9TH MIND
ADVISORY

STRENGTHENING CYBER RESILIENCE FOR AUSTRALIAN NON-PROFITS AND CHARITIES

A Strategic Approach

INTRODUCTION

In an era of escalating cyber threats, non-profit organisations in Australia are facing a unique set of challenges in securing sensitive data and maintaining compliance – all whilst continuing to watch the pennies and deliver critical services that matter to their communities. Non-profits are increasingly becoming targets of cyber crime and must step up to improve their resilience and ability to safeguard their customers, partners and supporters.

The sophistication and cost of cyber-crime against Australians is steadily increasing. In the Australian Government's 2023–2030 *Australian Cyber Security Strategy*[1] document, The Hon. Clare O'Neil MP, Minister for Home Affairs & Cyber Security, reflects on the Australian Signals Directorate's (ASD) estimate of a staggering $3bn per year[2] cost of cyber crime to the economy, highlighting the critical challenges facing Australian companies and citizens today.

The research indicates that non-profits, charities and healthcare organisations are increasingly becoming targets for cyber criminals and that the estimated cost impact of such attacks is also on the rise. Additionally, *The Australian Non-profits State of the Sector 2023*[3] report reveals that 8% of survey participants admitted to being affected by a cyber security incident in the past year.

To mitigate increasing cyber risks and to ensure the continued success of our non-profit and charitable sector, we need to recognise the pressing need for these organisations to enhance their cyber security posture without negatively impacting on their core missions – keeping in mind that, often, those missions impact lives, living standards and health of everyday Australians. To address these challenges successfully, non-profit sector organisations need help to urgently bridge the gap between IT and business stakeholders, and to address cyber security as a whole-of-business challenge. This gap is currently placing many organisations at unacceptable risk of becoming the next front-page story. For those who do not already have a comprehensive cyber security strategy tailored to the specific needs of their organisation, this should become a priority business action in 2024.

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
[2] https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
[3] https://www.uwa.edu.au/schools/-/media/Centre-for-Public-Value/Resources/230906-State-of-the-Sector-Report.pdf

In this introductory article, we address the cyber security context of the non-profit landscape in Australia and provide practical suggestions for getting started or bolstering your organisation's business driven strategy for combatting cyber security threats in 2024.

Why the Non-Profit Sector is Increasingly Targeted

A common perception in the non-profit sector and in the broader community is that organisations 'doing good' in the community would not be targets for cyber criminals. However, this is simply not true. Research into cyber crime shows a clear trend towards increasing focus on the non-profit sector due to a number of factors, which are somewhat of a *perfect storm*. Many such organisations often deal with highly sensitive personal data, enjoy a high level of trust and strong emotional ties with the communities that they serve. Coincidently, these same organisations often suffer from a general lack of funding for infrastructure spending and cyber security skills availability. These factors can impact a non-profit organisation's ability to stay on top of and counter cyber threats which, in turn, expose them to a particular set of emotionally charged vulnerabilities able to be exploited by cyber criminals. Indeed, rather than sympathising with an organisation's social mission and benefit, when cyber criminals target non-profit organisations, they see an opportunity to exploit data vulnerability and to apply significant pressures on the compromised organisation, due to the emotional connection to data, to force a reaction in the criminals' favour.

