NEW ZEALAND BUSINESS

CYBER SECURITY REPORT 2024

MARCH 2024

kordia®

GLOBAL BECOMES LOCAL – INTENSIFYING THREATS AGAINST AOTEAROA NEW ZEALAND

In a world increasingly dependent on digital and cloud first solutions, our geographical isolation offers no shelter against large scale cyber-attacks and breaches. Online operations link Kiwi businesses, their data, and infrastructure to the world wide web - as well as malicious cyber activity.

2023 saw global cyber threats reach our shores on a new scale. The hack on Australian financial services company Latitude saw personal data belonging to 1 million Kiwis (or 20% of the population) compromised in the largest ever privacy breach our country has ever seen.

More complex to quantify is the damage being caused by critical vulnerabilities and through third-parties. As cybercriminal gangs exploit security loopholes in widely used cloud platforms and enterprise software, Kiwi companies are being caught up in the fray – both directly and indirectly.

A Ministry for Business, Innovation & Employment report recorded almost $200million NZD lost to scams in the year through to September 2023. For the first time ever, the GCSB's National Cyber Security Centre's Threat Report recorded a higher proportion of financially motivated activity compared to that linked to state-sponsored cyber actors. The impetuous is clear - unscrupulous threat actors have discovered there is money to be made by targeting Kiwi organisations.

Our annual survey attempts to paint a picture of how businesses are managing the influx of global cyber-attacks and incidents, and the impact these are having on organisations. This report frames up insights on attacks and incidents from some of New Zealand's largest enterprises against commentary and analysis from Kordia's information security experts and consultants, to give a clear snapshot of the business of cyber security in our country.

WHO WE SPOKE TO..

Kordia commissioned independent marketing intelligence agency Perceptive to survey 219 business leaders from NZ organisations via an online survey, between 2 October and 26 November 2023.

ROLE TYPE	
OWNER / FOUNDER	33%
GENERAL MANAGER	20%
DIRECTOR / EXECUTIVE	16%
MANAGING DIRECTOR	14%
CIO / CDO / CTO / IT	10%
CISO / CYBER SECURITY	4%
COO / OPERATIONS	2%
CFO / FINANCE	1%

REGION	
AUCKLAND	60%
REGIONAL NZ	21%
WELLINGTON	10%
CANTERBURY	8%

NUMBER OF EMPLOYEES	
100-200	17%
201-500	32%
500+	51%

GLOBAL THREAT LANDSCAPE

ESCALATING IMPACTS

Gone are the days of cyber-attacks just impacting IT systems. Today, serious incidents spill across into the physical world, with hackers targeting operational downtime to cripple and extort businesses.

According to the IBM[1] Cost of A Databreach Report, the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over three years. More concerning is that the majority (57%) of respondents indicated data breaches led to an increase in the pricing of their business offerings, passing on costs to consumers.

It's not just the bottom line or operations that are hurting. A recent academic study found that cyber-attacks can cause high levels of psychological harm—equal to conventional political violence and terrorism.[2]

AI ASSISTED SCAMS RISING

AI technologies are being leveraged by hackers to create convincing fake audio, video, and imagery to launch phishing campaigns. The accessibility and availability of Large Language Models is also driving greater volumes of attacks – SlashNext Threat Labs intelligence saw a 1,265% increase in malicious phishing emails since the launch of ChatGPT at the end of 2022.[3]

As Generative AI becomes more advanced, social engineering will become more and more difficult to detect. One study found that even as the technology stands today, humans are only able to detect artificially generated speech 73% of the time – a number that barely improved even after participants received training to recognise aspects of deepfake speech.[4]

ZERO-DAY VULNERABILITIES REACH A NEW CRESCENDO

By leveraging new critical vulnerabilities and quickly exploiting them before patches can be released and deployed, attackers can reach a huge number of potential victims across the globe. Ransomware has also been observed as being used concurrently with zero-days – as criminal groups look to scale attacks to increase financial returns.

In 2023, serious vulnerabilities were exploited in major software used broadly by enterprise across the world – impacting Apple, Microsoft and Citrix to name but a few. According to Mandiant, there has been a continuous increase in zero-day vulnerabilities since 2012. Between January and September 2023, 69 zero-day vulnerabilities were exploited alone, on track to surpass the current record of 88, set in 2021.[6]

CLOUD SECURITY GAPS CONTINUE TO GROW

The cloud is proving a bountiful hunting ground for threat actors. Research by Sysdig has found that attackers targeting the cloud are building tools that automate the scanning, finding, and exploiting of the target in the attack, and then accessing systems via leaked credentials and common vulnerabilities.[7]

Attacks on cloud-based networks per organisation increased by 48% between 2021 and 2022, according to data from Check Point.[8] This trend is likely to continue, with another report showing nearly 600% annual growth in the vulnerable cloud attack surface.[9]

OUR RESEARCH AT A GLANCE

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

2/5

SAY **CLOUD MISCONFIGURATIONS** OR VULNERABILITIES WERE TO BLAME

29%

SAY **PERSONAL DATA WAS ACCESSED**

OVER **1/4**

EXPERIENCED **REPUTATION DAMAGE** OR NEGATIVE MEDIA COVERAGE

1 IN 3

SAW THEIR **BUSINESS OPERATIONS DISRUPTED**

46%

OF INCIDENTS AND ATTACKS TOOK **LONGER THAN 1 MONTH** TO RESOLVE

28%

POINT TO **3RD PARTY SUPPLIERS** AS THE CAUSE

CYBER-ATTACKS & INCIDENTS

In a bid to better understand how cyber-attacks and incidents have impacted New Zealand businesses, we asked survey respondents who had experienced an incident in the past 12 months to answer questions related to the root cause and impacts of the incident. Respondents selected all attack vectors that applied.

