convene

azeusconvene.com

WHITEPAPER

Navigating Cybersecurity Threats in Australian Boardrooms

TABLE OF CONTENTS

convene

NAVIGATING CYBERSECURITY THREATS IN AUSTRALIAN BOARDROOMS

In a business landscape where companies heavily depend on digital technologies, the significance of cybersecurity has never been more critical. Boards, traditionally responsible for strategic planning and corporate governance, now find themselves on the frontlines of defence against cybersecurity risks. This shift is essential because the board's responsibilities have expanded beyond financial and strategic concerns into the digital domain, where risks have escalated significantly.

STATE OF AUSTRALIA'S EVOLVING CYBER THREAT LANDSCAPE

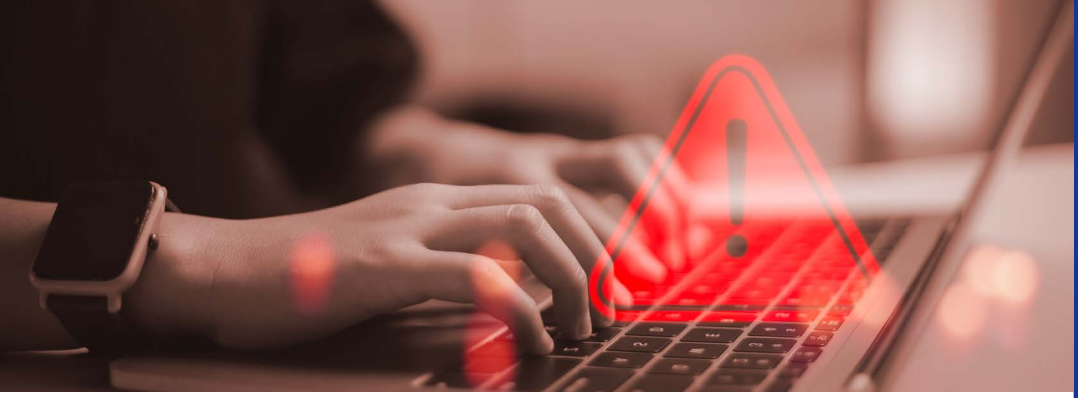
The cyber threat landscape is in a constant state of flux, setting forth a dynamic challenge for organisations worldwide. In Australia, cybersecurity risks are becoming increasingly sophisticated — with an average of 164 cybercrime reports in the country every day.

According to the Australian Cyber Security Centre's (ACSC) 2022 Annual Cyber Threat Report, cybercrime in Australia rose by nearly 13% from the previous financial year. Heightened cyber activities are also shown in the Cyber Security Industry Advisory Committee's (IAC) Annual Report 2022. The report found that Australia has been a lucrative hunting ground for cyber attacks, prompting the government to make cyber security a national priority.

In an effort to subdue this rising issue, the Australian government is enhancing cybersecurity frameworks for critical infrastructure and systems of national significance. Provision of cyber security advice and technical assistance will also be prioritised, cued by the $12.3 million expansion to ACSC's 24/7 cyber security hotline.

COMMON CYBERSECURITY RISKS FACED BY BOARDS

As boards navigate the complexities of the digital landscape, they encounter a host of IT security risks. Understanding such threats and their implications is paramount to steer organisations towards resilience and vigilance. Continue reading to learn about the most common corporate cybersecurity risks today.



DATA BREACHES AND PRIVACY CONCERNS

Data breaches and privacy concerns are pivotal issues for boards. Highlighting the urgency of such risk are high-profile incidents, like the 2019 Canva incident (wherein the Australian-based graphic design platform suffered a major data breach affecting about 4 million accounts) and the 2023 Latitude attack (involving 14 million loan customer records being stolen, making it one of Australia's biggest breaches in recent history).

Boards must understand that data breaches not only lead to financial losses but also erode trust and tarnish their organisations' reputations. Regulatory bodies typically impose hefty fines for data mishandling, intensifying the stakes.

INSIDER THREATS

Insider threats pose a distinct challenge to boards. Individuals initiating such attacks have intimate knowledge of an organisation's systems and can exploit classified information for malicious purposes. ACSC reveals that reasons for insider threats can include coercion, revenge, or an attempt for financial gain through intellectual property theft or espionage.

To promptly detect and mitigate insider threats, boards must implement robust access controls, employee training, and vigilant monitoring.

SUPPLY CHAIN VULNERABILITIES

Supply chain vulnerabilities have also become a major concern for organisations worldwide, particularly in Australia. According to PwC's 2023 Global Digital Trust Insights Survey, software supply chain threats are of much greater concern to Australian respondents (37%) than globally (26%).

