting faster.

AI and machine learning tools let hackers attack your business, test your passwords, and throw new malware at you before your systems can keep up

A Lot Can Happen Between your Morning Coffee and your Lunch.

That’s all it takes to go from ‘normal’ to ‘disaster’ when the hackers strike.
Microsoft researchers recently worked backwards through a ‘BEC’ attack (business email compromise – IT people love to convert everything into three-letter acronyms).

They found the hackers set up fake ‘typo-squatting’ email domains and had hijacked an email thread within a couple of hours. That’s the time from when they started setting up until when they struck.
The business would have had very little warning that they were under attack before the hackers were already harvesting confidential information.



What is at Stake?

Monetary loss is the least of your worries

This obviously can't be ignored. The smallest cost is any ransom you decide to pay (see below for data on whether that is a good idea). There is the cost of remedial action, lost productivity due to disruption, and the revenue impact from lost customer confidence. Add to that, the costs in dealing with any potential prosecution and fines. **Your insurance may not cover you for any of these events – 2 of the 3 global re-insurers no longer insure for ransomware payments.**

Reputation

A key risk for you and your organisation. You will likely be able to think of organisations you know were compromised. The impact on reputation is long-lasting. When an organisation had not taken due care, the reputations of the leaders and governors is also impacted. **That means you.**

Prosecution under the Privacy Act

Privacy legislation and regulation has tightened considerably as New Zealand aligns with Europe's General Data Protection Regulation (GDPR) for example, the December 2020 changes to the Privacy Act. Don't become a poster child for breaching NZ laws – **ensure you are aware of your obligations and have taken reasonable steps to protect privacy.**

HOW CAN YOU PROTECT YOU & YOUR ORGANISATION?

How much cyber-protection is enough?

New tools and systems means that Cyber-protection just gets more expensive every year

GCSB Annual Report 2021 – 22

DOWNLOAD

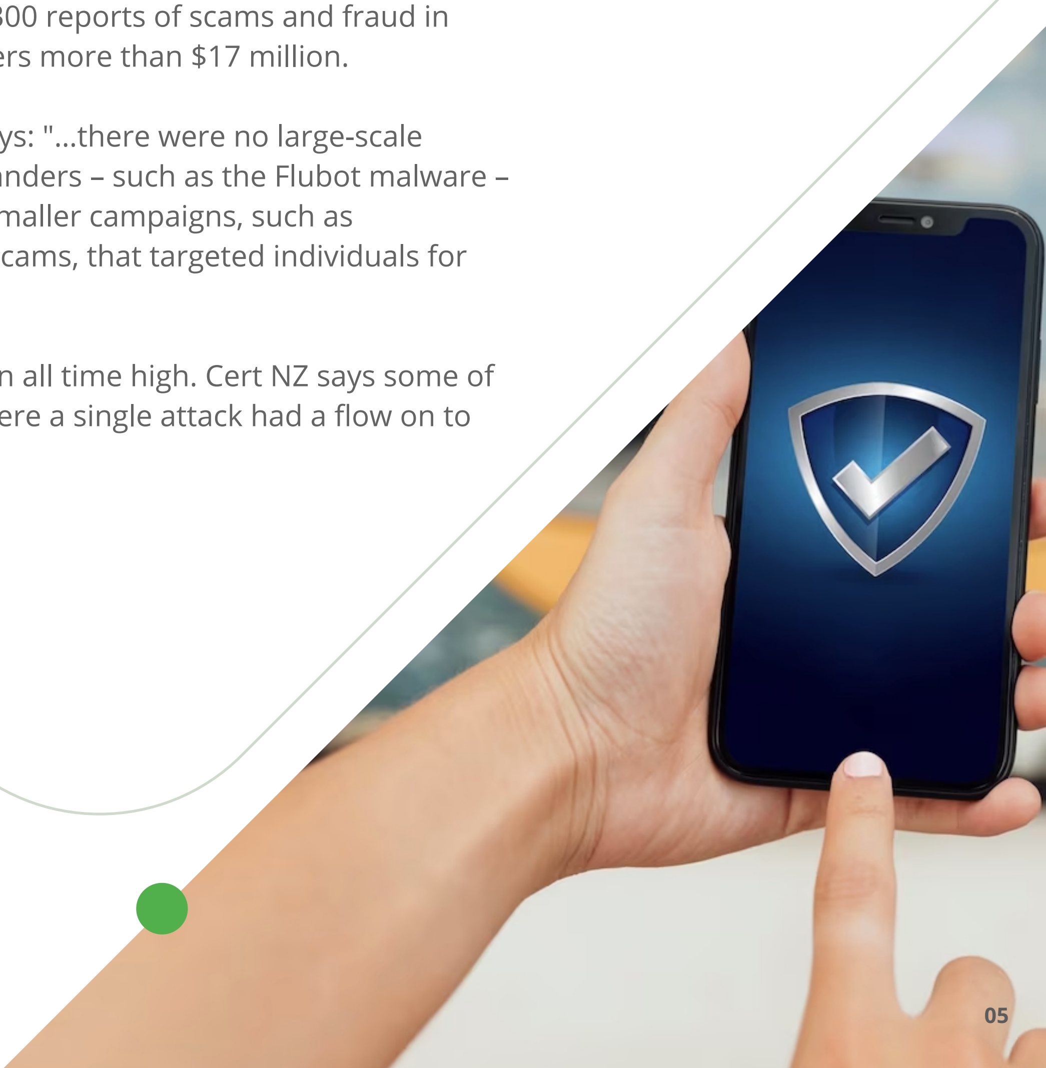
It's a trend that won't end soon. The latest GCSB Annual Report (March 2023) states "The cyber threats that Aotearoa New Zealand faces continue to evolve to become more persistent more sophisticated and more capable of causing severe impact to service delivery and information security"