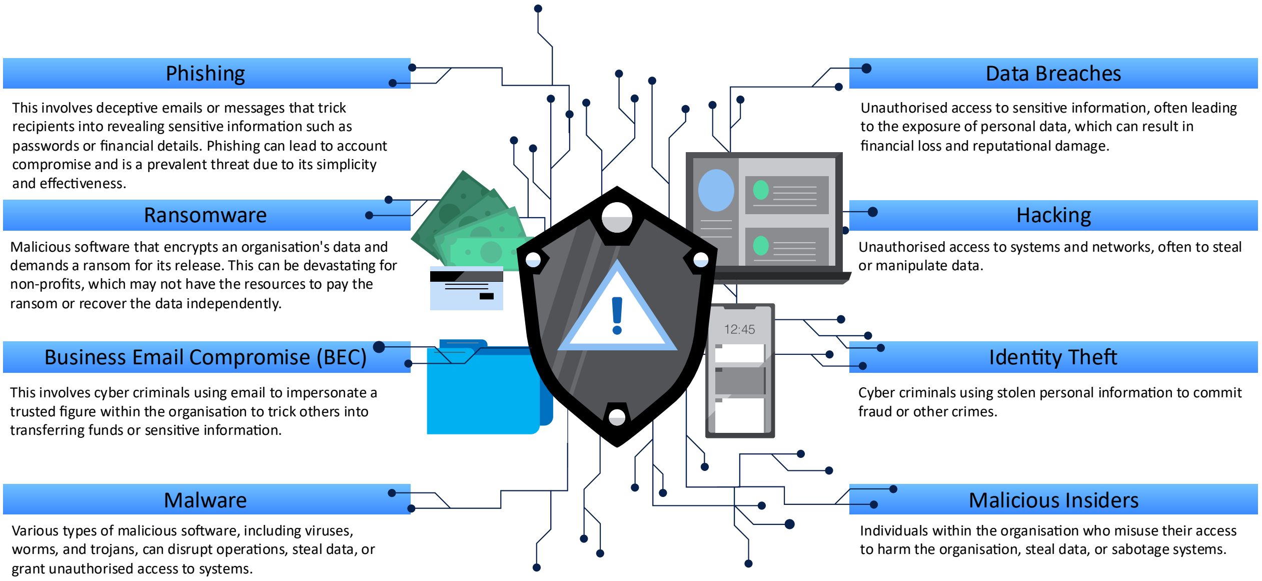
If you think this through, a likely potential scenario could involve a non-profit that deals in sensitive personal health data being targeted by cyber criminals who demand a ransom knowing that the emotional manipulation they can exert is likely to put significant pressure on the organisation to pay their ransom or risk significant fall-out from the data theft and reputational damage that inevitably follows. Clearly, exposure of such personal information would be incredibly damaging for the organisation and subsequent costs of recovery, damage control and reassurance may well be too great for the organisation to survive – not to mention the brand damage that can occur due to supporters and donors feeling that they no longer wish to support an organisation that has been hacked.

If that hypothetical organisation hasn't prepared itself for how to handle such an incident, isn't sure what their legal obligations are in dealing with a ransom attack, and has to scramble to even begin to understand the potential impact, we can be sure that the pressure on the organisation to respond is something that the cyber criminals will try to exploit and increase in order to increase their chances of having their demands met.

Emotional connection to data, time-pressures and the threat of the unknown are aspects that are likely to work in favour of the cyber criminals – therefore, having a response plan and working through attack scenarios in advance, is critical for all organisations.

Another aspect non-profit organisations need to consider is the accountability they have towards their supporters and their clients in ensuring that their spend on IT and cyber security is both proportionate and appropriate to their brand values and community. Spending significant amounts on cyber security may well protect an organisation from undue risk, but over-spending in this area may well be as detrimental to an organisation as tone-deaf overspending on luxurious office facilities and travel. Non-profits operate in a somewhat ‘Catch-22’ situation, where they desperately need access to enterprise grade cyber security capabilities whilst also being accountable for ensuring that their investment is both proportionate and effective, representing good value to their customers, supporters and stakeholders.

COMMON TYPES OF CYBER THREATS



Phishing

This involves deceptive emails or messages that trick recipients into revealing sensitive information such as passwords or financial details. Phishing can lead to account compromise and is a prevalent threat due to its simplicity and effectiveness.

Ransomware

Malicious software that encrypts an organisation's data and demands a ransom for its release. This can be devastating for non-profits, which may not have the resources to pay the ransom or recover the data independently.

Business Email Compromise (BEC)

This involves cyber criminals using email to impersonate a trusted figure within the organisation to trick others into transferring funds or sensitive information.

Malware

Various types of malicious software, including viruses, worms, and trojans, can disrupt operations, steal data, or grant unauthorised access to systems.

Data Breaches

Unauthorised access to sensitive information, often leading to the exposure of personal data, which can result in financial loss and reputational damage.

Hacking

Unauthorised access to systems and networks, often to steal or manipulate data.

Identity Theft

Cyber criminals using stolen personal information to commit fraud or other crimes.

Malicious Insiders

Individuals within the organisation who misuse their access to harm the organisation, steal data, or sabotage systems.

Figure 1: Common types of cyber threats that organisations need to defend against

Understanding the Challenges

Non-profits and charities shoulder the responsibility of safeguarding highly sensitive personal and health-related data, the sensitivity of which is often akin to that of data held by financial institutions. However, due to their very nature, they tend to operate with significantly constrained budgets, limited resources, and a workforce often stretched thin across numerous programmes. Balancing risk, compliance, and strategy while staying true to their core mission often proves to be a formidable challenge.

The sector's complexity is further exacerbated by significant compliance and governance requirements often across disparate data types that each have their own compliance obligations, toolsets, and teams - all of which can lead to an overwhelming volume of security controls and significant management overhead. Prioritising these controls becomes a critical business challenge, necessitating a pragmatic approach to cyber security, whilst the organisation does its best to fulfil its actual mission.

