FINANCIAL SERVICES
DIRECTORS' BRIEFING
CYBER SECURITY
FY 2024/25 Q1

PUBLISHED JULY 2024

The Australian financial services industry is increasingly under threat from cyber attacks and is facing stricter regulatory action on its cyber security obligations.

Australian Financial Services Licence holders need to implement robust cyber risk management systems to protect sensitive financial data and comply with stringent regulatory requirements and market expectations.

TABLE OF CONTENTS

Word From Our CEO

The Australian finance sector faces escalating cyber threats, making robust cyber security and compliance with regulatory standards paramount. AFSL holders must prioritise cyber risk management to safeguard sensitive financial data, their reputation and adhere to ASIC's stringent requirements, ensuring resilience against both cyber attacks and regulatory penalties

JAMES ORR

Chief Executive - Law Wyze

What Is Your Reputation Worth?

As cyber threats escalate and regulatory scrutiny intensifies, Australian Financial Services Licence (AFSL) holders face mounting pressure to safeguard their digital assets and ensure compliance. Failure to do so not only risks significant financial penalties but also the potential erosion of client trust and long-term damage to the company's reputation.

Cyber security breaches have far-reaching consequences beyond immediate financial losses. They can undermine stakeholder confidence, lead to legal repercussions, and tarnish a brand's image.

Regulatory bodies like the Australian Securities and Investments Commission (ASIC) have made it clear that AFSL holders must implement robust cyber risk management systems.

To protect their reputation, the finance industry must proactively address cyber security risks. This involves not only complying with regulatory standards but also adopting best practices such as regular security assessments, employee training, and engaging with cyber security specialists.

A company's reputation is one of its most valuable assets. In an era where digital threats are ever-present, the cost of safeguarding this reputation through robust cyber security measures is an investment that AFSL holders cannot afford to overlook.

Word From Our LPD

AFSL holders have clear statutory obligations. It would be prudent for all businesses or organisations that are at risk from cyber attacks to ensure that adequate risk management systems are in place.

PAUL MURRAY

Legal Practitioner Director - Law Wyze

What's Your Risk?

The regulatory landscape for Australian Financial Services Licence (AFSL) holders is becoming increasingly stringent concerning cyber security obligations.

The Australian Securities and Investments Commission (ASIC) has hardened its regulatory stance towards enforcing these requirements, and recent Federal Court decisions underscore the severe consequences of non-compliance.

The implications of these legal actions extend beyond financial penalties. They serve as a critical reminder of the broader risks associated with inadequate cyber security measures.

Such risks include potential data breaches, loss of client trust, and long-term reputational damage. For AFSL holders, the cost of inaction or delayed action in addressing cyber security risks can be devastating.

To mitigate these risks, AFSL holders must prioritise comprehensive risk management strategies.

This includes engaging with cyber security specialists, conducting regular security assessments, and ensuring timely implementation of recommended measures.

Doing so not only complies with regulatory requirements but also helps to protect licence holders' clients' sensitive information and enhances their reputation.

Regulator Statements

ASIC Statements:

- AFS licensees must adequately manage cybersecurity risks as part of their licence obligations.
- Licensees must have adequate technological and human resources to provide the services covered by the licence.
- Adequate technological systems, policies and procedures should be in place to ensure sensitive consumer information is protected and to minimise the risk of consumer harm.
- ASIC will take enforcement action when an AFS licensee does not meet their obligations.

ASIC Strategic Committments:

"We will work to combat digitally enabled misconduct through active supervision of regulated entities to ensure robust cyber resilience and risk-management practices are in place. "

"Technology risks
Focus on the impacts of technology in financial markets and services, drive cyber and operational resilience practices, including within companies and financial market infrastructure, and act to address digitally enabled misconduct."

Source ASIC: ASIC's Corporate Plan for 2023–2027.

Regulator Action

2022-24 Court Action Brought by ASIC Against:

- **Lanterne Fund Services Pty Ltd:**
  The decision in *Australian Securities and Investments Commission v Lanterne Fund Services Pty Ltd*, handed down on 10 April 2024, was a case brought by ASIC against a holder of an Australian Financial Services Licence.

