KINETICS GROUP
making IT work for you

CYBER THREAT UPDATE

10 minute read for Directors, CEOs & Operations Managers

Q1 2022

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 Combating 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.

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.

What Attacks are Now Common?

Identity Theft

This is getting enough information to pretend to be you. This is just enough to get control of your accounts or to impersonate you to others. It has been successfully used in New Zealand countless times to redirect payments, sometimes tens of thousands of dollars each time.

Malware

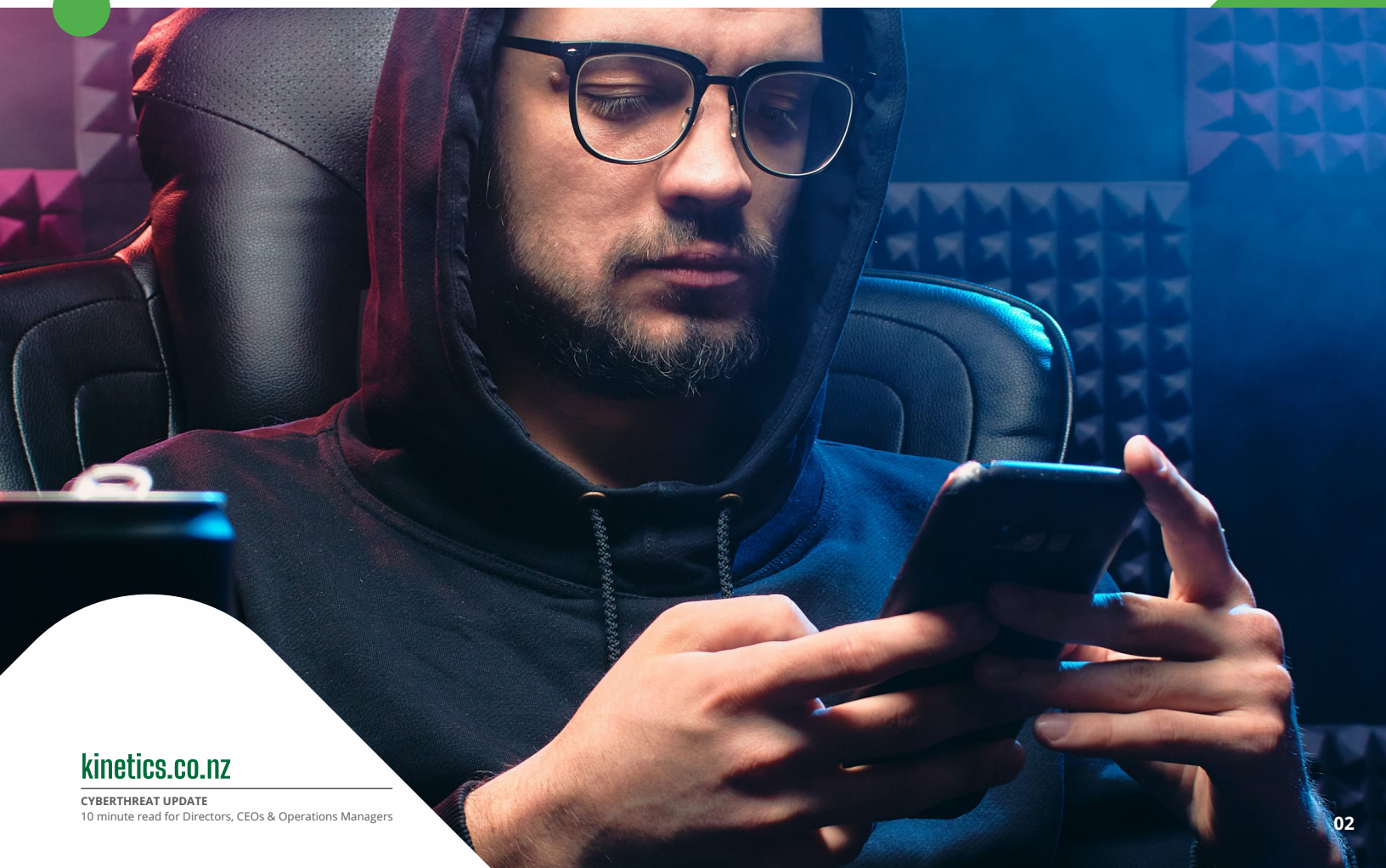
These infect websites you visit or attachments you receive. One click is all it takes to set the attacker loose into your system.