WHEN THE CLOUDS RAIN

Cloud has played a major role in recent cyber incidents, with two fifths businesses pointing to cloud misconfigurations and vulnerabilities as a factor.

DDOS STILL AN ISSUE

Reports of DDoS attacks continue to feature prominently. Globally, there has been an increase in activity stemming from geo-political events, including cyber warfare in Ukraine and Israel / Palestine. DDoS has also been observed as a tactic used in conjunction with other methods, leveraged by threat actors to mask other attacks occurring concurrently.

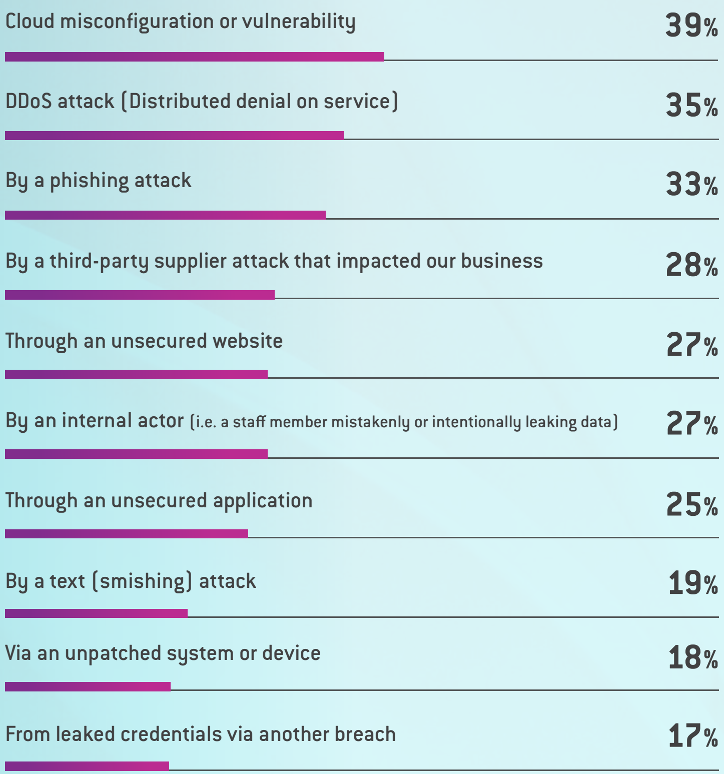
PHISHING STILL IN FOCUS

Smart phones are proving to be an attractive channel for phishing – with smishing attack reports up 6 percentage points year on year. Traditional phishing also remained high, with approximately one in three businesses reporting incidents.

THIRD-PARTY HEADACHES

Last year could arguably be known as the year supply chain attacks came into focus for New Zealanders – and unsurprisingly third-party attacks are a factor in over a quarter of all cyber-attacks and incidents.

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



BRACE FOR IMPACT

While the impacts from cyber-attacks and incidents were varied, they point to a wide range of disruptive and damaging consequences.

SERIOUS DISRUPTIONS

Approximately one in three businesses impacted in the past 12 months said the incident was serious enough to cause operational or business disruption. This is in line with patterns of behaviour observed amongst cybercriminals, targeting operational downtime as a means to extract gains from victims.

REPUTATION DAMAGE

Almost a quarter of business leaders said they saw negative media coverage or reputation damage as a result of a cyber incident.

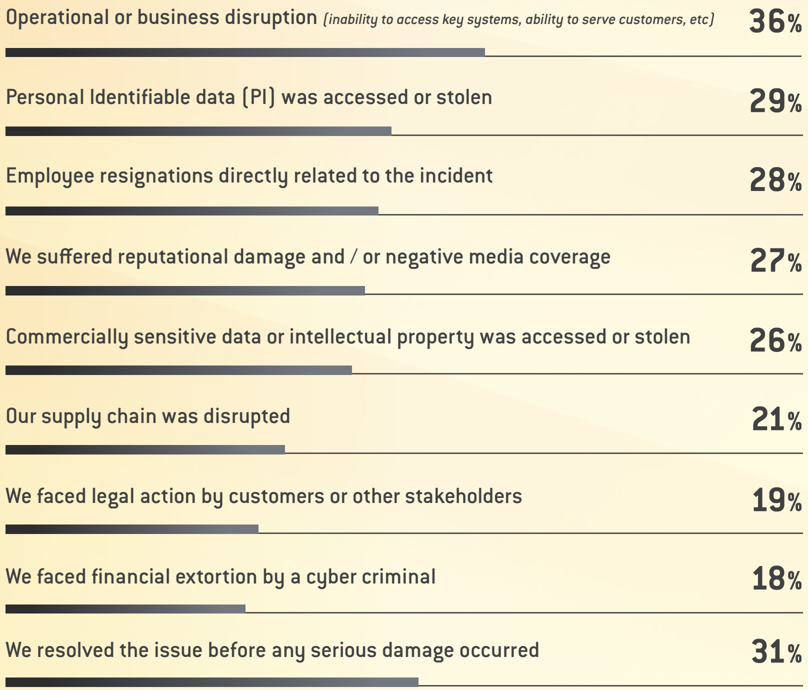
PEOPLE COSTS

Almost a third of business leaders say they saw resignations related to cyber incidents. While this number is higher than what we have typically seen in the market, it may indicate an emerging trend.

