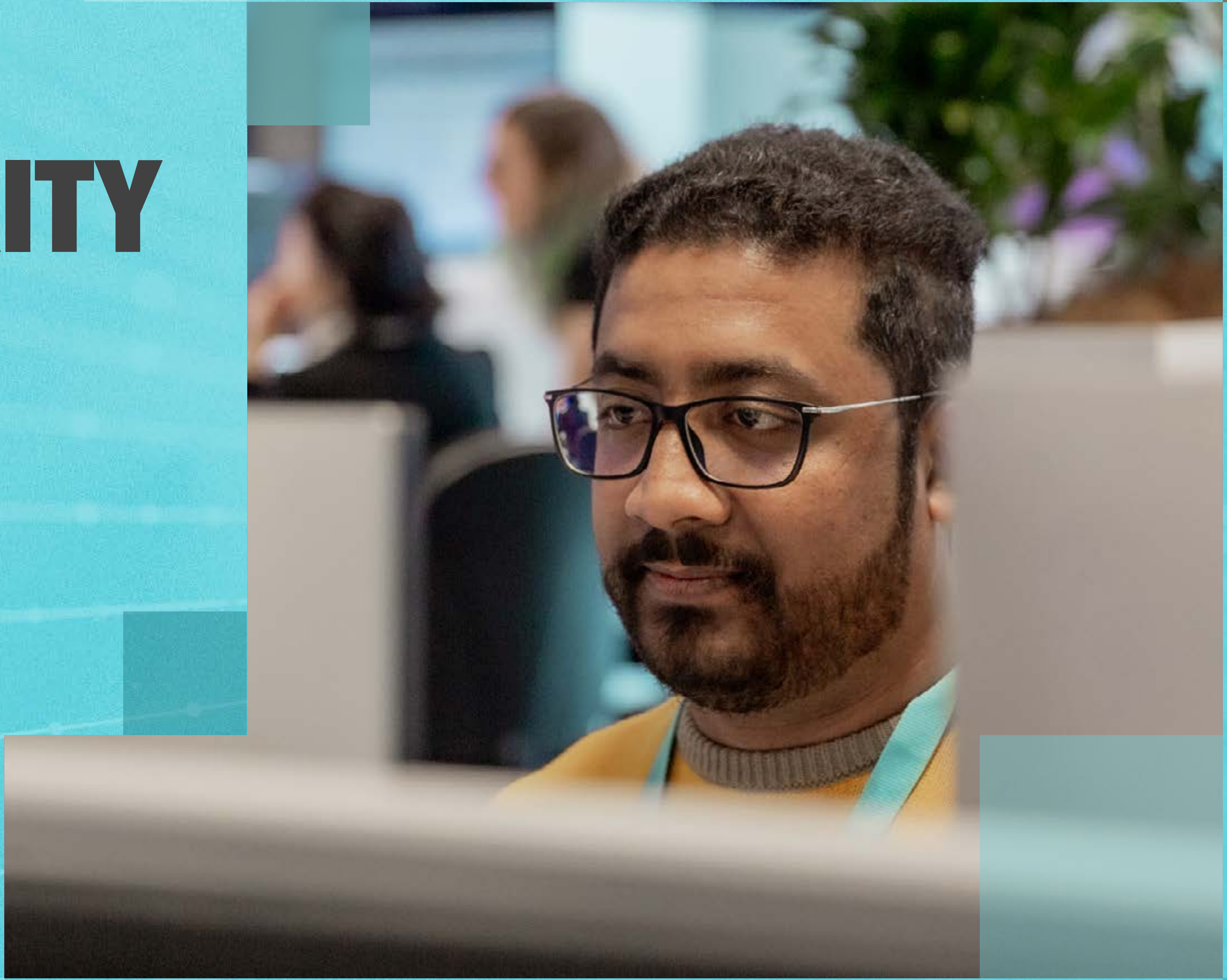
NEW ZEALAND BUSINESS

CYBER SECURITY REPORT 2025

MARCH 2025



kordia®

OUR RESEARCH AT A GLANCE

OF THE BUSINESSES WE SURVEYED:

59%

EXPERIENCED A **CYBER INCIDENT** IN THE PAST 12 MONTHS

43%

OF ALL ATTACKS & INCIDENTS INVOLVED **EMAIL PHISHING**

ALMOST **1/10**

VICTIMS OF CYBERCRIME PAID A **RANSOM DEMAND**

1 IN 6

SAW **PERSONAL INFORMATION** ACCESSED OR STOLEN

28%

RATE AI CYBER-ATTACKS AS A **TOP THREAT**

24%

ARE **NOT CONFIDENT** THEY COULD RECOVER FROM A MAJOR CYBER INCIDENT

NEW ZEALAND BUSINESSES AND THE EVER EVOLVING CYBER THREAT LANDSCAPE

The cyber threat landscape is constantly evolving, and this year technological shifts and geo-political forces saw cybercriminals adapt their strategies and leverage new tools like AI and automation to scale up efforts.

As a result, cyber-attacks across the globe increased by 44% in 2024, according to a report released by Check Point.[2] With financial gain playing a major role in motivating malicious cyber activity, studies from the International Monetary Fund[2] predict that cybercrime will cost the world $23 trillion in 2027, an increase of 175% from 2022.

The threat to New Zealand businesses is apparent. In the third quarter of 2024, the NCSC recorded 98 incidents impacting nationally significant organisations.[3] Data from Payments NZ suggests almost $200 million was lost by New Zealanders to scams in the 12 months to September 2024[4] – a number some industry figures have suggested may be much higher due to under reporting.

One thing is clear – New Zealand businesses must remain vigilant against cyber threats, and prepare adequately to both defend and recover from incoming attacks.

WHO WE SPOKE TO..

Kordia commissioned independent research agency Perceptive to survey 295 business leaders from large New Zealand organisations (50 seats +) via an online survey, between the 1st and 23rd of November 2024.