As work continues by the Australian Government to shape up its cyber security strategy, warning bells are sounding about the likelihood of cyber security measures becoming highly monitored responsibilities of board members and that, in time, direct professional and personal liabilities are likely to become the norm. Whilst these policy decisions are being formed, there is an opportunity for forward-thinking non-profits and charities to get a head start on their inevitable cyber security journey and to take a pro-active approach to protecting their critical data and ability to recover in the event of a cyber incident.

Industry Sector Cyber Security Perspectives

The Australian charity sector's contribution to the economy includes **$190 billion** in revenue, **$422 billion** in assets and employs **10.5% of the workforce.**

- Data from the Australian Charities Report - 9th Edition, published by the Australian Charities and Not-for-Profits Commission, 2023 [1]

"With stewardship of sensitive member, client and donor data, and the need to manage the potential, human, financial and reputational damage of data breaches, cyber security is an increasing priority of NFPs. Recent high profile data breaches have affected some of Australia's largest charities, including several universities. Despite this, across the sector, workforce cyber security skills continue to rank as relatively low priorities for organisational leaders (Price Waterhouse Coopers 2022) and lack of budget is a major reason why many NFPs do not have information security policies in place (Infoxchange 2022). This is a problem both for the sector itself, and where sector organisations interact across sectors as part of industry and service networks."

- Blueprint Expert Reference Group – Developing a Not-for-Profit Sector Development Blueprint – Issues paper[2]

"The board's role is to oversee thorough and comprehensive planning for significant cyber security incidents. Response plans should be rigorously tested at all levels – from operations and management through to leadership and the board."

- Governing Through a Crisis., the Australian Institute of Company Directors (AICD)[3]

"For all boards, cyber security and cyber resilience must be top priorities. ASIC also expects this to include oversight of cyber security risk throughout the organisation's supply chain. Failure to ensure adequate measures are in place exposes directors to potential enforcement action by ASIC based on the directors not acting with reasonable care and diligence."

- Australian Security and investment Commission (ASIC) Chairman, Joe Longo's comments at The Australian Financial Review Cyber Summit, 18 September 2023.[4]

Sources:

[1] https://www.acnc.gov.au/tools/reports/australian-charities-report-9th-edition

[2] https://engage.dss.gov.au/blueprint-expert-reference-group-developing-a-not-for-profit-sector-development-blueprint/blueprint-expert-reference-group-developing-a-not-for-profit-sector-development-blueprint-issues-paper/

[3] https://www.aicd.com.au/content/dam/aicd/pdf/news-media/research/2024/governing-through-a-cyber-crisis-280324.pdf

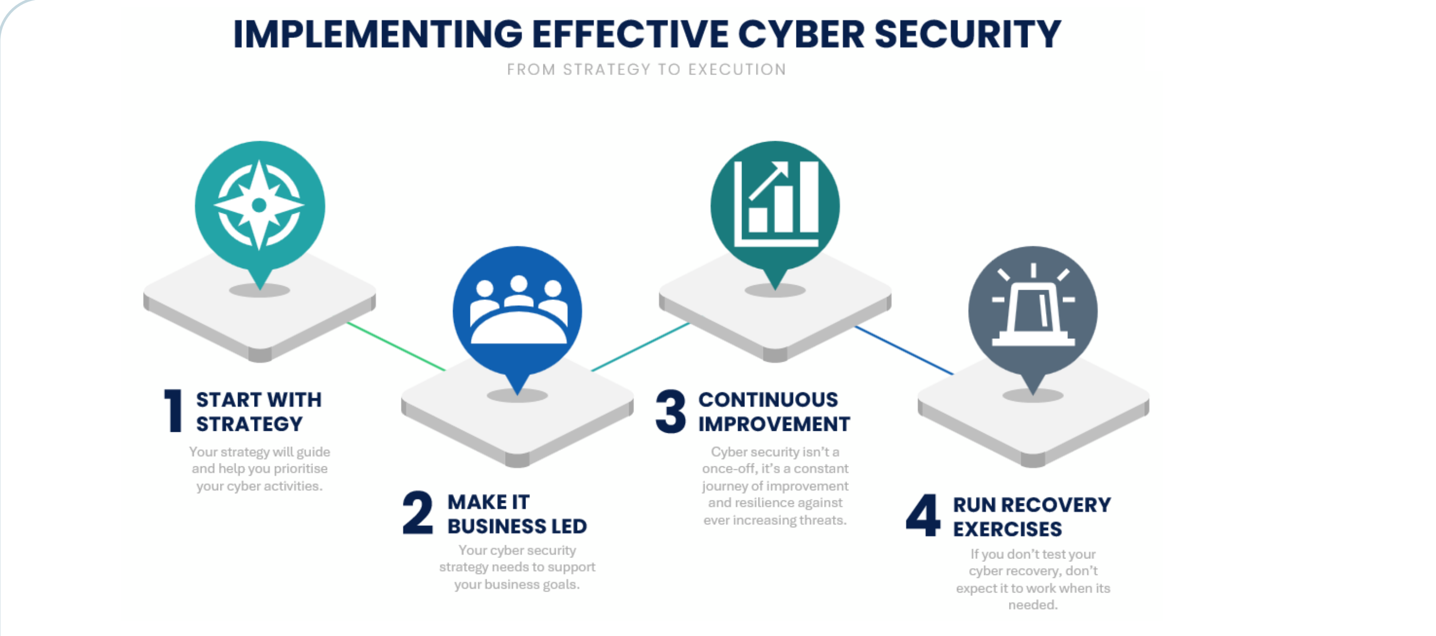
[4] https://asic.gov.au/about-asic/news-centre/speeches/marconi-s-illusion-what-a-120-year-old-magician-s-trick-can-teach-us-about-cyber-preparedness/