LEGAL AND FINANCIAL WOES

Financial extortion was not high on the list of impacts, which may point to better preparation by victims to backup businesses. However, the number of reports of businesses facing legal action has increased year on year.

WHAT WAS THE IMPACT OF THE CYBER INCIDENT ON YOUR BUSINESS?

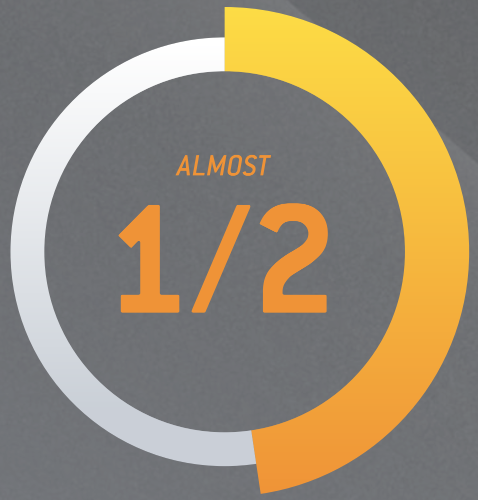


RESPONSE & RECOVERY

On average, across all attacks and incidents, 26% were resolved within a week, 28% between one and four weeks, and 46% took one month or more to resolve (including 9% taking five months or more).

Cyber-attacks involving leaked credentials via another breach took the longest time to resolve. This is to be expected – if there is a lack of monitoring, data can be exfiltrated and spread unknowingly until the data breach is announced, usually by the attacker. This can lead to a long period of investigation and remediation.

Phishing attacks were one of the quickest to be resolved, with 52% resolved within a week.



OF CYBER INCIDENT OR ATTACKS **TOOK MORE THAN ONE MONTH** TO FULLY RESOLVE

> *In cyber-attacks we've responded to here in New Zealand, generally speaking the detection and containment occurs fairly rapidly. What takes the most time is the restoration of operations and systems, especially if the business has not adequately backed up their data and systems. Backups must be carefully installed and tested to ensure the network is not overloaded, and do not contain malware. It's a time-consuming process.*

CONAN BRADLEY

INCIDENT RESPONSE & DIGITAL FORENSICS PRACTICE LEAD | KORDIA

LESSONS LEARNED FROM THE FRONT

We asked business leaders to tell us in their own words what they would do differently based on their experiences dealing with a cyber incident. Themes covered in the responses were varied – the most cited theme is to have invested in better cyber security systems and policies.

> *As a company we have all taken an extra step at keeping our information private and we have made our cyber security harder to break into.*

> *We now have a much more comprehensive cyber security policy.*

> *I would have bought the most reliable protection there is no matter the cost in order to keep everything safe.*

> *Improving or implementing employee training is another important action that would have been done differently.*

> *Create mock events so employees can visually understand the form of phishing attacks.*

> *Implement regular staff training on security attacks.*

> *Contact security experts in time, back up important data, and strengthen security measures.*

> *We could have hired IT specialists instead of relying on the company IT department to resolve the problem.*

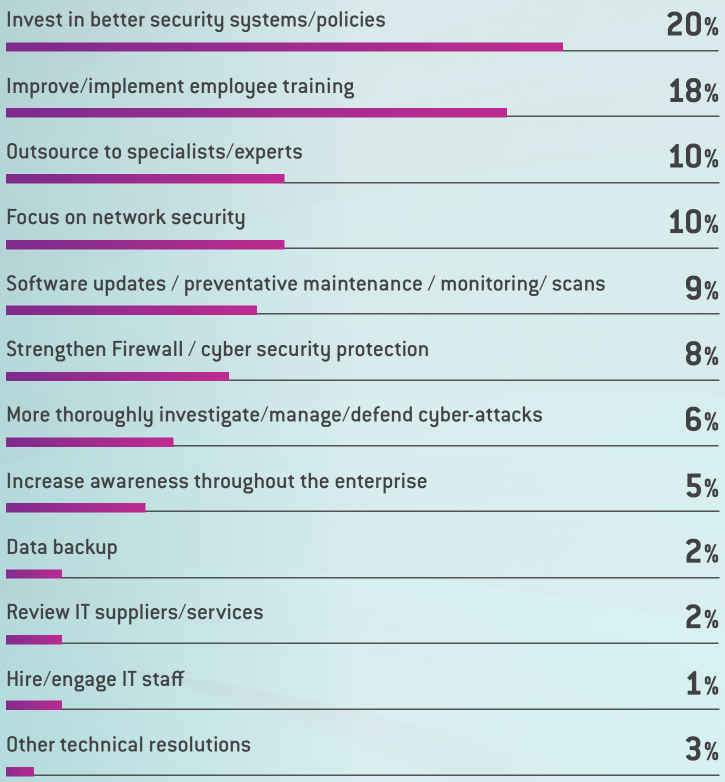
> *Strengthen network security management and pay close attention around the clock.*

> *Configure the cloud more securely so that the security breach does not occur.*

> *We should have updated our software earlier.*

BASED ON LEARNINGS FROM YOUR EXPERIENCES DURING THE CYBER INCIDENT, WHAT WOULD YOU HAVE DONE DIFFERENTLY?