ROLE TYPE	
GENERAL MANAGER	32%
OWNER / FOUNDER / CEO	18%
COO / OPERATIONS	16%
MANAGING DIRECTOR	10%
DIRECTOR / EXECUTIVE DIRECTOR	8%
SECURITY OR IT LEADER	8%
CFO / FINANCE	7%

REGION	
AUCKLAND	48%
REGIONAL NZ	27%
WELLINGTON	14%
CANTERBURY	11%

NUMBER OF EMPLOYEES	
50-99	31%
100-500	34%
501+	36%

Percentages rounded to nearest whole number.

TRENDS AND THREAT LANDSCAPE

IDENTITY ATTACKS THE LOW HANGING FRUIT

In a landscape dominated by the rise of cloud and SaaS applications, identity is the new perimeter.

According to Microsoft, there are over 600 million daily identity attacks, highlighting the persistent and pervasive nature of these threats.[5] Weak credentials prove to be the low hanging fruit for cybercriminals looking for entry points into critical cloud infrastructure.

While these attacks can be disrupted by using strong authentication methods, threat actors are shifting their focus onto new strategies to successfully compromise targets. Adversary in the Middle (AITM) phishing attacks rose 146% last year, as cybercriminals seek to bypass MFA and steal authentication tokens.[6]

This is set to increase, as AI, automation and phishing kits have made these types of attacks more accessible.

DOUBLE EXTORTION BECOMES THE NORM

While organisations have become better at restoring from backups to circumvent extortion demands, attackers have pivoted to encrypt and compromise backups as well as core systems. Research from Sophos found that 94% of respondents reported attempts by cybercriminals to compromise their backups during an attack.[7] Unsurprisingly, the research also made a link between compromised backups and an increase in ransom payments and recovery costs.

Data theft paired with ransomware has become the norm. In addition to encrypting systems, attackers are also stealing personal information and commercially sensitive material, with a threat to release the information on the dark web. This creates a public dimension to the attack, adding reputation damage and privacy breaches to the list of impacts.

AI: HYPE CYCLE ENTERS THE NEXT PHASE

AI is reshaping cyber security, but the early hype is giving way to more grounded expectations. While it has proven valuable in improving threat detection, streamlining security operations, and easing security analyst's workload, it's not a silver bullet.

Cybercriminals are also adopting AI, using it to develop more sophisticated attacks, from deepfake phishing scams to AI-driven malware. A study published in Harvard Business Review found the phishing process can be automated using LLMs, which reduces the costs of phishing attacks by more than 95% while achieving equal or greater success rates.[8] As a result, security teams must stay ahead by applying AI in practical, well-tested ways.

The next phase of AI in cyber security will be less about bold claims and more about delivering real, measurable outcomes. Organisations that take a strategic approach focusing on proven use cases rather than trends will see the biggest gains in resilience and security effectiveness.

TRENDS AND THREAT LANDSCAPE

CYBER LEGISLATION RAMPS UP

Cyber legislation has progressed globally, but perhaps most pertinent to New Zealand is the introduction of new laws and regulations in our neighbouring country Australia.

The Albanese government recently brought into effect new measures to counteract the effects of cybercrime, particularly against critical infrastructure, to bolster the nation's resilience against cyber-attacks. These include new standards for Internet of Things (IOT) devices, mandatory reporting on ransom payments, setting up a new Incident Review Board to review and report on major cyber incidents and increasing the government's powers to intervene in major crisis level attacks on nationally significant organisations.

As New Zealand looks to review its own cyber strategy, no doubt lawmakers will be taking note of the effectiveness of Australia's strategy.

STATE-ALIGNED CYBER CRIME

In the past there was a much clearer delineation between cyberespionage and profit driven attacks. However in the past 12 months the lines drawn between the two have eroded, with state-sponsored threat actors collaborating more closely with cybercriminals than ever before.

Ransomware is providing a source of income for cash-strapped governments, especially those suffering from sanctions and the cost of military conflicts. In other cases, malware is being deployed to cover evidence of spying, particularly against critical infrastructure providers. Acting as a virtual smoke screen to distract investigators, ransomware provides both a cover and a means to destroy evidence of data theft.

As the lines between cybercrime and state-sponsored attacks continue to blur, the threat landscape becomes increasingly fluid, particularly for nationally sensitive industries and critical infrastructure providers – and the motivations behind attacks becomes more opaque.

> “
> ***Worldwide, new legislation is driving intelligence gathering and government empowerment, best practice is becoming regulation, and professional licensing is emerging. Business leaders should leverage cyber experts to lift their standards to international best practice, or risk being left behind.***
>
> **PATRICK SHARP**
> GENERAL MANAGER | AURA INFORMATION SECURITY

CYBER-ATTACKS & INCIDENTS

Around two thirds of respondents told us their businesses suffered a cyber-attack or incident in the past 12 months. We asked those businesses to give us more information about the attack or incident and the impacts suffered as a result.

PHISHING REMAINS THE TOP THREAT

Email phishing continues to be the most frequently experienced type of cyber-attack by New Zealand businesses, with nearly half of respondents stating phishing was utilised to target their business. We expect email will continue to be the main avenue of compromise going forward.

SOCIAL MEDIA – HACKERS PLAYGROUND

1 in 6 businesses impacted by cyber-attacks pointed to business social media accounts as the root cause. As Meta relaxes its fact checking policies, we may see an influx of scams and deepfakes flooding popular social media platforms as scammers take advantage of less scrutiny over content.