  Outcome: Civil penalties of $1.25 million imposed on Lanterne.

- **RI Advice:**
  The decision in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd*, handed down on 14 April 2022, was a case brought by ASIC against a holder of an Australian Financial Services Licence (AFSL).

  Outcome: RI Advice paid $0.75 million in costs to ASIC.

Insights:
The judge in the Lanterne case, Justice McEvoy, quoted approvingly from Justice Rofe's observations in the RI Advice case, "the Court's assessment of the adequacy of any particular set of cyber risk management systems will likely be informed by evidence from relevantly qualified experts in the field", highlighting the judicial expectation that businesses seek expertise.

The Lanterne decision also gives us a list of the systems that the Court noted were lacking. For the specific issue of risk management, these included: IT generally (whether internal or external); adequate IT or cyber security infrastructure; an IT resources or security management plan; a back-up disaster recovery protocol, and general compliance software.

AFSL holders have a clear statutory obligation. No cases have yet been determined on directors' duties regarding cyber security. It would be prudent nonetheless for all businesses or organisations that are at risk from cyber attacks to ensure that adequate risk management systems are in place.

Key Takeaways

- Businesses should consider how various statutory and common law obligations can require them to reasonably address cyber security.
- These decisions should be considered a strong warning against complacency or delay in addressing those matters.
- Senior executives and officers must be aware of their obligations to act or delegate.
- Regulators are committed to enforcing the obligations of organisations to mitigate cyber and digital security risks, through the courts where necessary.
- The need for organisations to obtain relevant advice and expertise has been consistently identified by the Court as the appropriate step for them to take in addressing this risk.
- Judgments aren't restricted to the parties involved, and set precedent that affects all businesses that may find themselves subject to the same legal requirements.

Australian Commercial Cyber Threats Increasing

Australian Mid-Market cybersecurity research conducted in March-April 2024 showed:

61%

of businesses have reported having experienced a cyber event or incident.

81%

of finance and insurance businesses that responded confirmed that a cyber incident had occurred

83%

of mid-market businesses have invested in cybersecurity measures and training in the last 24 months

The finance industry was the 4th highest cyber breach reporting industry after Federal and state government reported by the Australian Signals Directorate. Broader industry data showed:

+90%

of these incidents involved ransomware or other forms of restriction to systems, files or accounts.

41%

of data breaches involved malicious cyber actors exploiting valid accounts and credentials to access cloud services, local systems, or entire networks