From the above sampling, it can be observed that there is a clear trend towards increasing obligations and scrutiny of board members to become directly accountable and involved in shaping and driving their organisation's cyber security strategy. Australia's non-profits and charities need to be able to meet these obligations confidently, whilst seeking approaches that help them achieve a high level of cyber security resilience and not impacting their ability to operate effectively.

Take a moment to reflect on a scenario relevant to your organisation, where in a hypothetical incident, the organisation suffers a cyber breach, and criminals encrypt all data essential for delivering the organisations entire set of services. Imagine staff arriving at work only to find themselves unable to access critical case files, lacking even basic contact information for who to call, halted in their duties until systems can be restored (assuming they are able to be). Imagine the people dependent on those services and what impact could arise as a result. Conversely, consider an organisation that, recognising the potential impact of such cyber threats, embarks on a strategic cyber resiliency program to assess risks, plan for recovery scenarios and practises data recovery. Striking the appropriate balance between robust cyber security measures and manageable operational costs is a paramount challenge for non-profits and charities, requiring a considered strategic approach to navigating potential pitfalls.

A Pragmatic Approach to Cyber Security Readiness for Non-Profits

As the threat landscape continues to evolve, understanding your organisation's current cyber security position is crucial for mitigating risks effectively. You do not need to be a cyber security expert; what matters is realising that you have a leadership responsibility and the commitment to ensuring that your non-profit or charitable organisation remains resilient against potential cyber threats. For non-profit organisations that are yet to make inroads on their cyber security journey, the following section provides some practical and pragmatic starting points that can help you uplift your cyber maturity and maximise the impact from your existing and future investments.



IMPLEMENTING EFFECTIVE CYBER SECURITY

FROM STRATEGY TO EXECUTION

1 START WITH STRATEGY

Your strategy will guide and help you prioritise your cyber activities.

2 MAKE IT BUSINESS LED

Your cyber security strategy needs to support your business goals.

3 CONTINUOUS IMPROVEMENT

Cyber security isn't a once-off, it's a constant journey of improvement and resilience against ever increasing threats.

4 RUN RECOVERY EXERCISES

If you don't test your cyber recovery, don't expect it to work when its needed.

Figure 2: A practical and pragmatic approach to implementing effective cyber security starting with a clear strategy.

1. Start With Strategy

Many organisations have a variety of IT, cyber security, and resiliency projects underway at any point in time - the larger the organisation, the more complex these initiatives can be. When every cent spent on IT systems counts, it is even more critical that non-profit organisations ensure they maximise the impact from spending on cyber security and achieve tangible benefit from these initiatives. Establishing a robust cyber security strategy aligned to the business objectives is a clear indicator of forward-thinking organisations. Think of your cyber security strategy as your organisation's roadmap for where it is heading, the major stops along the way, and why it is doing the things it is doing. Without a strategy to guide your various activities and investments, your team is likely just guessing at where they're heading without any clear direction or assurance that you're even doing the right things – let alone that all the bases are covered. A good strategy ensures that all cyber security activities are aligned, delivering benefit, and contributing towards your business goals being realised. Additionally, it's always a good idea to regularly step out of the day-to-day focus and take time to complete strategy health checks to ensure that the various in-flight projects and teams can be validated or course-corrected as needed – after all, your business and your customers are relying on it.