With that in mind, exercising due diligence to evaluate supply chain security is essential for boards. This is also crucial for assessing the cybersecurity posture of vendors and partners. Developing incident response plans for supply chain security is also important to prevent such attacks.

THIRD-PARTY RISKS

Boards must recognise that their corporate cyber security posture is intertwined with third-party risk. Recent cases, like the recent breach at The Good Guys, an Australian electronics retailer, have shown how third-party vulnerabilities can expose organisations to significant risks.

The personal data of about 1.5 million of The Good Guys' customers was stolen when one of its third-party suppliers was hacked. Such breaches highlight the critical need for strict security measures and vetting of third-party suppliers.

RANSOMWARE ATTACKS

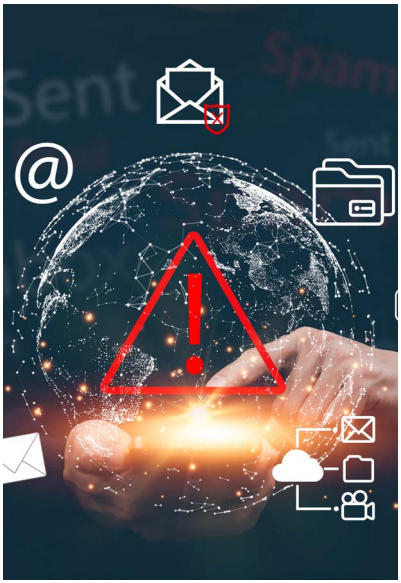
Ransomware attacks have evolved into a severe threat over the years. In 2021, the ACSC classified ransomware as the most destructive cybercrime threat in Australia. These attacks can paralyse organisational operations and lead to significant financial losses.

Considering the gravity of ransomware, boards are advised to allocate resources for incident response and disaster recovery planning. Regularly testing these plans and investing in security measures like email filtering and employee training are also vital for resilience.

ZERO-DAY EXPLOITS

Zero-day exploits are potent weapons in the hands of cyber adversaries. These attacks target vulnerabilities unknown to the software vendor or the public, making them particularly dangerous and challenging to defend against.

These attacks are called "zero-day" because there are zero days of protection against them; they strike before developers can create a patch or fix. The recent Barracuda ESG zero-day exploit, which hit the Australian Capital Territory Government, illustrated the speed at which these vulnerabilities can be exploited.



Boards must allocate resources to threat intelligence, vulnerability assessments, and proactive corporate cyber security measures. Regularly patching systems and implementing intrusion detection systems can also help reduce exposure to zero-day threats — enhancing overall security posture.

TOP CHALLENGES IN BOARDROOM CYBERSECURITY

Boards have become the frontline in the battle against cyber security risks for businesses. Concurrently, the challenges in addressing cybersecurity at the boardroom level have grown exponentially. Find out more about these below:

1. LIMITED TECHNICAL EXPERTISE AT THE BOARD LEVEL

The challenge here is that most board members come from diverse backgrounds without deep technical knowledge. This gap can hinder their ability to make informed cybersecurity decisions, potentially leaving the organisation vulnerable. To address this, boards should:

- **Invest in education** — Provide cybersecurity training and resources to board members so they can better understand the risks and solutions.
- **Appoint expert advisors** — Consider appointing cybersecurity experts or advisors to the board to provide guidance and insights.

2. BALANCING CYBERSECURITY INVESTMENT

Boards must delicately balance their cybersecurity investments with other strategic priorities and financial constraints. Allocating too little to cybersecurity can expose the organisation to risks while allocating too much can strain resources and affect profitability.

Boards need to work closely with the executive team to:

- **Assess risk appetite** — Boards should gauge the organisation's risk tolerance when it comes to cybersecurity. Understanding how much risk they are willing to accept helps in resource allocation decisions.
- **Do cost-benefit analysis** — Conducting thorough cost-benefit analyses can help prioritise investments. Such analyses evaluate the potential financial impacts of various cyber incidents and guide resource allocation accordingly.

3. INCIDENT RESPONSE PREPAREDNESS

Being prepared to swiftly respond to cyber incidents is imperative for boards. Cyberattacks are no longer a matter of "if" but "when." To ensure readiness, boards should:

- **Have a robust incident response plan** — The organisation should maintain a comprehensive incident response plan. This plan should delineate roles, responsibilities, communication protocols, and the precise actions to take during a cyber breach.
- **Conduct regular testing** — Regularly testing and simulating cyber incident scenarios help ensure the plan's practicality and the organisation's ability to respond effectively in real-world situations.