(CODED RESPONSES)



WHAT KEEPS BUSINESS LEADERS AWAKE AT NIGHT?

Despite ransomware attacks and extortion dominating the headlines, most business leaders say employees, cloud misconfigurations and third party suppliers pose more risk to their organisations.

Alarmingly, one in four respondents said a lack of understanding around cyber security risks and priorities was a top challenge in their organisation. Despite this, 88% of respondents said they were confident in their business's ability to withstand a major cyber-attack.

TOP THREATS TO CYBER SECURITY POSTURE AS PERCEIVED BY BUSINESSES

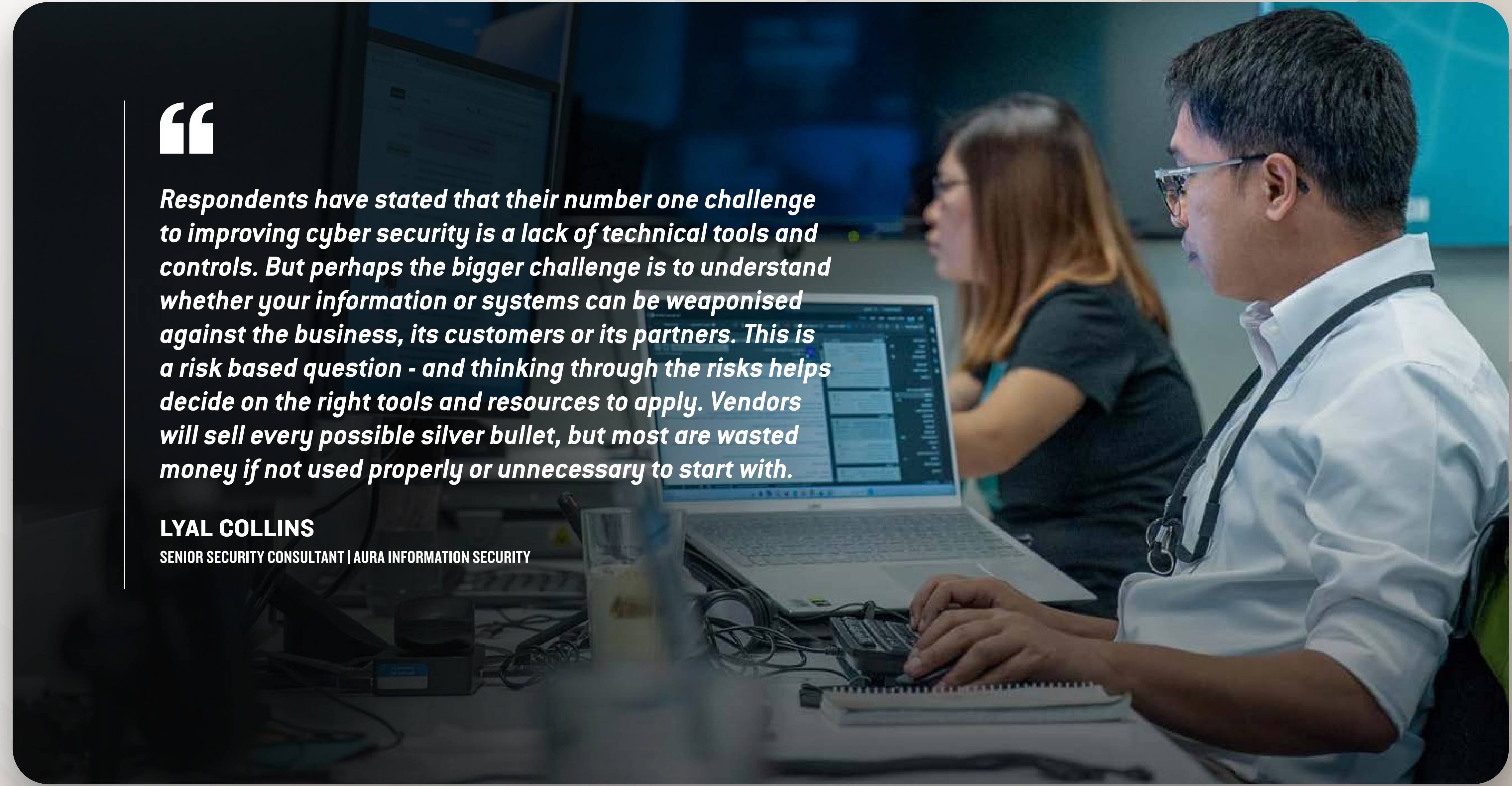
(RESPONDENTS SELECTED THEIR TOP THREE)

#1	Employees accidentally exposing our business
#2	Cloud misconfigurations
#3	Cyber-attacks or data leaks coming through third party suppliers
#4	IoT (internet of things) vulnerabilities and misuse
#5	Malicious insider threats
#6	Zero-day vulnerabilities
#7	DDoS attacks
#8	Stolen data leading to blackmail/extortion
# 9	Ransomware attacks

TOP CHALLENGES TO IMPROVING CYBER SECURITY AS PERCEIVED BY BUSINESSES

(RESPONDENTS SELECTED THEIR TOP THREE)