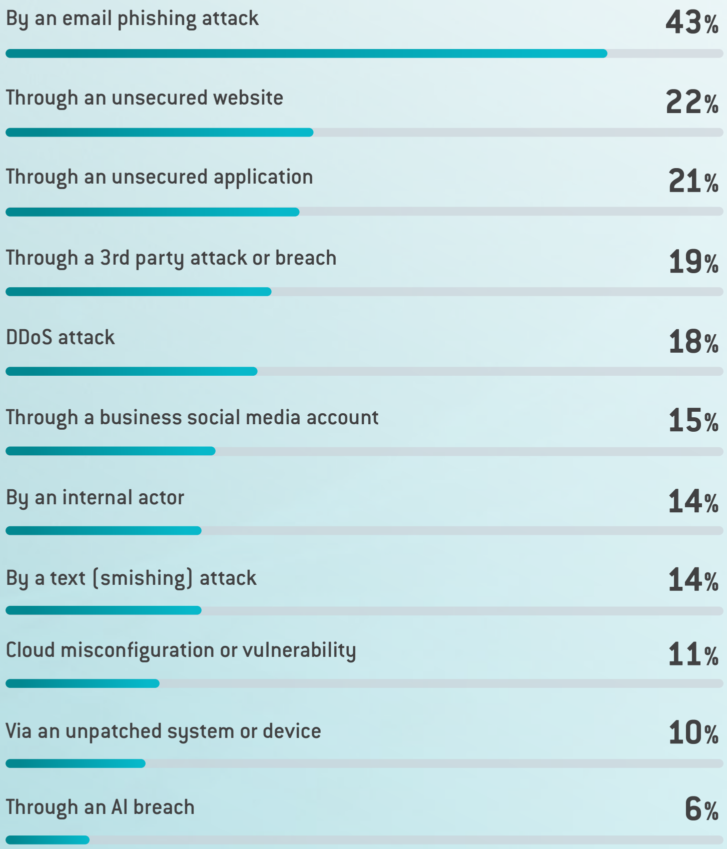
DDOS DISTRACTIONS

DDoS attacks impacted almost 1 in 5 respondents. While this type of attack may not lead to a breach in itself, malicious actors have been known to deploy DDoS attacks to distract targets and mask other activity.

AI BREACHES – THE ONE TO WATCH

While only 6% of respondents pointed to an AI breach as affecting their business, it is interesting to see that AI is having an impact on security posture for some businesses, despite still being relatively new in terms of adoption.

HOW WAS YOUR BUSINESS COMPROMISED IN THE CYBER-ATTACK / INCIDENTS?



Businesses were asked to select all responses that applied.

CONSEQUENCES & IMPACT

TWO THIRDS EXPERIENCE IMPACTS

The impacts of cyber incidents were varied. From interrupted supply chains to fines and insurance claims, around two thirds of those who experienced a cyber incident reported some sort of impact on their business.

EYES ON THE PRIZE

Personal information, a lucrative target for cybercriminals, was high on the list of impacts, with 1 in 6 respondents reporting cyber-attacks involving to stolen personally identifiable information (PII), which could result in a breach of the Privacy Act.

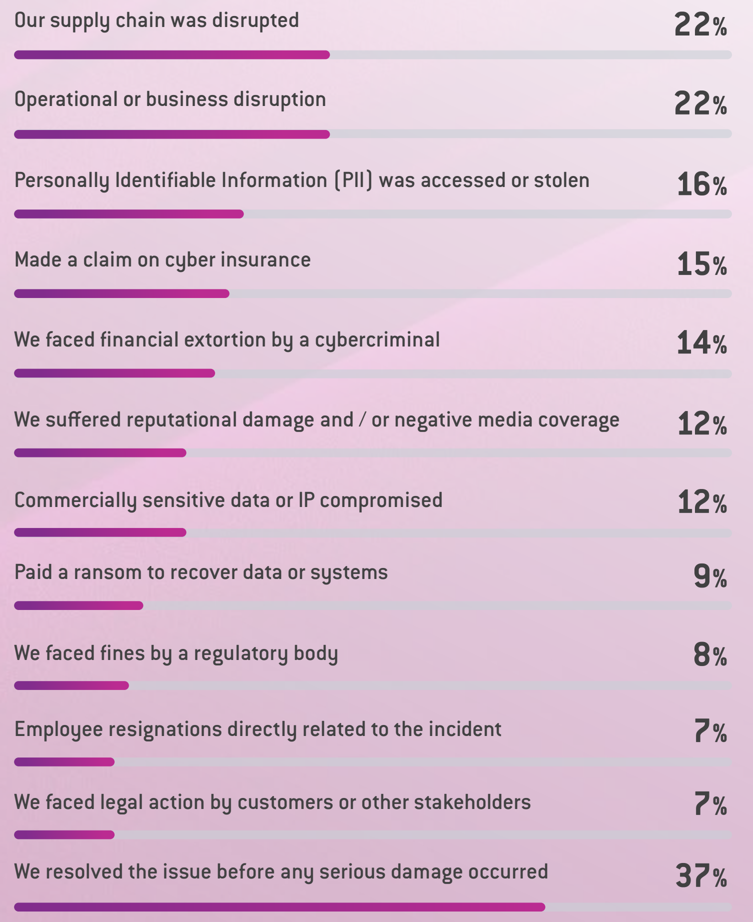
PAYMENTS TO CYBERCRIMINALS

Almost 1 in 10 impacted by a cyber incident indicated that they paid a ransom or extortion demand to a cybercriminal – a small, but troubling statistic.

CLOUD A LUCRATIVE TARGET

Our survey found a strong association between attacks involving the cloud and extortion – around 40% of businesses who experienced a cloud breach or misconfiguration in the past 12 months also faced financial extortion by a cybercriminal.

WHAT WAS THE IMPACT OF THE CYBER-ATTACK OR BREACH ON YOUR BUSINESS?



Businesses were asked to select all responses that applied.

LESSONS LEARNED FROM CYBER INCIDENTS

We asked New Zealand business leaders to tell us in their own words, based on learnings from your experiences during the cyber incident, what would you have done differently?

The **most common** theme that emerged from the survey respondents was to invest in better security systems and policies.

> *Should have invested more in cyber security.*

> *Been with a more secure platform to hold all of our data and tried to make transferring data easier.*

The **second** most cited learning was improving and implementing employee training.

> *More education company wide to all our employees.*

> *Be more educated and educate staff better on these things and make everyone aware what could happen.*

The **third** most cited learning was around better implementation of basic security controls, such as patching and monitoring.

> *Keep the operating system, applications, etc. updated in a timely manner to fix known vulnerabilities and prevent hackers from exploiting these vulnerabilities to invade the system.*

Some respondents reflected on a lack of preparation by the business to effectively deal with a cyber incident.

> *We had not updated our business continuity plan when an event like that occurs. Due to this we were inexperienced which meant we had a delayed response. Going forward we've made it our plan to update this plan and regularly refresh this.*

WHAT KEEPS BUSINESS LEADERS AWAKE AT NIGHT?

