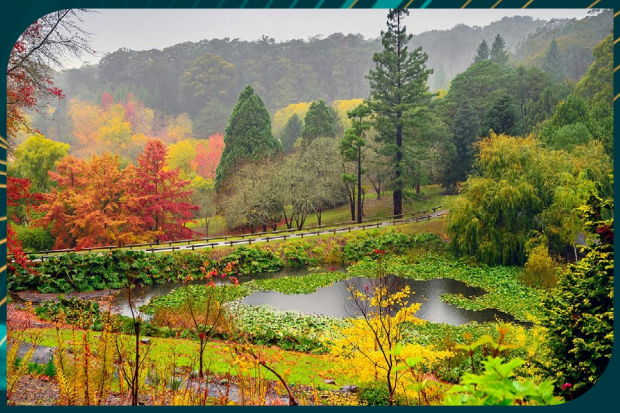
Nexia Australia

Not-for-Profit Newsletter



Edition 20 - May 2024

Contents

Welcome to the latest edition of our Not-for-Profit Newsletter. Please feel free to contact us if you have any questions about the content of this Newsletter.

In this edition

Following our previous edition that noted some high profile examples of organisations that have been impacted by cyber-attacks, this edition covers some cyber-security tips and how to respond to cyber-attacks. This edition also covers a number of changes to workplace laws that organisations need to be aware of. We have also included a number of governance and director-related matters and ACNC activities.

Governance

NFP directors at tipping point

The Australian Institute of Company Directors' *Not-for-Profit Governance* and *Performance Study 2023-24* has revealed that increasing demands and higher expectations has propelled directors to a tipping point.

The AICD partnered with Piazza Research Pty Ltd to conduct the study. More than 1390 directors responded.

As time commitments increased considerably, governance arrangements were being stretched, particularly in NFP sub-sectors such as aged care.

Recent royal commissions had shone a spotlight on governance in the 'are economy' and the results showed that while changes were being made to enhance governance, organisations were stretched to meet increasing demands.

Half of all respondents to the survey indicated that they were spending more time on director duties compared with the year before.

Close to half of respondents (47 per cent) were spending more than three days a month on governance. And of these, 22 per cent were spending more than six days a month.

Organisations were working towards ensuring quality care, half of boards using CEO and management reports as their primary mechanism for overseeing it.

The study also revealed that 21 per cent of respondents said that their organisation had been the target of a cyber-attack within the past 12 months.

Forty-two per cent of boards include cybersecurity discussion in every board meeting, 44 per cent discussing it only once a year.

Other key findings included:

- Twenty-one per cent of NFP directors were remunerated, which has steadily increased from 14 per cent five years ago. Just over three-quarters of board members reported being unpaid, or only had expenses covered
- The increased rate of mergers previously expected had yet to happen, just over a fifth of NFP organisations discussing a merger, but only six per cent undertaking one
- Only 44 per cent of respondents reported making a profit in 2022-23, down from 49 per cent the previous year. Health and residential aged-care sectors reported that only 36 per cent made a profit. By comparison, 67 per cent of development and housing respondents made a profit
- Fifty-two per cent of organisations reported governance of climate change never appeared on their board's agenda, and
- Seventy per cent of respondents rated their organisation as either highly or mostly effective in achieving its purpose.

Good-governance guide released

The Governance Institute has released a comprehensive governance guide that addresses the challenges faced by NFPs in today's environment.

Authority and Delegation of Decision-Making in Not-for-profit Organisations comes at a crucial time when NFPs are grappling with significant funding constraints and complex operating environments, among other challenges.

The guide covers a range of topics essential for effective governance, including the responsibilities of boards, their composition, and the delegation of authority. It also provides valuable insights into governance practices.

Institute CEO Megan Motto emphasised the guide's importance for NFP boards and directors.

'In today's rapidly changing landscape, not-for-profit organisations need robust governance frameworks to ensure accountability, transparency, and effectiveness', said Ms Motto.

The guide addresses the issue of board tenure, recommending a maximum of three terms for directors to balance continuity and fresh perspectives.