#1	Lack of technical tools and controls
#2	Lack of understanding of our risks and security priorities
#3	Lack of security awareness and good behaviours amongst employees
#4	Trying to manage increasing levels of attacks and attempts
#5	Difficulty recruiting skilled people to effectively manage cyber security
#6	Trying to keep security in step with digital transformation
#7	Lack of governance around cyber security and risk
#8	Burn out from security and IT teams due to high workloads
# 9	Ageing technology that can't be updated to meet current security standards



> *Respondents have stated that their number one challenge to improving cyber security is a lack of technical tools and controls. But perhaps the bigger challenge is to understand whether your information or systems can be weaponised against the business, its customers or its partners. This is a risk based question - and thinking through the risks helps decide on the right tools and resources to apply. Vendors will sell every possible silver bullet, but most are wasted money if not used properly or unnecessary to start with.*

LYAL COLLINS

SENIOR SECURITY CONSULTANT | AURA INFORMATION SECURITY

CLOUD SECURITY

Cloud adoption in New Zealand has been steadily growing for several years, with a burst of uptake following the Covid-19 pandemic. An IDC study predicts that by 2026, cloud delivery is expected to add $21 billion NZD to the economy and generate 134,000 new jobs.[10] Whilst digital transformation continues on an upward trajectory, businesses need to factor in adequate security from the outset, with ongoing management and testing.

The IBM X-Force Cloud Threat Landscape Report 2023 tracked 632 new cloud-related vulnerabilities (CVEs) between June 2022 and June 2023[11], a 194% increase from the previous year. The report also confirmed that cloud credentials are a hot commodity on the dark web, comprising around 90% of cloud assets for sale on the dark web.

> ***Cloud skills are hard to find and businesses tend to build in the cloud quickly, with security often an afterthought. The result often means that the cloud works, but it isn't secure. We find this from government down to small businesses. "DevOps" is more like "DevOops".***
>
> **ALASTAIR MILLER**
> PRINCIPAL CONSULTANT | AURA INFORMATION SECURITY

CLOUD SECURITY

2/5

OF **ALL INCIDENTS** ACCOUNTED FOR WERE **CLOUD INCIDENTS**

46%

OF CLOUD INCIDENTS TOOK **MORE THAN ONE MONTH** TO RESOLVE

24%

SAY KEEPING CYBER SECURITY **IN STEP WITH DIGITAL TRANSFORMATION** IS **A TOP CHALLENGE**

1 IN 3

SAY **CLOUD IS ONE OF THE TOP THREATS** TO THEIR ORGANISATION'S CYBER POSTURE

PEOPLE & CYBER SECURITY

Despite 84% of respondents saying that their organisation has a cyber security awareness or training programme for employees, phishing attacks and internal actors were a factor in around a third of reported incidents.

Labour issues are causing headaches for local businesses. The global talent shortage for skilled cyber security professionals has been well documented. The World Economic Forum indicates that there is a shortage of 3.4 million cyber security experts to support today's global economy, which the industry is struggling to fill.[13]

Securing talent is also an issue for New Zealand organisations, with one in four respondents saying that recruiting skilled cyber security employees was a top challenge. This resonates with other industry reports - a global survey found that 55% of cyber security professionals say they experience stress at work half the time, which in 21% of cases leads them to think about leaving the profession.[14]

PEOPLE & CYBER SECURITY

ALMOST 1/2 SAY **EMPLOYEES ACCIDENTALLY EXPOSING** THE BUSINESS IS A TOP CYBER RISK FOR THEIR BUSINESS

1 IN 4 SAY **RECRUITING SKILLED PEOPLE** TO MANAGE CYBER SECURITY IS A TOP CHALLENGE

28% OF BUSINESSES SAW **EMPLOYEE RESIGNATIONS** RELATED TO CYBER INCIDENTS

1/4 POINT TO A **LACK OF SECURITY AWARENESS** AND GOOD BEHAVIOURS AS HINDERING CYBER SECURITY

1 IN 5 SAY **BURNOUT AMONGST SECURITY AND IT TEAMS** IS A TOP CHALLENGE TO IMPROVING CYBER SECURITY

BUSINESSES BEHIND IN MITIGATING RISKS

More than 80% of surveyed leaders said their businesses experienced some sort of cyber incident or attack in the past 12 months. This shows there is evidence many organisations are still struggling to get basic cyber hygiene practices in order.

One fifth of businesses have not performed a penetration test in the past 12 months. One in six fail to monitor their network, and the same number do not track their assets to ensure patching and vulnerability management is kept top of mind.

Regular testing, training, monitoring and patching are examples of fundamental controls that every business needs to implement as part of a robust cyber security programme.

> *In the realm of cyber security, the strength of any programme rests on its foundational elements. Understanding which digital identities are in your digital ecosystem and where your assets are is key to understanding your business risk. But it doesn't stop there; monitoring and fine-tuning our defences are crucial steps towards ensuring a strong cyber security posture.*
>
> **JOSHUA REEDY**
> CISO | KORDIA

OF BUSINESSES HAVE NOT REHEARSED AN INCIDENT RESPONSE PLAN IN THE PAST 12 MONTHS.

DESPITE THIS,

OF RESPONDENTS SAY THEY HAVE CONFIDENCE IN THEIR BUSINESS'S ABILITY TO WITHSTAND A MAJOR CYBER-ATTACK OR INCIDENT.