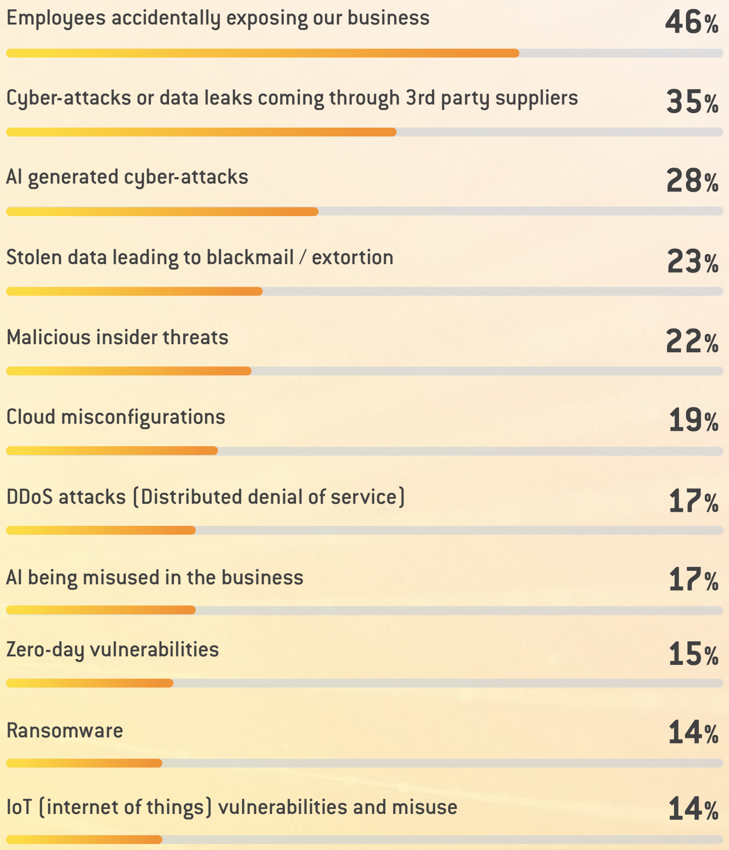
From 2023 to 2024, perceptions of risks did not shift significantly amongst New Zealand businesses we surveyed.

Human error and third-party attacks, which are both difficult to exert control over, remain high on the list of concerns.

The most obvious exception to this is the introduction of AI generated cyber-attacks, a new response added to the survey. 28% of business leaders said AI attacks are a top concern.

> ***Most companies outsource to third-parties and employ the use of hundreds and thousands of applications, without ensuring they comply with security. This increases their threat surface, hence becoming an easy target to exploit. A risk-based approach is required to successfully manage third-party risks.***
>
> **HORATIU PETRESCU**
> **SENIOR ADVISORY CONSULTANT**

WHAT DO YOU PERCEIVE AS THE BIGGEST THREAT TO YOUR BUSINESS'S CYBER SECURITY POSTURE?



Respondents were asked to pick their top 3.

PRIORITIES & CHALLENGES

Interestingly, perspectives on top challenges to improving cyber security varies depending on role. Security and IT leaders, such as CIOs, CISOs and IT Managers cited a lack of understanding about cyber risks and security priorities as the top challenge to improving cyber security (40%).

In comparison, Managers and Directors tended to put more emphasis on security awareness amongst employees and managing third-party risk.

> *We often see problems arise with security posture when managers and directors gravitate towards the easiest answers to address cyber security, rather than tackling the complexity of delving into a risk assessment.*
>
> **ALASTAIR MILLER**
> **PRINCIPAL ADVISORY CONSULTANT**

> *If more awareness or training was the answer to strengthening security, all companies would be fortresses. Managing third-party and human risks is more complex than this, and requires a holistic approach to security governance – starting at the board and exec level.*
>
> **HORATIU PETRESCU**
> **SENIOR ADVISORY CONSULTANT**

PERCEPTION OF CYBER SECURITY CHALLENGES BY ROLE

WE ASKED BUSINESSES TO TELL US "WHAT ARE THE TOP CHALLENGES TO IMPROVING CYBER SECURITY IN THE BUSINESS YOU WORK IN?"

OWNER / FOUNDER / CEO (N=52)	GENERAL MANAGER (N=95)	DIRECTOR / EXECUTIVE DIRECTOR (N=25)	MANAGING DIRECTOR (N=29)	IT OPERATIONAL (CIO,CDO, CTO, CISO, ITSM, ETC) (N=25)
1. Difficulty in recruiting skilled people to effectively manage cyber security	1. Lack of security awareness or good behaviours amongst employees	1. Managing third-party cyber risk	1. Trying to keep cyber security in step with digital transformation	1. Lack of understanding about our cyber risks and security priorities
2. Managing third-party cyber risk	2. Managing third-party cyber risk	2. Lack of security awareness or good behaviours amongst employees	2. Lack of understanding about our cyber risks and security priorities	2. Lack of security awareness or good behaviours amongst employees
3. Lack of prioritisation and focus from the board or Management	3. Ageing technology that can't be updated to meet current cyber security standards	3. Trying to keep cyber security in step with digital transformation	3. Lack of security awareness or good behaviours amongst employees	3. Burnout from security / IT teams due to high workloads
4. Trying to keep cyber security in step with digital transformation	4. Trying to keep cyber security in step with digital transformation	4. Difficulty in recruiting skilled people to effectively manage cyber security	4. Lack of cyber security strategy	4. Lack of budget
5. Ageing technology that can't be updated to meet current cyber security standards	5. Difficulty in recruiting skilled people to effectively manage cyber security	5. Lack of understanding about our cyber risks and security priorities	5. Lack of budget	5. Managing third-party cyber risk

SECURITY BASICS

OF THE BUSINESSES WE SURVEYED:

30%

HAVE NO SINGLE SOURCE OF **IDENTITY MANAGEMENT**

36%

NEGLECTED **PENETRATION TESTING** IN THE PAST 12 MONTHS

AROUND **1/4**

DO NOT HAVE A COMPREHENSIVE **ASSET DATABASE**

1 IN 5

DO NOT **MONITOR OR LOG** ACTIVITY IN THEIR NETWORK

LESS THAN **½**

CONDUCT A **RISK ASSESSMENT** WHEN ONBOARDING NEW TECHNOLOGIES

1/4

LACK EMPLOYEE CYBER SECURITY **AWARENESS TRAINING**

← →

RESILIENCE & RECOVERY

A CASE OF WHEN, NOT IF

With nearly two thirds of businesses saying they suffered a cyber-attack in the past 12 months, having a cyber incident response plan is imperative. While the vast majority of businesses have a plan, less than half have practiced it to verify it is fit for purpose.