One of its key recommendations is to diversify boards, ensuring a variety of perspectives and skills to meet an organisation's obligations effectively. It also emphasises the need for clarity in delegation, stating that boards can never delegate their ultimate responsibilities.

ASIC prosecutes a director without ID

ASIC has begun the first prosecution of a director for failing to comply with the obligation to have a director-identification number.

A director appeared in Downing Centre Local Court and was formally charged with one count of contravening section 1272C(1) of the *Corporations Act 2001* by failing to have a director ID. The court granted an interim non-publication order prohibiting disclosure of the defendant's identity. The charges were listed for a further mention in April.

Directors are required by law to verify their identity with Australian Business Registry Services before receiving a director ID. They must apply for their IDs within the following timeframes:

- Directors appointed before 1 November 2021 had until 30 November 2022 to apply
- New directors appointed for the first time between 1 November 2021 and 4 April 2022 had 28 days from their appointment to apply, and
- From 5 April 2022, intending new directors had to apply before being appointed.

The maximum penalty for an offence against section 1272C(1) of the act is 60 penalty units. The defendant in this matter is facing a maximum fine of $13,320.

Being a director isn't easy

A speech by ASIC chair Joe Longo at the Australian Institute of Company Directors Australian Governance Summit addressed the following themes:

- Complying with directors' duties may be difficult, but ASIC expects you to do it; it can be done, and there are benefits
- Developments in AI, cyber threats, sustainable finance, and ESG mean greater complexity in the business environment, and
- Directors need to ask themselves the right questions: Are you acting honestly? Are you putting the company first? Do you have a continuous curiosity to understand the business and associated risks? And are you challenging management and getting professional advice?

Cyber Security

Be wary about who handles personal information

The risk of outsourcing personal-information handling to third parties is highlighted in *Notifiable data breaches report July to December 2023* by the Office of the Australian Information Commissioner.

Information commissioner Angelene Falk said the OAIC continued to be notified about a high number of multi-party breaches, most resulting from a breach by a cloud or software provider.

'Organisations need to proactively address privacy risks in contractual agreements with third-party service providers', said Commissioner Falk.

'This includes having clear processes and policies in place for handling personal information and a data-breach response plan that assigns roles and responsibilities for managing an incident and meeting regulatory reporting obligations.'

From July to December 2023, 483 data breaches were reported to the OAIC, up 19 per cent from the first half of the year. There were an additional 121 secondary notifications, a significant increase from 29 in January to June.

Malicious and criminal attacks remained the leading source of data breaches, accounting for 322 notifications. Most (211) were cyber-security incidents. The health and finance sectors remained top reporters of data breaches, 104 and 49 notifications respectively.

Commissioner Falk said the notifiable data breaches scheme was well established and the OAIC expected organisations to comply with their obligations.

'The OAIC is escalating its regulatory actions into data breaches, and we have commenced civil penalty proceedings in the Federal Court', she said.

'We are prioritising regulatory action where there appears to be serious failures to comply with the scheme's reporting requirements and to take reasonable steps to protect personal information and where organisations are holding onto data much longer than is necessary.

'As the guardians of Australians' personal information, organisations must have security measures in place to minimise the risk of a data breach.

'If a data breach does occur, organisations should put the individual at the front and centre of their response, ensuring they are promptly told so their risk of harm can be minimised.'

ASD offers cyber-security tips

Cyber threats are on the rise in Australia, the Australian Signals Directorate receiving nearly 94,000 cybercrime reports in the 2022-23 financial year, a report every six minutes.

Charities and NFPs are cyber-criminals' prime targets.

Key cyber threats are phishing, business-email compromises, and ransomware, says the ASD.

Effects of a cyber-security incident can be devastating and include financial loss, data breaches, reputational damage, loss of trust from donors and beneficiaries, and harm to the communities the NFPs serve.