New tools, new processes and new staff awareness is required. **The protections that seemed excessive a year ago are now inadequate.** With the pace of change, tools and processes must be thoroughly reassessed every year.

According to Cert NZ, the government's Computer Emergency Response Team, there were 2,300 reports of scams and fraud in 2022. These cost New Zealanders more than $17 million.

Rob Pope, Cert NZ's director says: "...there were no large-scale campaigns targeting New Zealanders – such as the Flubot malware – in 2022. However, we did see smaller campaigns, such as unauthorised money transfer scams, that targeted individuals for large losses."

Ransomware reports were at an all time high. Cert NZ says some of these were linked incidents where a single attack had a flow on to other organisations.



Timing is everything.

Hackers aren't waiting for you to get ready. They are testing your systems today. If they don't succeed today, they will try again tomorrow, with smarter techniques

One day, despite everything, they might succeed.

You can delay a cyber event by laying down the right foundations and making it harder to disrupt your business.

Defence – EDR usurps antivirus

Antivirus (AV) is not good enough anymore. The threat landscape moves too quickly.

That's why we now need 'End Point Detection and Response' technology (EDR).

Full EDR adds to AV with advanced threat detection. It uses "Behavioural Analytics " to go beyond known signature libraries which are based on past activities and combines it with AI/Machine Learning to look holistically at patterns to detect live activity threats.

Deterrence

Smarter tools, and newer defences are needed.

> **DETECTION** is critical to ensure a rapid response if something does happen. That needs tools that are looking at your systems, such as your Microsoft 365, for unexpected behaviours like large file copies, unusual email rules and much more. Any of these can be a clue that a user account has been compromised.

Educate

The most common vector of an attack is human error. Whether it's complacency or a busy person working quickly, we are all at risk.

Reminders, education and testing is the best way of keeping up our vigilance.

Awareness training, briefings, phishing tests and fire drills all help to address human risk.

What tools do ORGANISATIONS NEED TODAY?

From 'Shadow IT' detection to 'dark-web monitoring', from 'zero-trust' to password vaults - cyber-protection software is a new and real cost burden that modern workplaces to allow for. The challenge is finding the right level to match your risk/reward profile.

Is Cyber-insurance worth it?

Like any insurance, the provider wants to manage their risk by checking you are taking reasonable steps to protect your organisation first, and keeping those steps in place

Unless you are prepared to take these steps, your insurance may not pay out.

Make sure your IT team or partner can prove your protection meets the requirement of your insurer so your insurance gives you the protection you expect

We can reduce your cyber-risk but no one can guarantee you won't get hacked.

That's why cyber-insurance makes complete sense to us. We just point out that meeting the providers requirements is important because if an insurance provider won't take your risk on, why should you?

Where do you start?