2. Empower Your Business to Drive its Cyber Security Initiative

If your organisation defers all cyber security solely to IT teams, you may have a solid technical approach to incidents but are potentially leaving the organisation open to risks relevant to your business that haven't been assessed or planned for. This is a common pitfall – whilst there is undoubtedly a significant IT component, cyber security is fundamentally a business risk issue and needs to be dealt with as such. The business needs to think about its purpose, its customers, the data that it handles and needs to balance the requirements for cyber security against its needs to serve its stakeholders – be they customers, partners, employees or institutions. All cyber security initiatives should ultimately roll up to an educated and informed risk stakeholder with ultimate accountability. The more support and engagement they have from other business leaders, the better. All board members have a remit to ensure the organisation's success, so should be encouraged to engage with key decision-makers to understand the strategic alignment of cyber security with broader business goals. Remember, you are not expected to be a cyber security expert, but simply to take the topic seriously. Then engage and ask questions until you are confident that your organisation is ready and prepared to respond to potential cyber threats successfully.

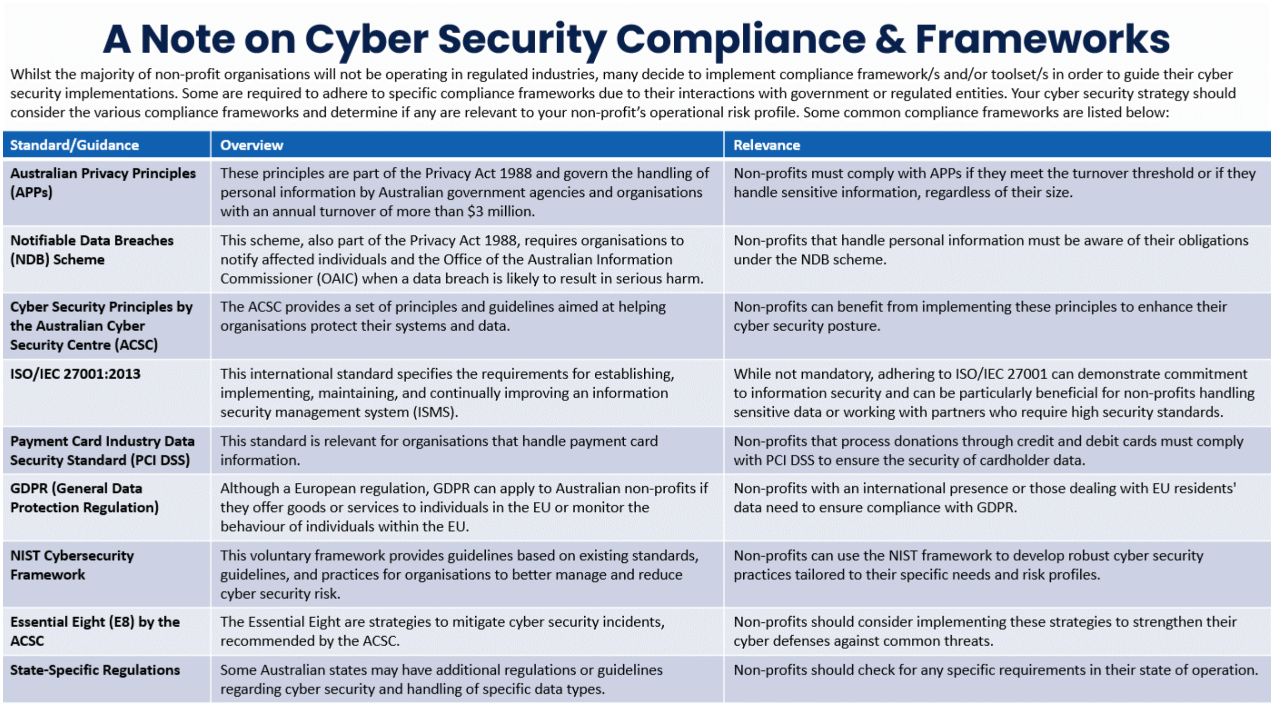
3. Adopt a Continuous Improvement Mindset

If your organisation perceives cyber security as an isolated activity conducted as a *one-off*, it is likely approaching the problem incorrectly. A strategic cyber security focus demands a commitment to continuous improvement, evolving alongside the ever-changing threat landscape and learning from simulations, industry experts and peers, as well as real life incidents. The key here is *learning* – the best prepared organisations have a business-led strategic program in place that clearly articulates their approach to cyber security, along with a documented and tested plan of action that can and will be followed in the event of an incident. They may never need to implement that plan, but if they ever do, they are in a good position to recover their operations successfully. So, don't wait for an incident to occur, inquire about your organisation's cyber security strategy now. Take a pro-active approach to finding out if and how it is tested and strengthened through learning activities such as simulations and drills. Actively participate in identifying potential gaps and areas where unnecessary risks might exist. Some of the best examples of engaged and pro-active board members are those who may only know the basics of cyber security but are persistent in demanding definitive responses in *plain-English* – and have the confidence to ask further questions to clarify any bamboozling technical responses.