4. EMBEDDING CYBERSECURITY INTO STRATEGIC PLANNING

Historically, cybersecurity was often seen as a separate, technical issue, but has now become a business-critical concern. Boards must actively participate in discussions that explore how cybersecurity aligns with and supports the organisation's strategic goals. To achieve this integration, boards can take the following steps:

- **Evaluate cyber risks strategically** — This step is imperative for ensuring that the board understands the potential impact of cyber risks on the organisation. Utilising risk assessments can effectively guide its strategic direction and priorities.
- **Cultural integration** — Cybersecurity should be woven into the very fabric of the organisation's culture and daily operations. It should not be seen as a standalone department but as a core component of every business decision. This means integrating and addressing it in all business aspects, may it be through:

    - Creating cybersecurity policies
    - Providing regular cybersecurity training to employees
    - Conducting risks assessments
    - Implementing ongoing security awareness programs

5. FACILITATING CLEAR COMMUNICATION

The technical intricacies of cybersecurity often pose challenges in conveying complex cyber risks to board members. To foster a seamless exchange of information between cybersecurity experts and boards, consider the following:

- **Clear channels** — Establishing clear communication channels can make it easier to facilitate a smooth flow of information, as well as immediate clarification when needed.
- **Jargon-free reports** — Encourage boards to request and receive briefings and reports on cybersecurity matters free from technical jargon. These documents should simplify complex technical concepts into plain language—easily understood by everyone.
- **Open discussions** — Foster open and candid cybersecurity discussions among all members. This promotes transparency, mutual understanding, and effective decision-making in the boardroom.

Addressing such cybersecurity challenges isn't just a technical concern but a fundamental strategic imperative. That said, boards must continually adapt and evolve their cybersecurity approaches to safeguard their organisations in an ever-changing threat landscape.

CYBERSECURITY BEST PRACTICES THAT BOARDS SHOULD FOLLOW

As boards try to navigate through cyber threats, employing the best practices can help foster a resilient organisation.

Here are seven cybersecurity best practices to follow:

I. Understand cybersecurity's business impact

Understanding the business impact of cybersecurity threats is crucial for boards. Cyberattacks can have severe financial and reputational consequences. For instance, the global average cost of a data breach in 2022 was $4.35 million, a 2.6% rise from 2021.

Boards must recognise that cybersecurity isn't solely a technical issue; it directly affects the organisation's financial health and reputation. This is why boards should allocate sufficient resources and prioritise cybersecurity initiatives accordingly. A few ways to do so are:

- Conducting regular cybersecurity seminars and forums.
- Creating and reviewing cybersecurity reports, including projections of potential risks.
- Arranging periodic briefings with external cybersecurity experts.

II. Ask informed questions

Boards must be well-prepared to ask informed questions about cyber security risks for businesses. The current 8% surge in global weekly cyberattacks underscores the urgency of this preparedness. Examples of key questions include:

- **Where is sensitive board information stored?** — Understanding the storage locations of critical board information is paramount. Recent breaches have exposed vulnerabilities in data storage, making this question crucial.
- **Who has access to these confidential documents?** — With insider threats on the rise, knowing who has access to sensitive documents is essential. Research indicates that a considerable portion of breaches originate from within organisations.
- **What is our incident response plan in case of a data breach?** — Having a well-defined incident response plan is non-negotiable. In light of escalating cyber threats, an effective response plan can mitigate the impact of a breach.
- **How often do we assess the cybersecurity practices of our third-party vendors?** — Third-party vendors are often a weak link in cybersecurity. Regular assessments of their practices are crucial. Recent data reveals that many breaches are linked to vulnerabilities in the supply chain.

III. Employ a cybersecurity expert

Incorporating a cybersecurity expert into the board provides a competitive advantage. Such experts bring insights into emerging threats, best practices, and the latest cybersecurity technologies.

Some upskill their boards via cybersecurity education and training sessions with outside experts. Nonetheless, employing the help of such experts allows boards to make informed decisions and assess cybersecurity risk factors more accurately.

IV. Vet vendors thoroughly

Selecting the right digital solution vendors is a critical task for any company. A study found that 59% of organisations experienced data breaches due to third-party vendors. Focusing on cybersecurity due diligence can help mitigate these supply chain vulnerabilities. This involves assessing the vendor's security practices, certifications, and adherence to cybersecurity standards. Ask your would-be providers the following questions:

- What are the measures in place to preserve data integrity?
- Which third-party certifications do you have?
- How often are penetration tests performed to guarantee data protection?
- Where will our data be hosted, and what security measures are in place at the hosting location to safeguard our data?