BUSINESSES BEHIND IN MITIGATING RISKS

1 IN 5

HAVE **NOT PERFORMED A PENETRATION TEST** IN THE PAST 12 MONTHS

~1 IN 6

DO NOT MONITOR/LOG THEIR NETWORK

14%

HAVE NO AWARENESS OR TRAINING PROGRAMME FOR EMPLOYEES

1 IN 5

ARE LACKING A SINGLE SOURCE OF **MANAGING DIGITAL IDENTITIES**

23%

HAVE NOT **PRACTICED AN INCIDENT RESPONSE PLAN**

1 IN 6

DO NOT TRACK THEIR ASSETS TO ENSURE THEY ARE BEING PATCHED AND VULNERABILITY SCANNED

70%

OF BUSINESSES SURVEYED WOULD **CONSIDER PAYING A RANSOM** TO A CYBERCRIMINAL

> *Any money paid to cybercriminals goes towards increasing the sustainability of organised crime. The decision to pay or not to pay comes with a degree of risk, whichever route you choose. If you pay, what guarantees are there that you will receive the decryption key, or that the actors will not sell your data anyway? Or worse, communicate with other ransomware gangs regarding the entry point and your willingness to pay?*

CONAN BRADLEY

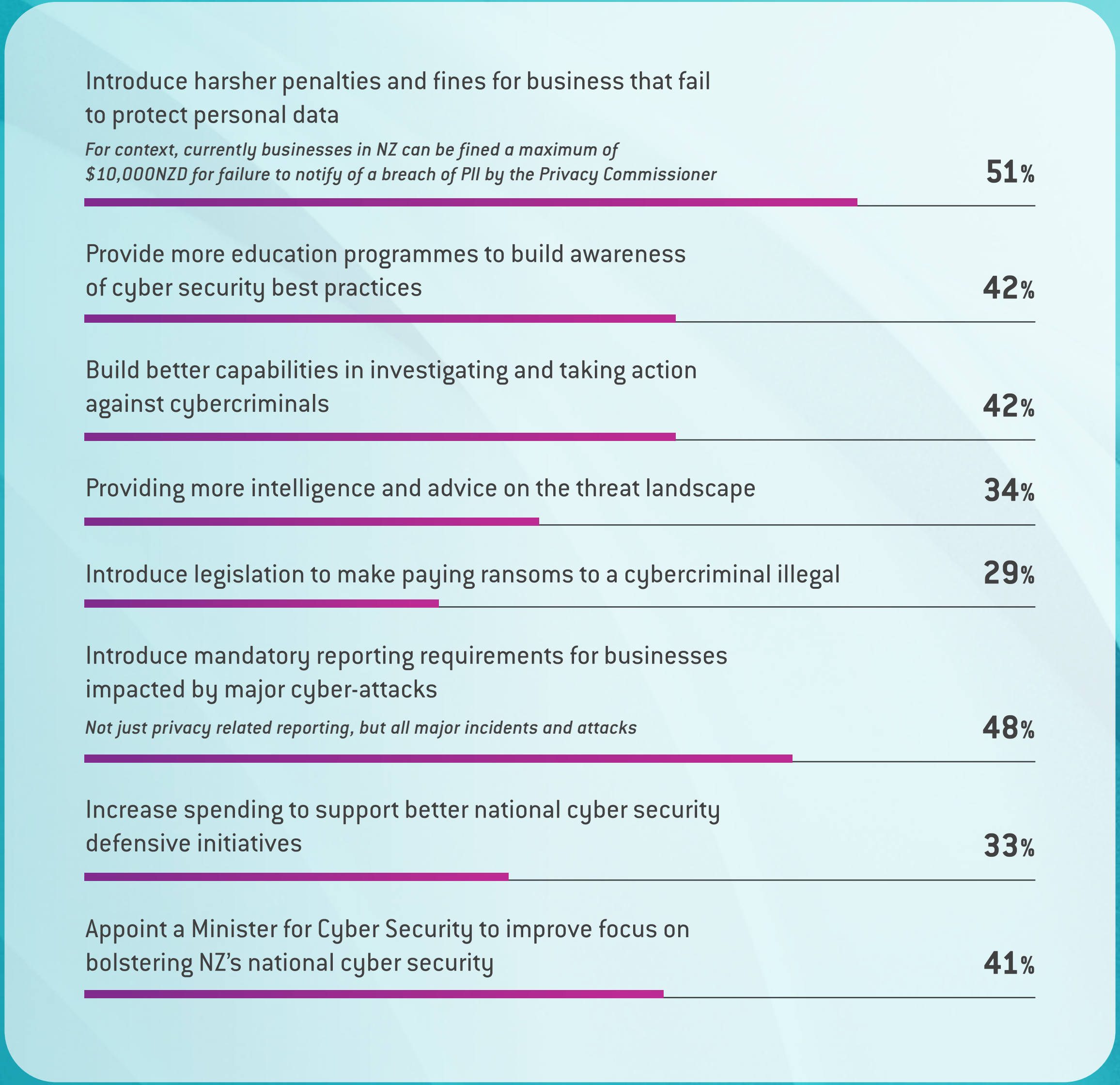
INCIDENT RESPONSE & DIGITAL FORENSICS PRACTICE LEAD | KORDIA

WHAT DO BUSINESS LEADERS WANT THE GOVERNMENT TO DO IN THE FACE OF INCREASING CYBER RISK?

Business leaders are eager to see more action to penalise organisations that fail to adequately protect data. New Zealand's current privacy laws cap penalties at $10,000 NZD – significantly lower than penalties in other five eyes nations.