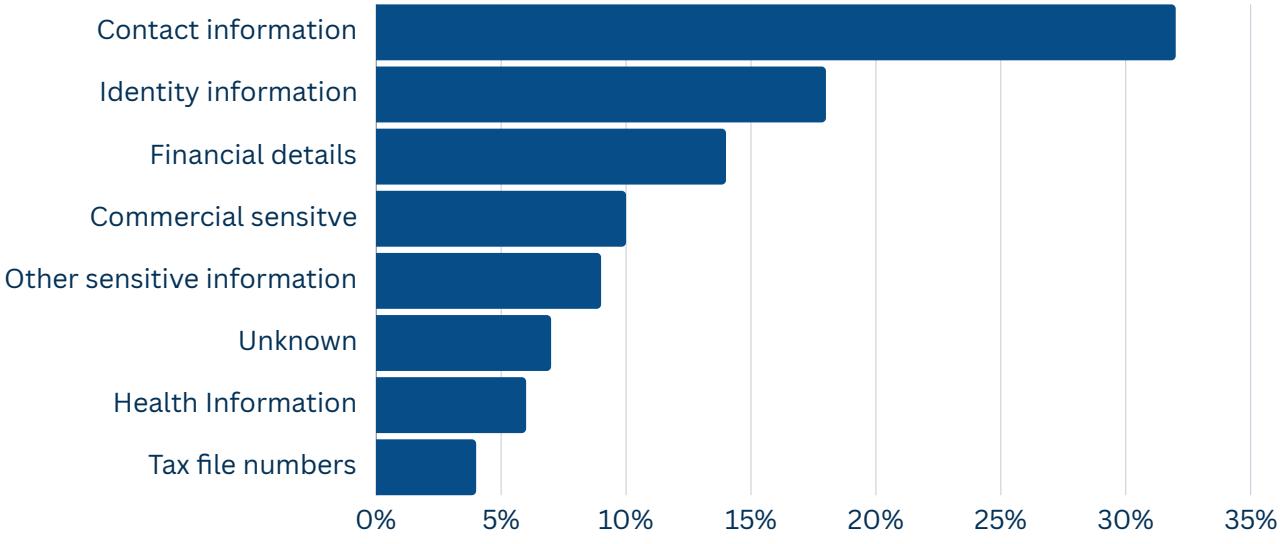
34%

of data breaches involved exploitation of internet-facing applications.

Australia's Mid-Market has seen heavy increases in cyber threat reporting, representing the largest average cost per incident of $97,203 as detailed by the latest ASD Cyber Threat Report .

3/5 Mid-market businesses reported in 2024's cyber survey having acknowledged a cyber incident had occurred previously within their business.

Top Information Types Exposed by a Data Breach in 22-23



Sources: Government & Industry research 2022-24 including the Australian Signals Directorate (ASD)

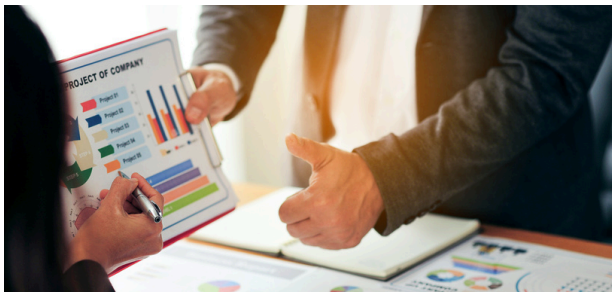
Budgeting for Success?

Cyber Security Budgeting

Cyber Security budgets developed in isolation of the corporate strategic agenda can fail to address the requirements of organisations.

We've gathered insights for the finance industries regarding their budget allocation as a percentage of revenue, and a further breakdown of the key focus areas for cybersecurity initiatives.

Strategy, talent and governance related activities dominate the focus of the finance industries which recognises the critical importance of cyber planning, expertise acquisition and aligned governance focus in ensuring cyber capabilities mitigate risk.



Cyber Security budget total was only 0.54% of commercial revenue in 2023

Finance Industry Investments in Cyber Security 2023	Total
Breakdown of Allocated Cyber Security Budget	
Emerging technologies + cloud	9%
Data protection & privacy	7%
Application	8%
Identity & access management operations	11%
Strategy, talent & governance	24%
Threat detection & response	16%
Infrastructure & network security	20%
Third-party security & Other	6%
	100%

Governance Steps to Address Cyber Risk

Taking active steps to prepare your organisation for immediate and ongoing cyber resilience and security capabilities can significantly mitigate the consequences of potential threats and ensure compliance with regulatory standards. The regulatory landscape for AFSL holders is becoming increasingly stringent, particularly concerning cyber security obligations.

Cyber GRC Legal & Compliance Advice

- Identify legal obligations to mitigate risk
- Design a Cyber GRC framework aligned to meet your business risk exposure and appetite
- Select appropriate cyber security framework
- 3rd party risk management obligations

Governance & Policy Development

- Adopt and integrate a cyber governance framework into commercial risk management practices
- Foster a cyber security culture through continuous improvement
- Deploy policies that guide operations every day

Incident Response and Business Continuity

- Privilege Protocols
- Media and communications
- Legal duties and notifications
- Data breach assessment
- Regulatory disclosures
- Data breach response measures
- Ransom response guidance
- Evidence preservation capabilities