The directorate offers the following tips:

- Turn on multi-factor authentication where possible
- Check automatic updates are on and install them as soon as possible
- Back-up important files and device-configurations often. Test your backups on a regular basis
- Use a reputable password manager to create strong, unique passwords or passphrases for your accounts
- Provide cyber-security training, particularly on how to recognise scams and phishing attempts
- Use access controls and review them often so that staff may access only what they need to for their duties. This will reduce potential damage caused by malware and unauthorised access to systems
- Use only reputable and secure cloud services and managed service providers
- Test cyber-security detection, incident response, business continuity, and disaster recovery plans often
- Review the cyber-security posture of remote workers and connections. Make sure staff are aware of secure ways to work remotely, such as not accessing sensitive information in public, and
- Report a cyber-crime, incident, and vulnerability.

Join ASD's *Cyber Security Partnership Program* as a business or network partner. This free program provides advice and insights on the cyber-security landscape.

Review cyber-security regularly to strengthen resilience. Seek help from an IT professional if you are unsure about it.

How to respond to cyber-attacks

New guidance on cyber security aims to help directors respond to cyber-attacks.

Governing Through a Cyber Crisis – Cyber Incident Response and Recovery for Australian Directors has been developed by the Australian Institute of Company Directors in partnership with the Cyber Security Cooperate Research Centre and law firm Ashurst.

Based around the 'four Rs' – readiness, response, recovery, and remediation – the guidance covers the most vexing issues directors face in cyber crises, from the development of a cyber-incident readiness plan, execution of an effective crisis communications strategy, whether or not to make a ransom payment, and the road to rebuilding reputation.

Federal Minister for Cyber Security Clare O'Neil said business leaders, boards, and directors have important obligations to protect their organisations and customers from cyber risks.

'Australians rightly expect businesses to take cyber security seriously. The explosion of cyber incidents over the past two years has shown that we cannot be complacent on cyber. All Australian organisations need to embrace better cyber governance from the board down', she said.

'This guidebook [provides] detailed guidance to corporate leaders on cyber preparation, response and recovery. I commend this guidance to Australian organisations of all sizes and encourage leaders to embed these principles into how they do business.'

AICD managing director and CEO Mark Rigotti said cyber security was at the forefront of contemporary Australian governance.

'Boards have a key governance role to play in dealing with increasing cyber threat. Cyber-security is consistently the number one thing keeping directors awake at night and this resource will put them in a stronger position to navigate the challenges posed by cyber risks.'

The guidance builds on the joint 2022 AICD and Cyber Security Cooperative Research Centre's *Cyber Security Governance Principles*.

An accompanying *Snapshot of Governing Through a Cyber Crisis – Cyber Incident Response and Recovery For Australian Directors* includes a checklist of practical steps for SME and NFP directors to respond to a critical cyber incident.

Workplace Laws

Know the new workplace laws

The Fair Work Ombudsman (FWO) is encouraging employers to learn and comply with workplace-law changes or risk facing new significantly higher penalties.

The second set of *Closing Loopholes* changes were legislated in February and follow the federal government's first *Closing Loopholes* changes passed in December.

The second set of changes take effect at various dates throughout this year and next, many already in effect. The new laws cover gig work, casual employment, and the right to disconnect, among other areas.

'Employers, employees and independent contractors need to understand the changes, which create new or changed responsibilities and rights in a range of areas', FWO Anna Booth said.

'The changes substantially increase the penalties which a court can order for non-compliance with a range of workplace laws, by up to five times for non-small business employers.

'This sends a clear message and expectation - employers must invest the time and resources to meet their new legal obligations.'

Workers to be redefined in August

From no later than 26 August, there will be new definitions of *employee* and *employer* under the Fair Work Act.

In determining whether an employment relationship exists, the totality of the relationship must be considered, including the 'real' substance, practical reality, and true nature of the working relationship.

Definition changes mean an employee is a casual only when:

- There fails to be a firm advance commitment to continuing and indefinite work, factoring in the real substance, practical reality, and true nature of the employment relationship, and
- The employee is entitled to be paid a casual loading or a specific pay rate for casuals.

A new pathway will also replace existing rules for eligible casual employees to change to permanent employment if they want to.

Big hikes in Fair Work Act penalties

New maximum penalties that courts can impose for certain contraventions of the *Fair Work Act* have come into effect. They apply only to employers who aren't individuals or small businesses.