Australia has made notable changes to cyber security governance, through a slew of legislative changes including harsher privacy law penalties of up to $50 million AUD and mandatory reporting requirements for ransomware attacks. A notable number of respondents have indicated they would be supportive of similar initiatives in New Zealand.

A third of business leaders want the government to increase spending on national cyber security.



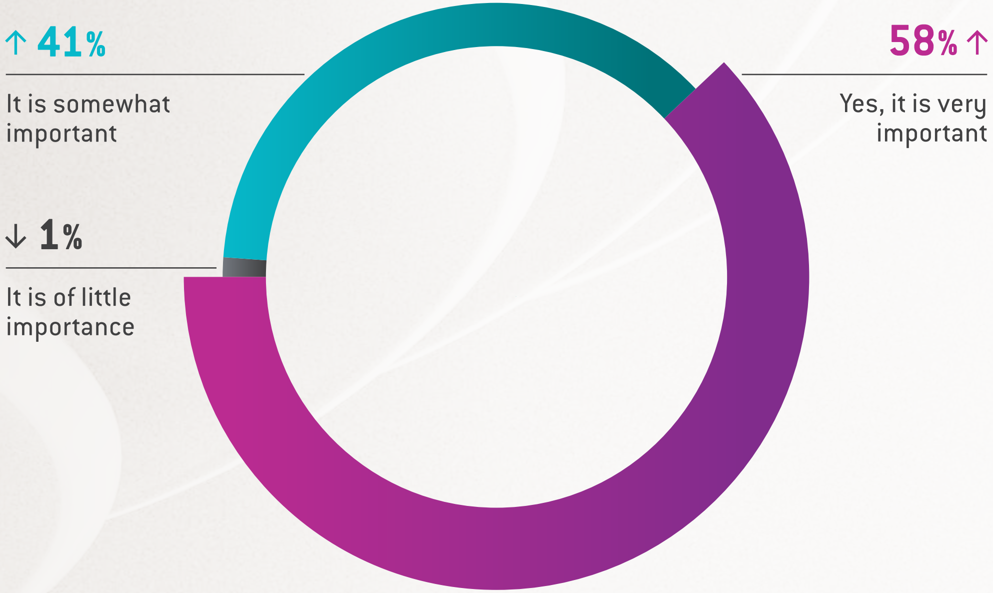
CYBER SECURITY GOVERNANCE

Cyber security is often seen as a technical and complex area of business. Directors need to develop an understanding of how increasing attacks and a larger digital footprint impacts the cyber resilience of their organisation.

In the 2023 IoD Director Sentiment Survey[11], just 23.5% of directors said cyber security and cyber-attacks were a key issue for boards. The survey also found that only 62.3% of respondents said their boards regularly discuss cyber risk and are confident their organisation has the capacity to respond to a cyber-attack or incident.

> *One of the main challenges for boards is what questions to ask and how to measure the effectiveness of the controls in place for managing the risk. Due to the technical nature of cyber security, it's more challenging for boards to assess the risk compared to other fields such as Financial or Health & Safety risk management.*
>
> **DERMOT CONLON**
> EXECUTIVE GENERAL MANAGER CYBER SECURITY | KORDIA

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



FOCUS AREAS FOR BUSINESS IN 2024

1

PLAN FOR RECOVERY AS PART OF YOUR RESPONSE

Operational downtime can damage a business more than the initial cyber-attack. Effectively recovering as rapidly as possible after a major cyber-attack depends on a properly deployed backup and restore regime. This offers you resilience in the event of a major cyber-attack, as well as protecting your critical data from accidental destruction or deletion. Any solution should include encryption, along with the combination of full, incremental, and differential backups. This will ensure that even if your data is breached, it is completely worthless to any malicious actor wishing to exploit it.

2

SECURITY SHOULD GO HAND IN HAND WITH CLOUD TRANSFORMATION STRATEGY

There are lingering perceptions that the cloud is more secure than more traditional on premise systems. While there are certainly security and accessibly benefits that can be leveraged from the cloud, without the right security layers, businesses are just as exposed. The best way to ward against misconfigurations and security gaps in cloud environments is to implement an adoption framework that sets out how security is factored into your cloud environment, and how it evolves as your platforms do. That way you can make the best decisions around the deployment – whether that be public, private or hybrid cloud solutions. Regular testing of cloud environments is also critical.

3

RATIONALISE SPEND VIA RISK-BASED PLANNING

Assessing how to invest appropriately in security can be challenging – especially in the face of rising costs and tough economic conditions. As organisations expand their digital operations, a risk-based approach can help rationalise spend and set strategic objectives to ensure security needs are being addressed. Understanding your risks will help determine areas of focus, providing a starting point to building out a holistic security programme. Ongoing measurement of the effectiveness of your strategic roadmap will determine whether your organisation is focusing and investing in the right areas.