Another critical aspect to look into is whether the vendor has undergone an Independent Registered Assessors Program (iRAP) assessment. This gives you insights into their adherence to the latest cybersecurity standards set by regulatory bodies. So before making a decision, be sure to ask potential vendors about their iRAP assessment status.

V. Regularly assess cybersecurity

Having a proactive approach to risk management is of utmost importance, and this can be demonstrated through routine cybersecurity assessment. This involves a thorough evaluation of the organisation's cybersecurity posture.

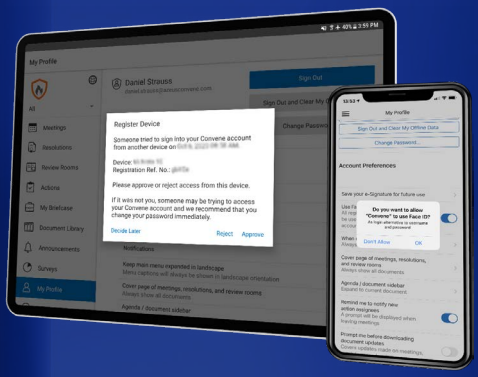
Boards can pinpoint vulnerabilities, weaknesses, and areas that require enhancement. By conducting regular assessments, boards gain insights into the evolving threat landscape. This then enables them to allocate resources judiciously to address the most immediate risks.

Lastly, remember that threat actors continuously develop new tactics. That's why it's critical for boards to execute ongoing cybersecurity education. This includes regular briefings or training, and staying updated with the best practices. Staying informed ensures boards can adapt to emerging threats and make informed decisions to enhance cybersecurity resilience.

CONVENE: UNRIVALED BOARD SECURITY SETS US APART

The relentless evolution of cyber threats demands vigilance. And with business operations and data under constant threat, boards must adapt swiftly to protect their organisations' interests. Notably, many are turning to board portals to fortify meetings and protect confidential data.

Introducing Convene, a leading board portal that places a premium on security and privacy. Its top-notch security standards offer robust support for board confidentiality and regulatory compliance. It also provides multi-layered security measures that act as a powerful deterrent against data breaches — significantly reducing the risk of unauthorised access.



Convene also boasts an impressive array of certifications and accreditations, including ISO 14001 for Environmental Management Systems, ISO 9001 for Quality Management Systems, SSAE16 Certification, CMMI-DEV Level 5, and its recent Independent Registered Assessor Program (IRAP) assessment.

convene

azeusconvene.com

iRAP Assessment of Convene: Ensuring Compliance with Australian Government Standards

In addition to its robust security features, Convene has undergone an iRAP assessment, ensuring compliance with the Australian Government's Information Security Manual (ISM). The evaluation validates our commitment to maintaining a high degree of security while meeting stringent cybersecurity standards set forth by the Australian government.

Why iRAP is critical for listed companies?

For listed companies, iRAP certification signifies adherence to the ISM controls and commitment to robust cybersecurity practices. Undergoing this assessment allows listed companies to validate the correct implementation and operation of security controls within their systems. Consequently, iRAP provides assurance that a company's digital assets are fortified against cyber threats, making it a trusted choice for secure business operations.

What does our iRAP Assessment say?

Conducted by an ASD-endorsed assessor, the evaluation shows that Convene's overall security posture is sound with strong coverage and alignment to the majority of ISM controls. Other highlights of our iRAP assessment include:

- *Our commitment to continuous compliance with Australian government standards* — notably, showing adaptability in aligning with updated ISM guidelines and enhanced data protection.
- *Our inheritance of security is from Amazon Web Services (AWS),* which has its own IRAP assessment. This provides Convene with a layered, more resilient security approach.

To experience Convene's top-tier boardroom security, contact our team now and book a demo!

Let's Get Started

Visit us at azeusconvene.com
today for your free trial.

sales@azeusconvene.com
azeusconvene.com

Contact Us

Australia:	+61 0431 395 477	+61 0421 072 206
New Zealand:	+61 0421 072 206	+64 4830 3496

convene

Azeus Convene is a multi-awarded and leading board portal solution used by boards of directors of FTSE 100, Fortune 500, financial institutions, governments, and non-profit organisations in more than 30 countries. Our innovative board meeting software gives you complete control over the entire meeting process and ensures good governance driven by security and accountability.

Accolades, Integrations, Affiliates and Partners