Maximum penalties have increased five times to a total of $469,500 per contravention for a company.

For serious contraventions, maximum penalties have increased also five-fold, to $4,695,000 for a company (previously $939,000).

Maximum penalties applying to individuals and small businesses are $18,780 per contravention for an individual and $93,900 for a company.

Maximum civil penalties available for non-compliance with a compliance notice have doubled for employers of any size to a total of $18,780 for an individual and $93,900 for a company per contravention.

From no earlier than 1 January, penalties for underpayment-related contraventions by non-small businesses can be three-times the amount of the underpayment if an applicant chooses to pay this way.

A serious contravention under the Act has become one that is done either knowingly or recklessly (it is no longer required to prove a breach was done knowingly and systematically).

'Employee-like' workers to be protected

From no later than 26 August, the interests of 'employee-like' workers in the gig economy will be protected under new laws.

'Employee-like' workers work through a digital labour platform and can have low bargaining power, low pay, and little say in how they perform their work.

The Fair Work Commission – a separate government organisation from the FWO – will be able to set minimum standards by making orders and will be able to establish guidelines. They will also be able to deal with disputes on the unfair 'deactivation' of an employee-like worker from a digital-labour platform.

Unions that are registered organisations representing employee-like workers will be able to make collective agreements with digital-labour-platform operators.

Independent contractors who earn less than a high-income threshold, including employee-like workers, will be able to apply to the commission if they think their services contract contains unfair terms. The threshold is yet to be set.

Similar rules and processes will also apply to independent contractors in the road-transport industry.

Workers to have a right to leisure time

Employees will soon have the right to refuse to monitor, read, and respond to contact or attempted contact from an employer or third party outside working hours.

The change will be mandated in 18 months for small-business employers and in six months for other employers.

An employer may deem that the refusal is unreasonable in certain cases, including the reason for the contact, the level of disruption, any compensation the employee receives to be available or work additional hours, and the employee's role, responsibilities, and circumstances.

Disputes can be taken to the Fair Work Commission if they can't be resolved at work.

Fraud

Billions lost through fraud

To support organisations and anti-fraud professionals, the Association of Certified Fraud Examiners has released *Occupational Fraud 2024: A Report to the Nations*.

The 13th edition of the ACFE's biennial research continues a pivotal role in shedding light on occupational fraud, offering insights into the mechanics of fraud within organisations worldwide.

The report contains:

- Global fraud statistics, highlighting the impact globally of occupational fraud, losses in the cases analysed amounting to more than $3.1 billion
- Case studies and implications analysing 1921 actual fraud cases investigated by the examiners, providing insights into the schemes used and lessons learned
- The impact of COVID-19 as cases were investigated between January 2022 and September 2023. As the typical fraud case lasts 12 months before being detected, most cases in the study probably occurred at the height of the COVID-19 pandemic, and 53 per cent of them had at least one pandemic-related factor contribute to the fraud
- Profile of a fraudster, detailing the typical fraudster, including his or her position within an organisation, tenure, and the methods he or she most commonly used to conceal fraud
- Methods of detection, emphasising the increasing role of technology and data analytics in uncovering fraudulent activities, and
- An evaluation of the importance of effective anti-fraud controls, more than half of occupational frauds occurring due to a lack of internal controls or an overriding of them.

Fake invoices cost millions

Australians last year reported losing $16.2 million to payment-redirection scams.

The Australian Consumer & Competition Commission is urging organisations and individuals to check payment details direct with a business before paying an emailed invoice following a rise in losses to payment-redirection scams.

'Scammers are sophisticated criminals and are becoming more targeted in how they exploit Australian consumers and businesses', ACCC deputy chair Catriona Lowe said.

'These criminals are posing as genuine businesses that a consumer has recently dealt with, sending fake invoices with altered payment details so that the money ends up with the scammer.

'This scam is hard to detect because the scammer will either hack into the email system of the business or impersonate the business's email address by changing as little as one letter.

'If you receive an invoice via email, take the time to call the business on a number you have found yourself to confirm that the payment details are correct.