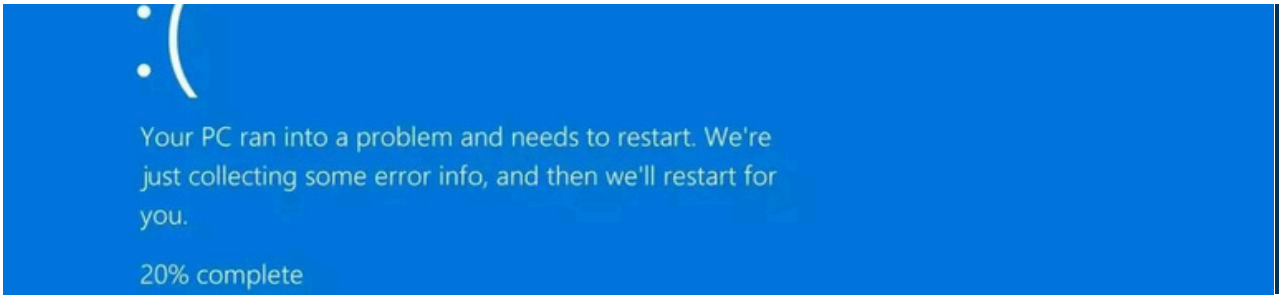
Training & Exercises

- Director and executive training
- Tabletop exercises
- Policy design and implementation
- Resilience strategy testing and validation

Business Resilience: CrowdStrike Incident Lessons

Cyber security extends beyond bad actors and malicious threats. Digital disruptions to business continuity as felt globally by the CrowdStrike and Microsoft incidents in July 2024 highlight the need to integrate technology risk into general governance, risk, and compliance frameworks. The fundamental resilience capabilities necessary to respond to a cyber incident must be driven by commercial risk management structures.

Third-party supply chains and trusted sources can pose significant business continuity threats, as seen in the recent CrowdStrike incident where a software update error disrupted systems. This highlights the necessity of aligning business continuity, incident response, and disaster recovery plans with legislative, regulatory, and commercial obligations. Effective risk management should be designed to maintain operational stability and compliance amid disruptions, including cyber incidents.



Strategies to Manage Business & Technology Risk:

Governance, Risk, and Compliance Framework Alignment:
• Integrate cyber security into existing governance, risk, and compliance (GRC) frameworks.
• Ensure alignment of cyber security policies with organisational objectives and regulatory requirements.
Accountability:
• Define clear roles and responsibilities for cyber security at all organisational levels.
• Establish accountability mechanisms for cyber security practices and incident response.
Board/Director Overview:
• Engage the board of directors in cyber security strategy and decision-making.
• Provide regular updates to the board on cyber risks, incidents, and mitigation efforts.
Reporting and Continuous Improvement:
• Implement regular reporting on cyber security posture and incidents.
• Establish processes for continuous improvement based on evolving threat assessments and business risk.
Policies and Plans:
• Develop and maintain comprehensive cyber security policies and incident response plans.
• Ensure policies are regularly reviewed and updated to reflect evolving threats and technologies.
Risk Management Practices:
• Integrate cyber risk management into overall enterprise risk management (ERM) processes.
• Conduct regular risk assessments to identify and mitigate potential cyber threats.
External Audits and Vulnerability Assessments:
• Schedule regular external audits and vulnerability assessments to evaluate cyber security measures.
• Address identified vulnerabilities promptly and reassess to ensure effective remediation.
Expertise:
• Invest in skilled cyber security professionals and continuous training for staff.
• Leverage external expertise and threat intelligence to stay ahead of emerging threats.
Culture of Cyber Security:
• Foster a culture that prioritises cyber security as a key component of business resilience.
• Promote awareness and training programs to ensure all employees understand their role in maintaining cyber security.
Regulatory and Commercial Obligations:
• Ensure compliance with relevant legislation, industry standards, and commercial contracts.
• Align cyber security practices with regulatory requirements to avoid legal and financial penalties.
Third-Party and Supply Chain Risk:
• Ensure third-party risk management includes assessing the cyber resilience of supply chain partners.
• Implement continuous monitoring and regular audits of third-party cyber security compliance.

Selecting a Cyber Security Framework: ASD Essential 8 Framework

The Australian Government has developed the Essential 8 to help organisations like yours safeguard against cyber attacks. This initiative outlines eight vital strategies to boost your cybersecurity and shield your business from potential threats. The cybersecurity framework was revised in late 2023.