- 1 in 4 businesses say they are not confident that their business could fully recover from a major cyber incident.
- 86% of businesses say they have an incident response plan, but only around half have practiced that plan.
- 1 in 4 businesses do not have a plan in place to communicate with customers and stakeholders in the event of a cyber security incident.

> *Successfully recovering from a cyber-attack doesn't happen by accident. You need to be prepared, you need robust policies and plans, and you need to simulate how you'd respond as an organisation if the worst was to happen.*

CONAN BRADLEY
INCIDENT RESPONSE AND DIGITAL FORENSICS PRACTICE LEAD

HEALTHCARE CYBER ATTACK
NEVADA HOSPITAL REPORT
74% of nation's hospitals impacted
Workarounds only 11% effective
Safety net providers could close
Pharmacy network & payment restored
FILE
FOX 5
73° 3:01

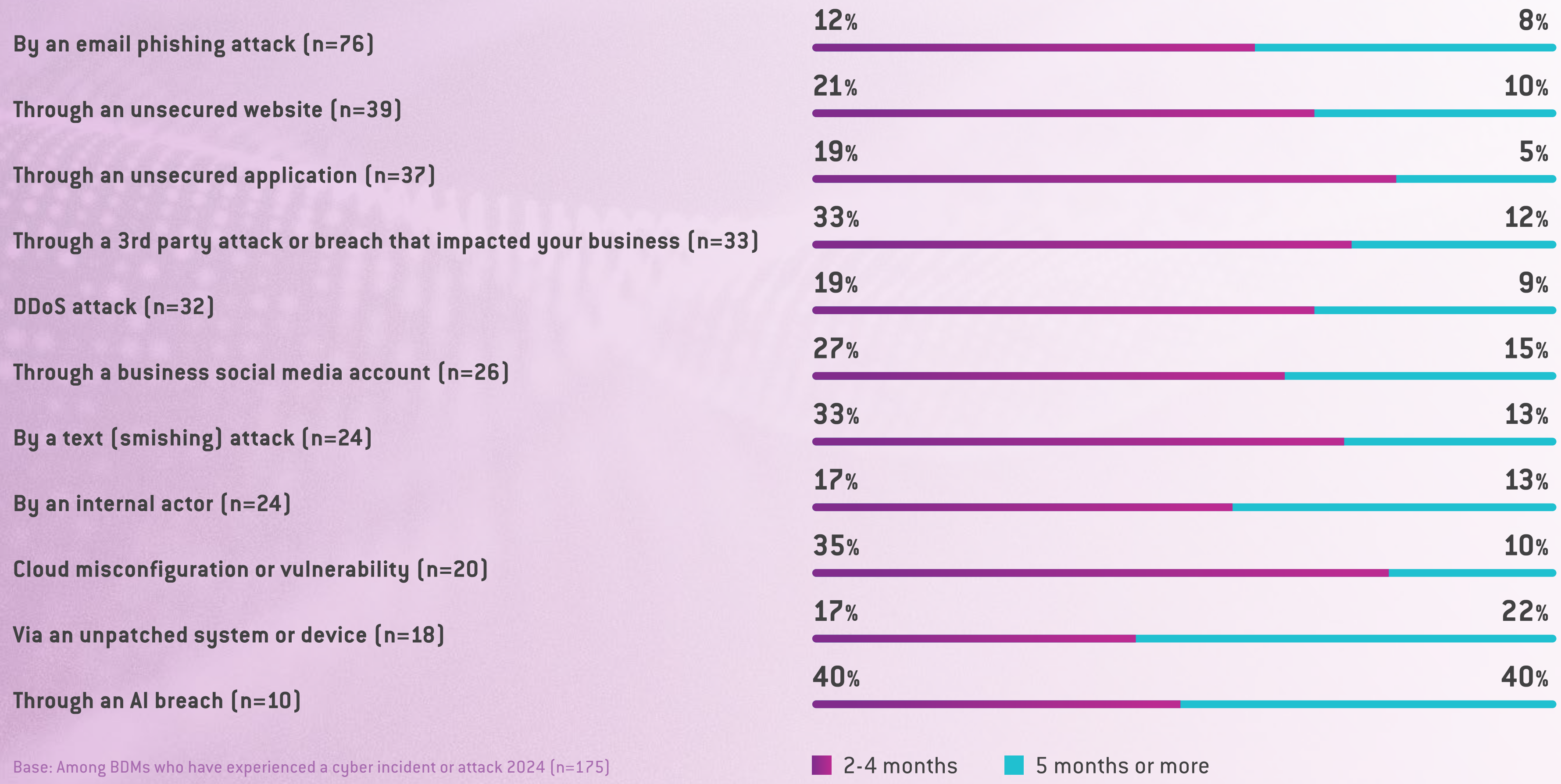
UNITEDHEALTH
THE COST OF A BREACH

In February 2024, UnitedHealth Group's subsidiary, Change Healthcare, experienced a ransomware attack, severely disrupting healthcare billing systems across the United States. Recovery was extensive and complex, and it took months for full restoration. UnitedHealth's Chief Information Security Officer later revealed that the company had to "start over" with its computer systems, replacing routers, switches, and infrastructure to ensure security. The total cost of the incident is estimated to be in excess of $2.3billion USD.

RESILIENCE & RECOVERY

CYBER-ATTACKS THAT TOOK MORE THAN 2 MONTHS TO RESOLVE

APPROXIMATELY HOW LONG DID IT TAKE FOR YOUR BUSINESS TO RESOLVE THE CYBER INCIDENT?