How the scam works:

- You receive an email from a business you are dealing with and are expecting an invoice from
- You pay the invoice thinking that the payment is going to the business

- You are unaware that scammers have gained access to the business email account or changed the email address and modified the payment details (BSB and account number). You make a payment to the scammer instead of the actual business
- You are unlikely to notice anything unusual until you receive a demand for payment from the business for an invoice you believe you already paid, and
- If you respond to the email to query the change to the payment details on the invoice the scammer will respond, justifying the change.

The ACCC says you should:

- Stop – don't rush to act. Take the time to call the business you are dealing with – using independently sourced contact details – to check that payment details are correct
- Think – ask yourself if you really know who you are communicating with? Scammers can make invoices appear legitimate by copying logos and ABNs. Scammers can send emails that appear to be from the business you have been dealing with after changing invoice banking details
- Protect – act quickly if something feels wrong. If you have shared financial information or transferred money contact your bank immediately, and
- Help others by reporting to *Scamwatch*.

ACNC Activities

ACNC announces targets

The Australian Charities and Not-for-profits Commission has announced that it will focus on the misuse of complex corporate structures and the way charities manage cyber-security challenges.

'The ACNC is becoming increasingly concerned about the misuse of complex structures [that might] be part of attempts to conceal non-compliance with the ACNC Act and regulations', commissioner Sue Woodward said.

'Charities are free to use a variety of structures to suit their purpose and we acknowledge there can be good and legitimate reasons to do so. However, the decision to utilise complex structures, or the gradual and perhaps ad hoc development of complex structures, also comes with more complex governance obligations.

'While many charities are well advised and adhere to robust compliance regimes, there are others which may not appreciate that complex structures bring associated governance complexity and risk. Inadvertent non-compliance is more likely because there may not be clear delineation in the oversight of each entity, including the required focus on each charity's particular charitable purpose.

'At the rarer and more extreme end, we are concerned about entities that may deliberately use complex corporate structures to try and obscure illegal activities. Our enforcement and compliance activities will focus on charities that attempt to conceal non-compliance with the ACNC Act and Regulations by deliberately using complex structures to avoid adherence to the law [...].

'We will also continue to refer matters to other appropriate government agencies when we have concerns about suspected breaches of other laws.'

Another compliance focus will be the challenges charities face on cyber-security.

'This is a key governance risk for charities', Ms Woodward said.

'In our reviews we work with charities to better understand how they protect themselves from cyber risks and manage cyber-security incidents.'

The ACNC will look at cyber-challenges faced by charities by asking:

- What makes charities vulnerable to cybercrime
- How charities manage and mitigate cyber security risks, and
- How charities ensure third parties manage risk on their behalf.

Ms Woodward said that the ACNC will maintain a focus on conduct that poses the greatest risk to people, funds and assets.

'Consistent with our statutory objectives, we take enforcement action when there is a significant risk to public trust and confidence in registered charities.'

The ACNC will prioritise:

- Conduct that harms people, particularly children and vulnerable adults
- Misuse of a charity for terrorist purposes or to foster extremism, indirectly or directly
- Financial mismanagement, including fraud and significant private benefit, and
- Activities that put a charity at risk of having a disqualifying purpose so they are no longer eligible to be registered with the ACNC.

ACNC aims for more transparency

The ACNC aims to publish more information about its regulatory and compliance activities to improve transparency and educate the charity sector.

Its Secrecy Reforms Project will use examples from real life, the identities of entities involved hidden.

A registration-decision summary, for instance, outlines an application for charity registration by an organisation that was structured as a proprietary company limited by shares.

A second summary outlines key factors that the commission considers in determining an organisation's eligibility to be registered as a charity.

A charity with a purpose of relieving what are known as 'necessitous circumstances' will be entitled to registration with the subtype 'advancing social or public welfare', for instance.

Simple checks to meet compliance obligations

Important checks ensure that charities meet their obligations, the ACNC says.

Charities should be aware of their reporting obligations and when reporting is due.

Addresses should be up-to-date. They are where ACNC correspondence is sent, including reminders to submit annual information statements.