FOCUS AREAS FOR BUSINESS IN 2024

4

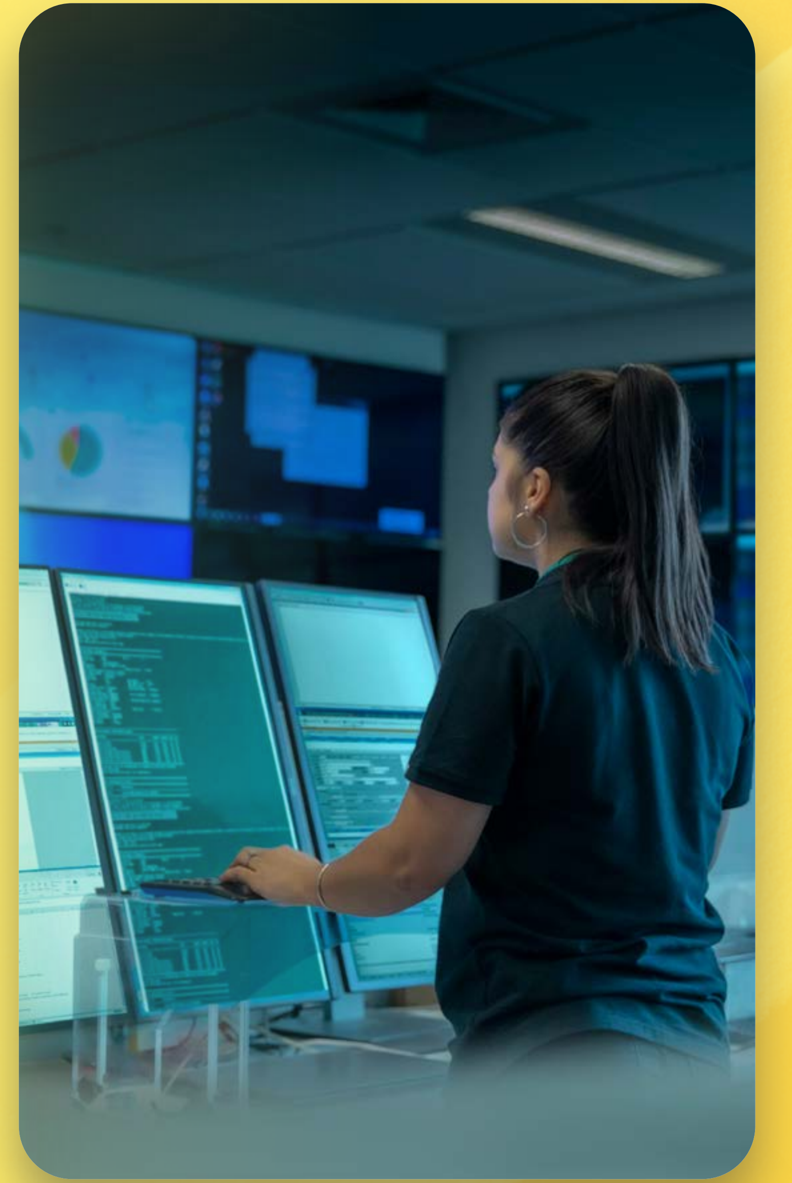
FACTOR PEOPLE INTO YOUR CYBER STRATEGY

Human error accounts for many cyber security incidents and data breaches. Whether it's through an employee mistakenly clicking on a phishing email link, or a developer failing to factor in security into software design, there's a need for better awareness and adoption of security behaviours across all facets of organisations. A once-a-year online training programme on cyber tips is no longer effective. Business leaders need to champion a culture change within the organisation, that sees all employees adopting a mindset shift. Start by making cyber security a priority at the top of the organisation, to embed responsibility for cyber security across all levels of the business.

5

ELEVATE CYBER SECURITY TO THE BOARD

Only two thirds of respondents told us that cyber security was deemed a very important issue for their organisation's board. With a significant number of businesses confirming they are being compromised, it is imperative that board members take cyber defences seriously. Cyber security is no longer an IT or operational issue – it requires good governance to ensure that it's aligned with the overall business strategy, and that initiatives have the right level of focus and resource from the top. We'd recommend all board directors take steps to ensure they are well versed in the risks presented by digital threats. Participating in an incident simulation or tabletop exercise can also be useful to the board for response and recovery planning.



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 2023

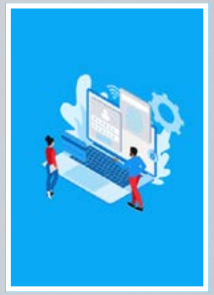
Compare our latest findings with research conducted with New Zealand businesses in 2023.

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.



WEB-APP SECURITY

Understand how your web-apps can be exploited and how to implement a web-app operational security program.

REFERENCES

1. IBM Cost of Databreach Report 2023 **2.** Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis – Journal of Global Security Studies **3.** "Report shows 1265% increase in phishing emails since ChatGPT launched" - Security Magazine **4.** "Humans can detect deepfake speech only 73% of the time, study finds" - The Guardian **5.** "Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before" - Mandiant **6.** "A Guide to Zero-Day Vulnerabilities and Exploits for the Uninitiated" – Infosecurity Magazine **7.** "What We Can Learn From Major Cloud Cyberattacks" – Dark Reading **8.** "Check Point Research flags a 48% growth in cloud-based networks attacks in 2022" – Checkpoint **9.** "2023 State of Cyber Assets Report Reveals Nearly 600% Annual Growth in Vulnerable Cloud Attack Surface" – JupiterOne via PR News Wire **10.** "Public cloud to add $21 billion to NZ economy by 2026" – Microsoft **11.** " New X-Force Cloud Threat Landscape 2023 Report" **12.** "The cybersecurity skills gap is a real threat — here's how to address it" – World Economic Forum **13.** Cybersecurity and Burnout: The Cybersecurity Professional's Silent Enemy – ISACA

kordia®

KORDIA.CO.NZ