4. Conduct and Plan for Regular Cyber Recovery Simulation Exercises

Assessing your organisation's current ability to recover in the event of a cyber-attack, data theft, or ransomware incident is paramount. Despite the recent cyber-crime headlines, many Australian organisations are still unprepared, relying on luck rather than a well-defined and structured recovery plan. Each organisation needs to factor into their cyber strategy a regular cadence for conducting detailed recovery readiness assessments (remember, cyber security is a journey, not a destination). Gauge your organisation's readiness by asking critical questions about things like how recovery data and passwords are managed, how up to date documentation for system restoration procedures is, and what incident response protocols exist. Understand the steps your organisation has in place today that will be implemented to ensure a swift and effective recovery in the event of an incident. Recent headline grabbing victims of cyber-crime would attest to the fact that the best time to discover the gaps in your recovery capabilities is *not* during a cyber crisis.

To summarise, boards members can no longer leave cyber security in the hands of their IT teams and hope for the best outcome. They need to be involved – both in advance, in setting cyber security policy, decision-making and testing response capabilities. Additionally, they need to be accessible for notification and for supporting incident management teams to navigate and respond to any significant cyber security incident as soon as it arises.



A Note on Cyber Security Compliance & Frameworks

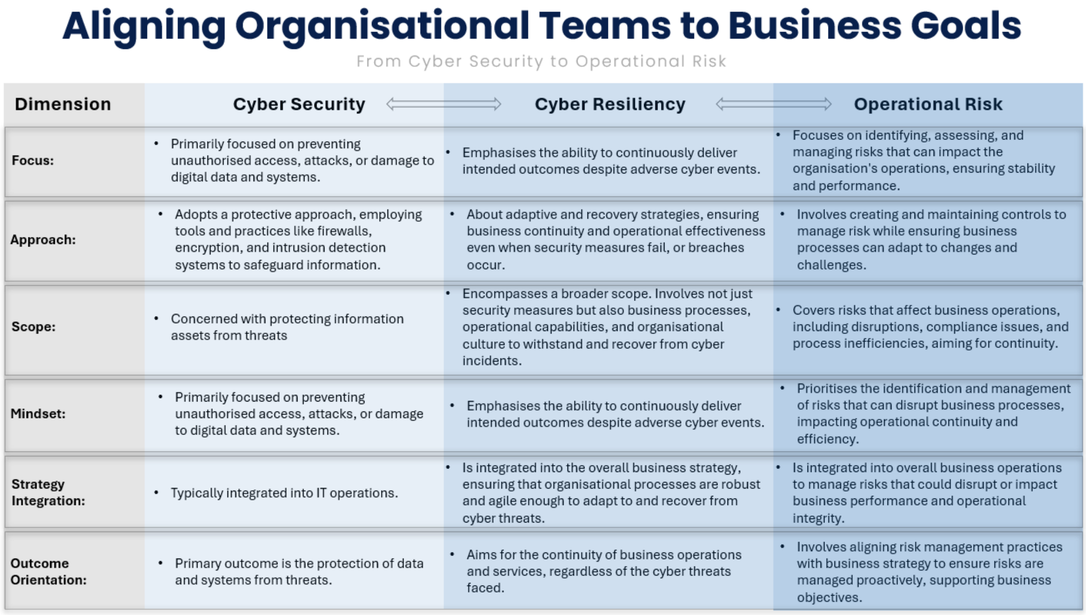
Whilst the majority of non-profit organisations will not be operating in regulated industries, many decide to implement compliance framework/s and/or toolset/s in order to guide their cyber security implementations. Some are required to adhere to specific compliance frameworks due to their interactions with government or regulated entities. Your cyber security strategy should consider the various compliance frameworks and determine if any are relevant to your non-profit's operational risk profile. Some common compliance frameworks are listed below:

Standard/Guidance	Overview	Relevance
Australian Privacy Principles (APPs)	These principles are part of the Privacy Act 1988 and govern the handling of personal information by Australian government agencies and organisations with an annual turnover of more than $3 million.	Non-profits must comply with APPs if they meet the turnover threshold or if they handle sensitive information, regardless of their size.
Notifiable Data Breaches (NDB) Scheme	This scheme, also part of the Privacy Act 1988, requires organisations to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm.	Non-profits that handle personal information must be aware of their obligations under the NDB scheme.
Cyber Security Principles by the Australian Cyber Security Centre (ACSC)	The ACSC provides a set of principles and guidelines aimed at helping organisations protect their systems and data.	Non-profits can benefit from implementing these principles to enhance their cyber security posture.
ISO/IEC 27001:2013	This international standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).	While not mandatory, adhering to ISO/IEC 27001 can demonstrate commitment to information security and can be particularly beneficial for non-profits handling sensitive data or working with partners who require high security standards.
Payment Card Industry Data Security Standard (PCI DSS)	This standard is relevant for organisations that handle payment card information.	Non-profits that process donations through credit and debit cards must comply with PCI DSS to ensure the security of cardholder data.
GDPR (General Data Protection Regulation)	Although a European regulation, GDPR can apply to Australian non-profits if they offer goods or services to individuals in the EU or monitor the behaviour of individuals within the EU.	Non-profits with an international presence or those dealing with EU residents' data need to ensure compliance with GDPR.
NIST Cybersecurity Framework	This voluntary framework provides guidelines based on existing standards, guidelines, and practices for organisations to better manage and reduce cyber security risk.	Non-profits can use the NIST framework to develop robust cyber security practices tailored to their specific needs and risk profiles.
Essential Eight (E8) by the ACSC	The Essential Eight are strategies to mitigate cyber security incidents, recommended by the ACSC.	Non-profits should consider implementing these strategies to strengthen their cyber defenses against common threats.
State-Specific Regulations	Some Australian states may have additional regulations or guidelines regarding cyber security and handling of specific data types.	Non-profits should check for any specific requirements in their state of operation.

Table 1: An introductory overview to common compliance frameworks and standards

Aligning Differing Business Priorities Around Operational Risk and Cyber Security

One of the most significant challenges for organisations to address concerning cyber security is to think about the topic as a *whole-of-business* focus and to ensure that the business, *rather than IT,* owns and leads the response. IT teams are critical partners in delivering cyber security, but their skills, advice and efforts form one vital part of the organisation's comprehensive response to cyber security. A whole-of-business approach means that the various parties concerned with aligning cyber security, cyber resiliency and operational risk with business goals no longer operate in silos and work together with a common purpose to implement measures appropriate to the organisation's needs. Each business will assess and articulate its appetite for risk versus its need to operate and conduct necessary business activities, and this will in turn guide cyber security and resiliency practises. There are further opportunities to be derived from a joined up cyber security and operational risk approach, such as capability redesign, supplier assessment and maturity and internal teams' skills uplift.



Aligning Organisational Teams to Business Goals

From Cyber Security to Operational Risk

Dimension	Cyber Security	Cyber Resiliency	Operational Risk
Focus:	• Primarily focused on preventing unauthorised access, attacks, or damage to digital data and systems.	• Emphasises the ability to continuously deliver intended outcomes despite adverse cyber events.	• Focuses on identifying, assessing, and managing risks that can impact the organisation's operations, ensuring stability and performance.
Approach:	• Adopts a protective approach, employing tools and practices like firewalls, encryption, and intrusion detection systems to safeguard information.	• About adaptive and recovery strategies, ensuring business continuity and operational effectiveness even when security measures fail, or breaches occur.	• Involves creating and maintaining controls to manage risk while ensuring business processes can adapt to changes and challenges.
Scope:	• Concerned with protecting information assets from threats	• Encompasses a broader scope. Involves not just security measures but also business processes, operational capabilities, and organisational culture to withstand and recover from cyber incidents.	• Covers risks that affect business operations, including disruptions, compliance issues, and process inefficiencies, aiming for continuity.
Mindset:	• Primarily focused on preventing unauthorised access, attacks, or damage to digital data and systems.	• Emphasises the ability to continuously deliver intended outcomes despite adverse cyber events.	• Prioritises the identification and management of risks that can disrupt business processes, impacting operational continuity and efficiency.
Strategy Integration:	• Typically integrated into IT operations.	• Is integrated into the overall business strategy, ensuring that organisational processes are robust and agile enough to adapt to and recover from cyber threats.	• Is integrated into overall business operations to manage risks that could disrupt or impact business performance and operational integrity.
Outcome Orientation:	• Primary outcome is the protection of data and systems from threats.	• Aims for the continuity of business operations and services, regardless of the cyber threats faced.	• Involves aligning risk management practices with business strategy to ensure risks are managed proactively, supporting business objectives.