Charities should inform the commission of any changes to the names and positions of those who run them, the responsible people. They include directors, committee members, and trustees. They need to have access to charity portals.

Charities should notify the commission about changes to governing documents and submit revised copies via the portal. Your charity may also need to notify other agencies of any changes, such as state or territory regulators.

ACNC lists charities operating overseas

The ACNC's Charity Register has a new feature listing Australian-registered charities that operate programs overseas.

The list aims to connect donors, volunteers, and philanthropists with thousands of organisations that operate programs internationally.

The *Australian Charities Report* says that six per cent of Australian-registered charities operate in other countries, the five most common being India, Cambodia, the Philippines, Indonesia, and Kenya.

The change builds on enhancements made in previous years, such as the ability to look up charities based on the types of programs and services they deliver. These enhancements help users find registered charities to support based on their interests, such as housing or education, and the ability to search for a charity working in your preferred location, anywhere in Australia.

NDIS

NDIS cracks down on overcharging

A new taskforce will crack down on unfair price hikes for National Disability Insurance Scheme participants.

The ACCC will run the body with the NDIS Quality and Safeguards Commission and the National Disability Insurance Agency.

The ACCC will focus on investigating and clamping down on misleading conduct, unfair contract terms, and anti-competitive agreements that might impact NDIS participants.

Every NDIS participant, their carers, guardians, and nominees, will receive a letter explaining their rights and how to counter the NDIS 'wedding tax' – where prices are increased just because someone joins the scheme.

'Charging you more just because you are simply an NDIS participant is wrong and it is a breach of federal law', said NDIS minister Bill Shorten.

'We have upgraded the NDIS rules to make it clear overcharging is prohibited and we have further legal changes coming to more strongly prohibit and punish such practices.'

The NDIS commission can impose severe penalties for breaches of disability law. They include permanent banning, infringement and compliance notices, civil financial penalties and/or injunctions, and, where fraud is suspected, urgent referral to the fraud-fusion taskforce for criminal sanctions.

'The ACCC will remain a tough cop on the beat, with additional resourcing to take action against providers who breach the existing consumer-protection laws', said assistant minister Andrew Leigh.

'When you are on the NDIS you have a legal right to pay a fair and reasonable rate and not be subjected to price hikes. You also have a right not to be pressured into buying a support or service you don't want or need.'

Australia

Adelaide Office
Level 3, 153 Flinders Street, Adelaide SA 5000
GPO Box 2163, Adelaide SA 5001
p +61 8 8139 1111, f +61 8 8139 1100
receptionSA@nexiaem.com.au

Brisbane Office
Level 28, 10 Eagle St, Brisbane QLD 4000
p +61 7 3229 2022 , f +61 7 3229 3277
email@nexiabrisbane.com.au

Canberra Office
Level 5, 17 Moore Street, Canberra ACT 2601
GPO Box 500, Canberra ACT 2601
p +61 2 6279 5400, f +61 2 6279 5444
mail@nexiacanberra.com.au

Darwin Office
Level 2, 80 Mitchell Street, Darwin, 0800
p +61 8 8981 5585 f +61 8 8981 5586
receptionNT@nexiaem.com.au

Melbourne Office
Level 35, 600 Bourke St, Melbourne Vic 3000
p +61 3 8613 8888, f +61 3 8613 8800
info@nexiamelbourne.com.au

Perth Office
Level 3, 88 William Street, Perth WA 6000
GPO Box 2570, Perth WA 6001
p +61 8 9463 2463, f +61 8 9463 2499
info@nexiaperth.com.au

Sydney Office
Level 22, 2 Market Street, Sydney NSW 2000
PO Box Q776, QVB NSW 1230
p +61 2 9251 4600, f +61 2 9251 7138
info@nexiasydney.com.au

New Zealand

Auckland Office
Level 1, 5 William Laurie Place, Albany Auckland 0632
p +64 9 414 5444, f +64 9 414 5001
office@nexiaauckland.co.nz

Christchurch Office
Level 4, 123 Victoria St, Christchurch
p +64 3 379 0829, f +64 3 366 7144
office@nexiachch.co.nz

www.nexia.com.au