3 STEPS to find the right protection for your business

01 Policy/Posture (Governance)

This involves defining clear guidelines, policies, and procedures for cybersecurity within the organization. Key actions to take include:

- Establishing a cybersecurity framework: Adopt a recognized framework such as NIST Cybersecurity Framework or ISO/IEC 27001, which outlines guidelines for cybersecurity best practices.
- Conducting regular risk assessments: Assess the organization's cybersecurity risk, identify vulnerabilities, and prioritize areas that need attention.
- Developing security policies: Establish security policies that address access control, password management, data handling, remote work, and incident response.
- Establishing incident response procedures: Develop clear procedures for detecting, reporting, and responding to security incidents.

KINETICS OFFERS A "POLICY, PROCESS AND RISK – IT POSTURE SECURITY REVIEW"

02 People Protection

The most significant risk in many organisations is their people. Often busy people are the most vulnerable simply because they are operating at speed, or because people are too trusting. Every day it seems the NZHerald or Stuff websites have stories about people who have been scammed.

Most workers, especially the more senior they are, can be under increased pressure, and try to be more available and urgent than ever before. The increased work-from-home and other remote work trends have created more isolation in workplaces that make people more vulnerable. Unfortunately, cyber-criminals are well aware of these demands and take advantage of them to find their weaknesses. Some of their attempts are obvious and easily evaded, but others can be much more sophisticated and subtle.

YOUR DEFENCE STRATEGY:

Ensure that employees are trained and equipped to protect against cyber threats. This includes:

- Employee training and awareness: Provide regular training and awareness programs to educate employees on cybersecurity threats and how to identify and avoid them.
- Access control: Ensure that access to sensitive data is limited only to authorized personnel and that access is regularly reviewed.
- Employee monitoring: Monitor employee activities and behavior to detect any anomalies or suspicious activity.
- Secure password management: Enforce strong password policies that require regular password changes and the use of complex passwords.

KINETICS OFFERS A "AWARENESS AND PRACTICES– IT PEOPLE SECURITY REVIEW"

03

Platform Resilience

How reliant are the organisation's platforms, systems, and applications are resilient against cyber attacks?

Do your system protections match the policy position you have defined for your business? These involve:

- Implementing security controls: Deploy and configure security controls such as firewalls, intrusion detection/prevention systems, and anti-malware solutions.
- Regular vulnerability scans: Conduct regular vulnerability scans and penetration testing to identify and patch any security vulnerabilities.
- Patch management: Ensure that all software and operating systems are regularly updated with the latest security patches.
- Backup and recovery: Implement a backup and recovery plan to ensure that critical data can be restored in the event of a security incident.

Kinetics Offers a "Platform - IT Cyber - Vulnerability Security Review"

Conclusion

Cyber threats have, unfortunately, become extremely common and disruptive. The new threats bring an unwelcome cost to organisations. No one can promise to eliminate your risk, but it can be reduced by taking all reasonable steps. What is reasonable will differ from one organisation to the next.

Your minimum next steps are to check your cyber insurance and apply the best security you can reasonably afford, which should be more than you had last year. Expect it to be more again next year as new tools and new threats emerge. Consider managed security solutions like KARE Foundation and KARE Security Plus for added reassurance. **https://www.kinetics.co.nz/cybersecurity/**

We don't know where this will end, or if it will end. It is an increasing drain on economies and holds organisations back from investing in tools that make them more productive.

> It is better to invest and reduce the risk of attack than to pay the price later.

How do your policies and posture compare?

Use our checklist that summarises essential cybersecurity policies that modern businesses should consider:

Access Control Policy: Established guidelines for controlling access to sensitive data and systems, including user account management, password policies, and multifactor authentication.

Incident Response Policy: In the event of a cybersecurity incident, there is a documented process including reporting procedures, containment and mitigation, investigation, and recovery.

Data Backup and Recovery Policy: All critical data is backed up regularly, stored securely, and can be recovered quickly in case of data loss or corruption. How far back do your backups go, how frequent are they, and when did you last test them?

Security Awareness Training Policy: Guidelines are in place for educating employees on cybersecurity risks, best practices, and company policies, including periodic training and testing.

Mobile Device Management (MDM) Policy: Confirmed procedures are in place for managing company-owned mobile devices, including device registration, remote wiping, and software updates.

Network Security Policy: Guidelines and expectations are current for securing the company's network infrastructure, including firewall configuration, intrusion detection and prevention systems, and access control list

Third-Party Security Policy: Establish guidelines for managing third-party vendors and partners who have access to company resources, including due diligence, contract requirements, and security assessments.

KINETICS GROUP

making IT work for you

Ph +64 9 379 8200 / 0800 546 384

Email info@kinetics.co.nz