Figure 3: Understanding and aligning the parties involved in effective cyber security risk mitigation is critical

Our Approach

9th Mind Advisory assists customers in the non-profit, charitable and healthcare sector to elevate their cyber security resilience to the highest levels whilst also being mindful of their need to ensure responsible and proportionate IT infrastructure expenditure. We achieve this by facilitating a more informed dialogue between IT and critical business stakeholders to clarify and clearly articulate the organisation's strategic cyber security needs in line with its operational risk framework. Facilitating this dialogue helps to bring business-centric strategic needs to the centre of the discussion and to align other initiatives under that strategy. With that clarity, our customers can better prioritise activities that build on their existing infrastructure and maximise the impact of any further investments. Customers can then establish a baseline for and work towards increasing the maturity of their cyber security capabilities.

Use of Strategic Toolsets to Manage Maturity

Many of our customers either operate in or interface with regulated industries, therefore much of our focus is on assisting them to understand, interpret and to comply with industry and regulatory frameworks that they are obligated to implement. Again, strategy is critical - our approach ensures that our customers can clearly articulate their cyber security strategies and subsequently manage their regulatory compliance obligations as a component of that strategic approach.

For organisations that have not already invested in a methodology for managing their cyber security regulatory compliance journey, we help them to assess several approaches to make this process as simple as possible and, importantly, to help them to adopt an approach that lets them update or add new regulatory frameworks easily in the future. This approach ensures that *achieving* compliance and *staying* compliant become part of the organisation's cyber security DNA.

Mitigating Risks

The risks of neglecting cyber security vulnerabilities for non-profits and charities are substantial, including potential damage to brand reputation, legal penalties, hindrances to critical service delivery, and operational disruption.

We hope the advice above proves helpful to many non-profit organisations so that we can all collectively raise the bar of cyber security across this vital sector. It is important to remember that each and every team member has a role to play in ensuring effective cyber security and that effective cyber security and resilience is not just a one-off job – it is a process of continuous improvement and the ability to adapt the organisation to protect itself against ever increasing cyber threats.

Getting Help

9TH Mind Advisory delivers cyber security strategy services to our customers in several ways, tailored to each organisation's needs. Some of our services include:

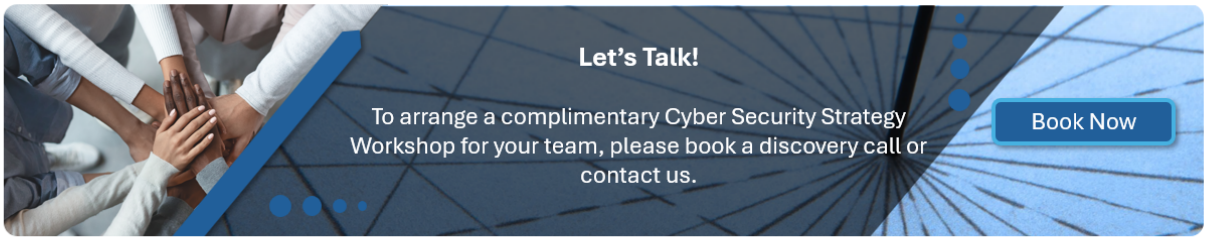
- Cyber Security Strategy Planning
- Cyber Simulation Exercises
- Supply Chain Assessment, Management & Uplift
- Fractional/Interim CISO
- CIO Agenda/Coaching
- Board Member Education
- SOCI, NIST Compliance

Take Action with 9th Mind Advisory Today

If you know you need to do something but don’t know where to start, book a discovery workshop with us today. Our workshops are designed to quickly bring clarity to your current position and provide recommendations about where you should focus your efforts to improve your cyber security posture and, importantly, how you can make pragmatic progress, more quickly. These workshops provide a significant amount of benefit on their own and are delivered at no charge to non-profit organisations.

Our workshop approach will also help you understand how an expanded, tailored activity could potentially benefit your organisation’s cyber security journey – we are confident that we can demonstrate the best approach for your organisation’s needs and show you the fastest route to making real progress.

We aim to work with customers who will benefit from strategic cyber security services, and we work hard to ensure that any engagement is highly efficient and delivers significant strategic value. We take cyber security seriously and work hard to ensure that our clients adopt the best possible cyber security strategies and practices appropriate to their needs.



Let’s Talk!

To arrange a complimentary Cyber Security Strategy Workshop for your team, please book a discovery call or contact us.

9TH MIND ADVISORY

At 9th Mind Advisory, we're committed to empowering businesses to discover, assess, mitigate, and manage cyber risks in today's rapidly evolving digital landscape. Our comprehensive services include cyber resilience consulting and advisory services, cyber recovery, innovative risk management and evaluation tools along with capabilities designed to help safeguard your organisation’s critical operations & services.

You can contact us at:

☎ 1300 432 956

✉ contact@9thmind.com.au

www.9thmind.com.au