Base: Among BDMs who have experienced a cyber incident or attack 2024 (n=175)

AI – DOUBLE EDGED SWORD

From an attacker's perspective, AI has proven to be an attractive tool, helping hackers craft personalised and realistic phishing emails through to highly adaptive malware that can learn and evade detection systems. And we're only at the beginning. Check Point predicts that in 2025 we will start seeing the next generation of phishing attacks, which will use AI to learn from real-time data, and adapt to changing security measures, making detection even more challenging.[9]

AI has its merits when it comes to effective cyber defence. Automation and AI learning tools woven into security software can be trained to handle manual tasks, alleviating analysts from time consuming tasks and freeing human experts to focus on more critical areas of security.

With AI speculated to be behind increases of general attack volumes, this presents a scalable way of monitoring environments in real time.

However, it's essential that business leaders are aware of AI's limitations, and ensure human expertise and oversight is in place across AI cyber security tools to ensure false positives and other errors are sense checked. Overreliance on AI may further expose the business, if tools are not trained, monitored or tuned correctly. Similarly, there is an expectation by some businesses to leverage AI, with a WorkDay report finding 73% of business leaders said they felt pressure to increase AI adoption. Rushing any AI deployment could result in adverse outcomes, if the right guardrails for proper usage aren't in place.[10]

> ***Defensive AI will always lag behind offensive AI, so it is key not to bank on it alone to solve all your problems.***
>
> **ALASTAIR MILLER**
> **PRINCIPAL ADVISORY CONSULTANT**

AI & CYBER SECURITY

6%

OF CYBER INCIDENTS INVOLVED **AI BREACHES**

28%

SAY AI GENERATED CYBER-ATTACKS ARE THE **TOP THREAT** TO THEIR BUSINESS

1 IN 6

VIEW **IMPROPER USE** OF AI AS A TOP CHALLENGE TO **IMPROVING** CYBER SECURITY

ALMOST **½**

SAY THEY **LACK POLICIES OR GUIDELINES** TO PROTECT THEIR BUSINESS FROM DATA BREACHES

CYBERCRIME AND NEW ZEALAND BUSINESSES

Our survey reveals that funds from New Zealand are flowing to cybercriminals, as some businesses struggle to respond to and recover from incoming attacks.

While the number of survey respondents who admitted to paying a ransom is small, it does highlight the difficult position facing businesses whose operations are crippled by a cyber incident.

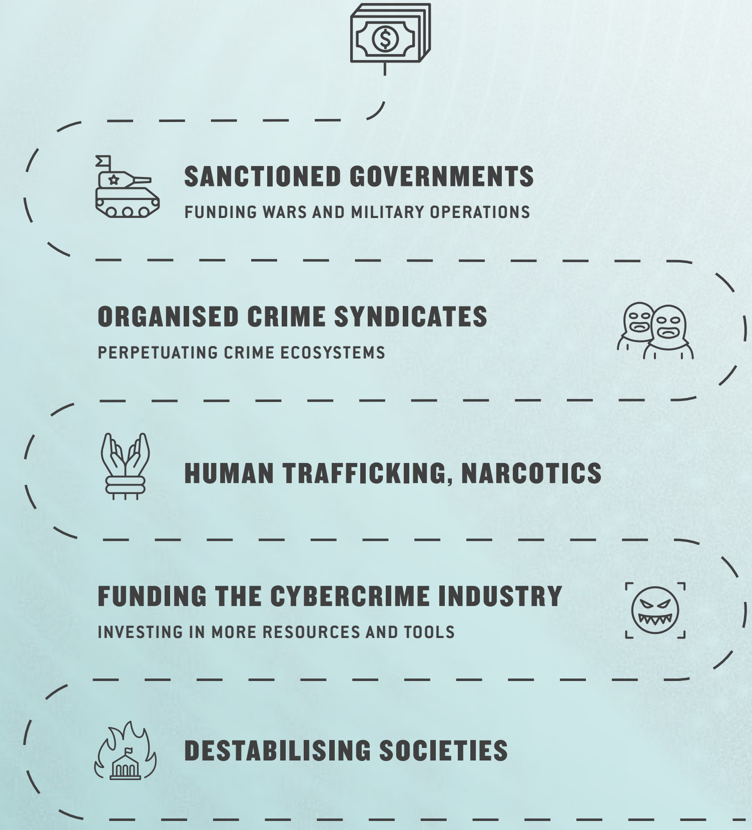
Businesses that have robust response and recovery plans in place have the best chance of overcoming a cyber-attack without having to pay any extortion demands, however all businesses should discuss how they will handle such threats as part of their incident response plan.

A board discussion in a stress-free environment is the best time to consider options.

> ***I should have contacted my company IT engineer for proper rectification the moment we discovered the attack but we were carried away by extortion from the swindlers.***
>
> **SURVEY RESPONDENT**

WHERE DO THE PROCEEDS OF CYBERCRIME GO?

Paying a cybercriminal may be a last resort for a business severely impacted by a cyber-attack, but its important to note that any money that flows through to malicious hackers fuels a range of illegal and nefarious activity.



SANCTIONED GOVERNMENTS
FUNDING WARS AND MILITARY OPERATIONS

ORGANISED CRIME SYNDICATES
PERPETUATING CRIME ECOSYSTEMS

HUMAN TRAFFICKING, NARCOTICS

FUNDING THE CYBERCRIME INDUSTRY
INVESTING IN MORE RESOURCES AND TOOLS

DESTABILISING SOCIETIES

CYBERCRIME & NEW ZEALAND BUSINESSES

OF THE BUSINESSES WE SURVEYED WHO SUFFERED A CYBER-ATTACK OR INCIDENT IN THE PAST 12 MONTHS:

AROUND **1 IN 6**

CYBER INCIDENTS RESULTED IN **FINANCIAL EXTORTION**

16%

OF BREACHES INVOLVED THE **THEFT OF PERSONAL INFORMATION**

1 IN 6

SAY TRYING TO **MANAGE INCREASING VOLUMES OF ATTACKS** IS A TOP CHALLENGE

AROUND **1 IN 10**

ADMITTED TO PAYING A **RANSOM OR PAYMENT DEMAND**

22%

OF CYBER INCIDENTS LED TO **OPERATIONAL DISRUPTION**

12%

OF ATTACKS SAW **COMMERCIALLY SENSITIVE INFORMATION** OR IP COMPROMISED

← →

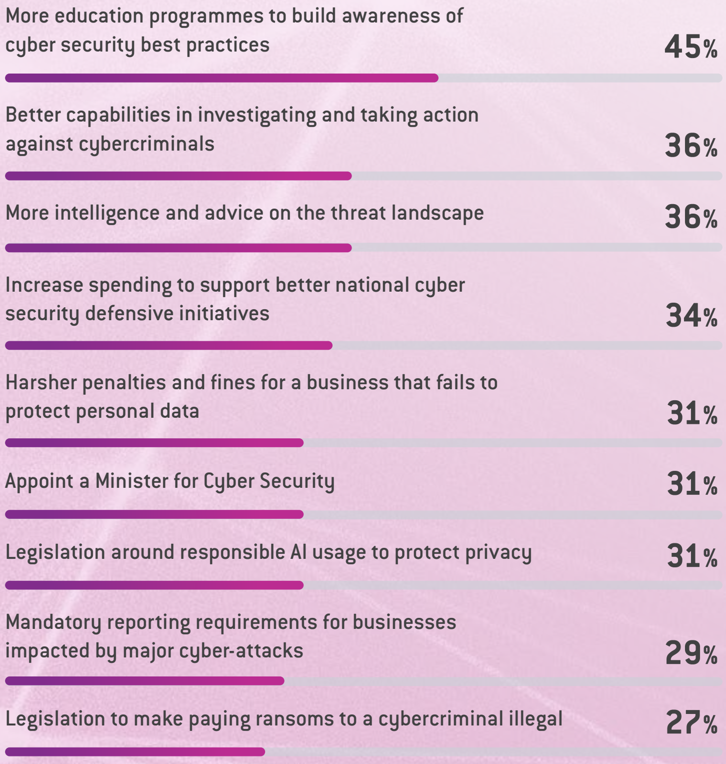
GOVERNANCE & LEGISLATION

The past 12 months have seen increased activity by legislators, looking to bolster resilience against cyber-attacks, particularly against critical infrastructure.

In addition to the earlier mentioned Australian laws, the European Union and Singapore have also brought new cyber legislation into force in the past 12 months. In the US, new regulations from the Securities and Exchange Commission taking effect from December 2023 required publicly traded companies to disclose new details about cyber-attacks and cyber security oversight from the board.

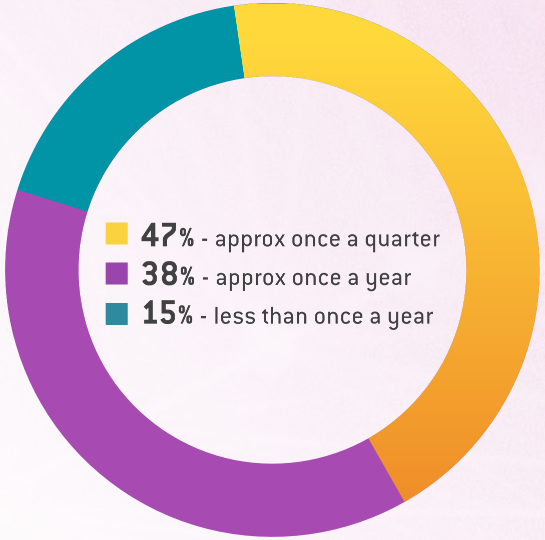
While New Zealand regulations don't currently encompass that degree of governance, based on global trends directors of New Zealand companies should be engaging in cyber matters and ensuring that cyber security is treated as an important risk area for the business.

WHAT WOULD YOU LIKE THE NEW ZEALAND GOVERNMENT TO DO TO SUPPORT CYBER SECURITY FOR BUSINESSES?

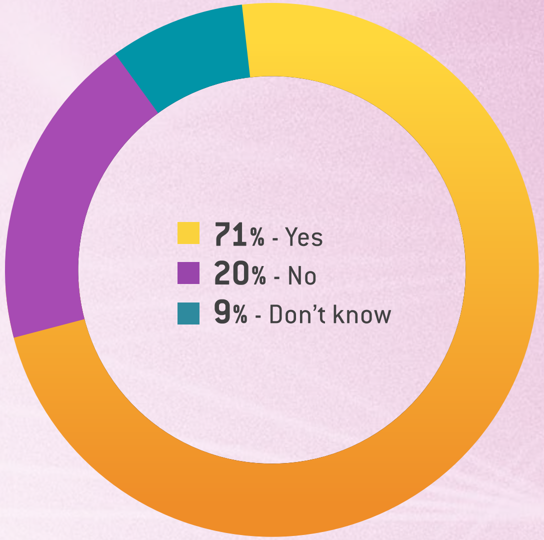


CYBER SECURITY & THE BOARD

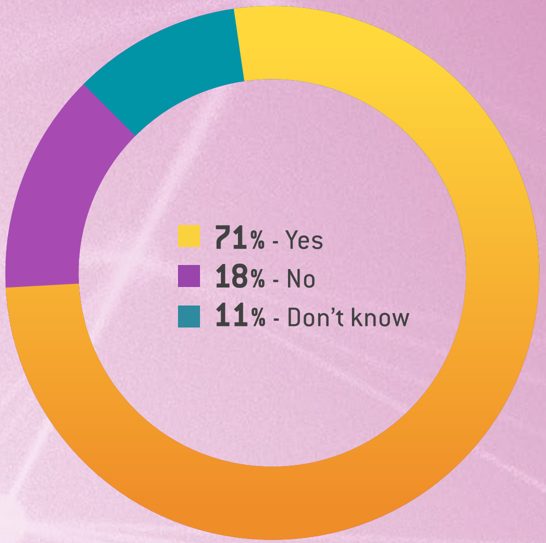
HOW OFTEN DO YOU PERFORM AN ASSESSMENT OF THE CYBER RISKS FACING YOUR ORGANISATION?



IS CYBER SECURITY PERCEIVED AS AN IMPORTANT RISK AREA FOR YOUR BUSINESS BY YOUR BOARD OF DIRECTORS?



DOES THE PERSON RESPONSIBLE FOR CYBER SECURITY PROVIDE RISK BASED CYBER SECURITY REPORTING TO YOUR BOARD OF DIRECTORS?