E8 Mitigation Strategies:

- **Patch Applications:** Keeping software up-to-date with the latest security patches.
- **Patch Operating Systems:** Ensuring operating systems have the latest security patches.
- **Use Multi-Factor Authentication:** Requiring multiple forms of verification for access.
- **Restrict Administrative Privileges:** Limiting admin access by design and restricting privileges to only those that need it.
- **Application Control:** Restricting applications to only those approved and necessary.
- **Restrict Microsoft Office macros:** Limit or disable office macros
- **User Application Hardening:** Limit application functions to those required.
- **Regular Backups:** Regularly backing up critical data.

Selecting a Cyber Security Framework: SOC 2 Framework

SOC 2 is a rigorous auditing process that helps organisations like yours ensure the security, availability, integrity, confidentiality, and privacy of your customers' sensitive information. Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is built on the Trust Services Principles and Criteria.

Systems and Organisation Controls 2:

- **Security:**
  Protecting information from unauthorised access
- **Availability**
  Ensuring employees and clients can rely on your systems to perform their work
- **Processing Integrity:**
  Verifying that company systems operate as intended
- **Confidentiality:**
  Protecting confidential information by limiting its access, storage, and use
- **Privacy:**
  Safeguarding sensitive personal information against unauthorised users

About Law Wyze

Law Wyze Pty Ltd ("Law Wyze") is an Incorporated Legal Practice focusing on cyber security and artificial intelligence (AI) governance, risk, and compliance (GRC) legal advice and solutions.

We believe partnering with clients to identify legal and commercial digital risk and developing a bespoke governance framework is the key to integrating a robust cybersecurity culture through strong Cyber GRC practices and continuous improvement solutions.

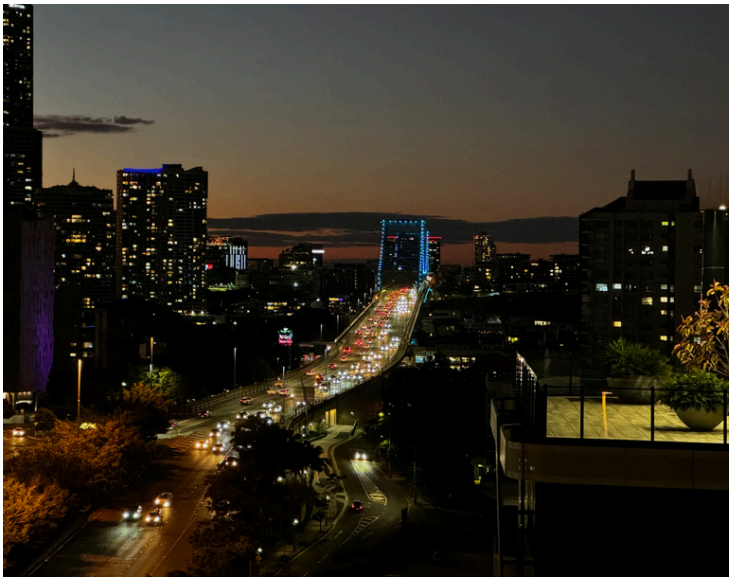
Cyber GRC

Cyber Governance, Risk and Compliance (GRC) is concerned with establishing a culture and framework of cyber security and resilience in your business. With reputation on the line and obligations to consider, it's essential to understand the evolving threat landscape, and take proactive steps to establish a culture of cyber security and resilience by adopting and prioritising cyber in your GRC practice.

Australia's disparate legislative and regulatory frameworks add an extra layer of complexity to managing GRC, making it challenging to determine the right governance, risk, and compliance approach to mitigate these risks effectively.

At Law Wyze, we are committed to helping businesses establish the safeguards they need to defend against cyber risk through providing tailored legal advice and solutions.

We are committed to working together to build a robust governance, risk and compliance framework that integrates with business to foster a culture of security and continuous improvement. Let us work with you to secure your business with confidence.



WHAT'S YOUR RISK?

FOR MORE INFORMATION

Phone :
1300 744 915

Website :
lawwyze.au

Address :
Level 1 - South Tower
527 Gregory Tce Fortitude Valley QLD

Email :
inquiries@lawwyze.au

Law Wyze

FOCUSED CYBER & AI LEGAL EXPERTISE