Email Attacks

Phishing and whaling emails trick you into doing something to benefit the cyber-hacker.

Compromised Systems

These include your cloud tools, even the ones you don't know about (a glaring weak point for many organisations). Hackers work hard to trick people to give up their credentials or use brute-force to guess them, then they set up mechanisms to steal data or change it. Commonly used software can have vulnerabilities that are exploited before the industry realises and make defensive patches available.



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?

01 Your biggest risk is people and process

Take a representative group of people in your organisation and mirror the practice of a Health and Safety Committee. This 'e-Security' committee should focus on identifying how someone could accidentally give away confidential data – start by thinking about what data is held, then what is confidential, who are the stakeholders, where it is held, and who has access to it. They should then review things like credential checks. For example, if a client calls up for anything – an account question, how do you verify who they are before providing any confidential info?

02 Protecting against malware and ransomware

These typically get in through software bugs, so the best defence is to ensure everything is patched. Do you get regular reports to prove everything is patched or do you simply trust that it is done? "Everything" can be quite a long list, but you can divide it up by types of device (Servers, laptops etc). Patching isn't just for Microsoft tools, everything that you use can be compromised – Adobe, Google Chrome and so on.

03 We're all aware of antivirus but we need to go further

More intensive end-point protection and personal firewalls are now required, even for computers that are behind your corporate firewall. It is surprisingly common for 'guest' machines to connect to networks. You simply don't know what state they are in and what viruses they may introduce. Look for the new generation of EDR and consider a "zero trust" implementation for sensitive users.

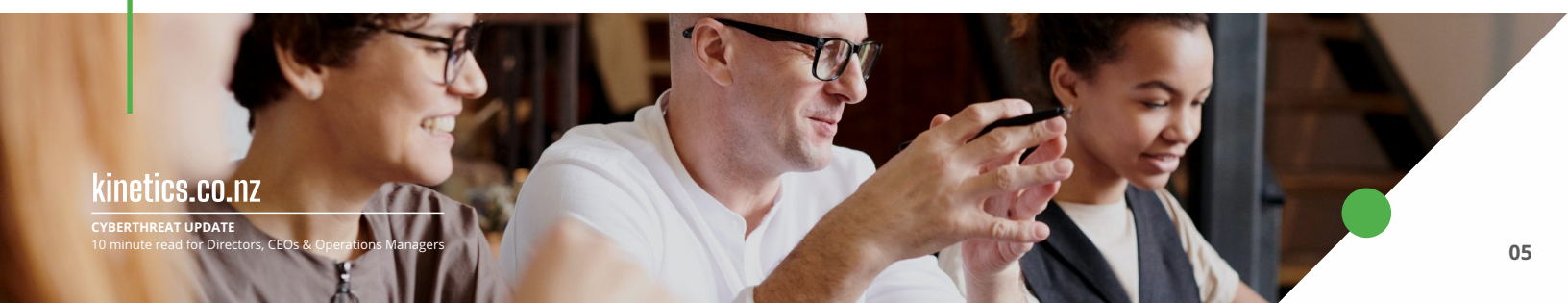
04 Common attack vectors include "phishing". The best defences are:

- Regular phishing tests, to test the awareness of everyone in your organisation.
- Security briefings and awareness training to help everyone stay alert and support each other, both via eLearning and in-person presentations.
- URL scrubbing – testing the URLs that people click on BEFORE the site opens to warn them before they inadvertently browse to a potentially infected website.

05 Beware of the Darkweb

It pays to be aware that some of your data is ALREADY in the darkweb. It will mostly be credential information scavenged from historical hacks of sites like Sony, LinkedIn, Marriott and many others. Occasionally this will surface as an email that states your account name and password for a particular site, along with a threat. For example, "We know what you have been up to, pay a ransom or we will share this publicly". If you recognise the username and password and it's a common one that you use, then this threat can be very compelling.

The best defence is to ensure everyone uses unique passwords for everything, and the best way to do that is with a **secure password vault tool.**



06 Multi-factor authentication (MFA)

MFA isn't infallible, but in conjunction with the items above, it's a very important layer. We regularly see compromise attempts on Office 365. These are being defeated by simple steps like enforcing multi-factor authentication, and where possible, limiting logins to geographical territories that people log in from. For example, unless you have people currently in eastern Europe, you can simply block access from IP addresses from those countries. MFA should be on EVERYTHING, not just Office 365 but also the less common sites your people access.