FOCUS AREAS FOR BUSINESS IN 2025

RISK ASSESS AI AND OTHER EMERGING TECH

Any major IT breakthrough presents both risk and opportunity for cyber security. The democratisation of generative AI tools is a classic example.

Whether your organisation intentionally uses AI tools in your corporate environment or not, as vendors increasingly incorporate AI technologies into enterprise software and move towards an "opt out" model, even using everyday platforms such as Microsoft Office can mean you're exposing your data to AI analysis.

Similarly, shadow AI, when employees use AI tools on their own volition, can also put your business at risk if proper data management and privacy guardrails are not in place.

Businesses need to assess what data or systems may be impacted by AI usage, determine whether the benefits present an acceptable level of risk, and be well across any AI upgrades in commonly used tools.

A similar risk assessment should be done against any new technology, to ensure your organisation is well versed on any impacts to your security posture.

FACTOR THIRD PARTIES INTO BUSINESS CONTINUITY PLANS

Third-party cyber threats are intensifying, as more and more businesses adopt SaaS platforms and cloud-based operations. While you may outsource many functions to cloud providers, you can't outsource accountability when it comes to ensuring your business can recover should these platforms be impacted by a cyber incident.

A great example, while not specifically caused by a cyber-attack, was the recent Crowdstrike issue, that caused entire systems outages for thousands of businesses and critical infrastructure providers last year.

All organisations should have a robust business continuity and cyber response plan that can be activated should any major provider you rely upon suffer from a cyber-attack or incident.

Understanding what data and systems your SaaS and cloud partners provide or access, and having workarounds in place to continue operating even if that platform suffers an outage, is the key to building better resiliency around third-party attacks.

LET RISK GUIDE YOUR SECURITY INVESTMENTS

Our research revealed many businesses lack understanding about security risks and priorities. This is one of the biggest challenges to improving cyber security, closely followed by difficulties keeping security in step with digital transformation.

We often see an organisation's entire risk profile shift simply by adopting a new cloud platform, where a lack of skills or bandwidth, and even just the rate of change, results in unexpected vulnerabilities. The security market is now flooded with products, most of which claim to fix all of your security issues, however they should be selected and implemented based on how effectively they can mitigate your core risks.

Security investment should be targeted where it will enable the business to run effectively, limited to where is it is cost effective, and implemented with process and metrics.

Understand the threats and how they could impact your business, in order to prioritise investment where it will be effective.

FOCUS AREAS FOR BUSINESS IN 2025

TREAT IDENTITY AS A SECURITY FOUNDATION

The vast majority of security incidents involve an adversary accessing a legitimate account, where credentials have been exposed through a data breach or phishing attack. There is already mounting research that indicates the increasing incidence and effectiveness of AI based deepfakes and phishing, so we expect identity attacks will continue to intensify.

Given the ongoing move towards the cloud, the most effective set of security controls that your organisation can implement include reviewing your identity and access management processes and systems, implementing single sign on, segregating admin functions, enforcing phishing resistant MFA, managing access to key resources, making admins use just-in-time access, and implementing processes for tight credential management.

Where possible, companies should prefer the Zero Trust principle of “Never Trust, Always Verify” and require every user access request to be explicitly authenticated and given least privilege.

QUANTUM – THE NEXT WAVE OF ENCRYPTION

Increasingly advanced quantum computers are being developed, with the ability to break through the encryption currently used to protect electronic communications. IBM and Google have plans to achieve the technical advancements that would make this possible by 2030. While this may seem like tomorrow’s problem, some researchers and experts are already assessing what impacts this step change in technology might have on current cyber security and data protection measures.

New Zealand organisations, particularly those in industries such as critical infrastructure, finance and health should be formulating a risk-based approach to prepare for the advent of quantum.

Businesses in these critical sectors could look at how they might approach the transition to quantum algorithms for encryption, including how they might manage older data and systems that will be vulnerable should quantum technology be leveraged by a malicious actor.

Our advice would be to table discussions at a board level, with a 3-year outlook on how your business might prepare ahead of any major developments in quantum computing in the next decade.

> “ ***Translating complex cyber risk into cost-effective action requires businesses to maintain a common language that connects the board and operational teams.***
>
> **PATRICK SHARP**
> **GENERAL MANAGER | AURA INFORMATION SECURITY**

RELATED RESOURCES

MANAGING THIRD-PARTY CYBER RISK

Discover the five areas you need to focus on when assessing third-party risk.

AI POLICY CHECKLIST

An AI Usage Policy can help safeguard your business from data privacy risks. Get started with our guide.

CYBER REPORT 2024

Compare our latest findings with research conducted with New Zealand businesses in 2024.

EXECUTIVE INCIDENT RESPONSE CHECKLIST

This checklist can be used as a tool to help your organisation refine its incident response plan.

ZERO TRUST GUIDE

Discover what Zero Trust is and what steps can be helpful to follow to implement this method as part of your cloud migration.

CYBER SMART HUB

Visit our Cyber Smart Hub for tips and resources to help your business stay protected.

REFERENCES

1. Check Point Software's 2025 Security Report Finds Alarming 44% Increase in Cyber-Attacks Amid Maturing Cyber Threat Ecosystem - Check Point Software 2. Key Cyber Security Statistics for 2025 3. Quarter Three Cyber Security Insights 2024 | CERT NZ 4. MBIE is helping New Zealanders spot scams through Fraud Awareness Week | Ministry of Business, Innovation & Employment 5. Microsoft Digital Defense Report: 600 million cyberattacks per day around the globe - CEE Multi-Country News Center 6. 'Adversary in the middle attacks' are becoming hackers' go-to method to bypass MFA | ITPro 7. The impact of compromised backups on ransomware outcomes – Sophos News 8. AI Will Increase the Quantity — and Quality — of Phishing Scams 9. 2025 Cyber Security Predictions – The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation - Check Point Blog 10. Workday Research: 'AI IQ' Study Reveals Artificial Intelligence Adoption Barriers for Business Leaders | Workday UK

kordia®

KORDIA.CO.NZ

WINNER
iSANZ Best Security
Company 2024