07 Shadow IT Detection

You will be amazed at some of the tools in use by your people. It is extremely common for people to set up an account on an external website to get a job done. They often just use their email address and make up a password. That means that if they leave your organisation, they can still log in with the email address – the SaaS service they subscribed to doesn't know they've left! Even worse, you don't know how secure the tool is, and often you don't even know about the tool at all!

08 Microsoft have baked some excellent protections into Microsoft 365. Are you using them?

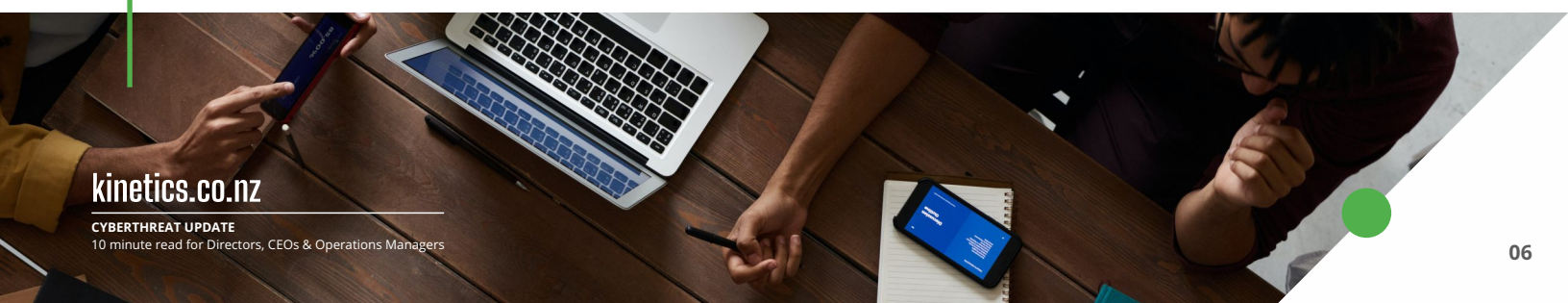
For example, there is 'data leak protection' to help set up a regime where Office 365 can detect confidential data (eg credit card numbers, health records and so on) and then permit or prevent certain actions – for example preventing emailing a spreadsheet with more than say 5 of these records in it, or at least warning you before you do. It can also warn when it detects unusual behaviour such as copying or deleting large numbers of files. The trick is that this needs to be turned on, configured and, above all, maintained and monitored.

09 Consider vulnerability scanning on a regular basis

Vulnerability scans are based around CVE (Common Vulnerability and Exposures) and CVSS (Common Vulnerability Scoring System) and are maintained by First.org, a global forum for response and security teams. CVE's can describe vulnerabilities in software on any connected device, from baby monitors to virtual appliances. CVE's can be found everywhere and anywhere. A deep vulnerability scan is intensive. In addition to scanning devices, it will attempt to use common login and passwords to brute-force hack devices.

10 Review your insurance requirements

Insurers are continually updating their policies for cyber-attacks. It is not uncommon for organisations to discover their policies and practises make their coverage redundant. They are effectively uninsured for a critical and very real business risk.



If you Get Ransomed, should you Pay?

Recently, we asked the question if organisations should pay ransomware demands. There is the balance between desperation and the uneasy knowledge that you might be funding further criminal attacks on the community.

Evidence suggests that, not only do ransom payments fund further attacks, but they also don't necessarily save you further harm. Research tells us that 80% of organisations that pay a ransom are attacked again, often by the same criminals. These ransoms are crippling once, let alone twice. The same research papers go on to report that paying the ransom doesn't necessarily give you back your data. In almost half the ransoms paid, the data came back infected or damaged.

> ***In general, we would discourage paying the ransom because it encourages more of these attacks, and frankly, there is no guarantee whatsoever that you are going to get your data back.***

CHRIS WRAY
Director - FBI

There have been discussions to make paying a ransom illegal in NZ but so far, Minister Faafoi has left that open. I suspect your perspective changes when your business, your job or livelihood is threatened. Not an easy decision and hopefully one you can avoid by being paranoid.

For more information and links back to the source reports, visit www.kinetics.co.nz/yet-another-reason-why-paying-ransomware-demands-hurts

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 our KARE for Security and more advanced KARE for Security S2 plans.
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.

Ph +64 9 379 8200 / 0800 546 384

Email info@kinetics.co.nz