ALPMA SUMMIT 24 + ALTACON

2024

State of Cyber Security in Law Report

Discover the latest insights into the state of cyber security within the legal sector, highlighting key challenges and opportunities when it comes to cyber resilience.

AUCYBER LEXVERITAS ALPMA Australasian Legal Practice Management Association

Foreword

In an era where digital transformation and technology reliance continues to reshape the practice of law, the importance of data resilience and cyber security cannot be overstated. Australian law firms rely on efficiency producing cloud technologies to help manage sensitive data and streamline matter information.

The global threat of, and exposure to, cyber criminals and threats is at unparalleled levels. This report, based on comprehensive survey data of ALPMA members and the wider legal community, provides an insight into the state of cyber security within the legal sector; outlining the key challenges and opportunities when it comes to cyber resilience.

The **2024 State of Cyber Security in Law Report** is a study of Australian and New Zealand law firms, delving into the web of digital and data security challenges that Australasian law firms face, shedding light on the complexities that require both the attention of strategic foresight and proactive planning.

The findings reveal a legal industry acutely aware of growing cyber risks, yet grappling with the complexities of building resilient digital defences. With **56%** of respondents identifying cyber security as their top operational concern — an increase from last year — it is clear that law firms are recognising the urgency of this issue. However, the decline in confidence in cyber security resilience, coupled with gaps in preparedness and response strategies, highlights the need for a more concerted and strategic approach.

A special focus of the report also places emphasis on evaluating firms' readiness for cyber incidents, particularly regarding in-house expertise, cyber incident planning and the implementation of effective cyber security measures. The varied approaches to tackling cyber threats and the differing levels of preparedness highlight the diverse perspectives within the legal sector.

This report serves not only as a reflection of the current state of cyber security among Australasian law firms but also as a call to action. It emphasises the importance of proactive measures such as the implementation of robust cyber incident plans, regular security assessments and comprehensive employee training.

As we look to the future, it is imperative that law firms continue to prioritise cyber security, ensuring that their digital infrastructure is not only secure but resilient against evolving cyber threats. The insights provided in this report aim to guide firms in strengthening their cyber security posture, safeguarding their operations and ultimately, protecting the trust and confidence of their clients.

We thank all respondents who took part in the study and encourage you to share the **2024 State of Cyber Security in Law Report** with fellow colleagues.

Peter Maloney
Chief Executive Officer
AUCyber | AUCloud

Duncan Little
Chief Executive Officer
LexVeritas

Emma Elliot
Chief Executive Officer
ALPMA

Background & Research Methodology

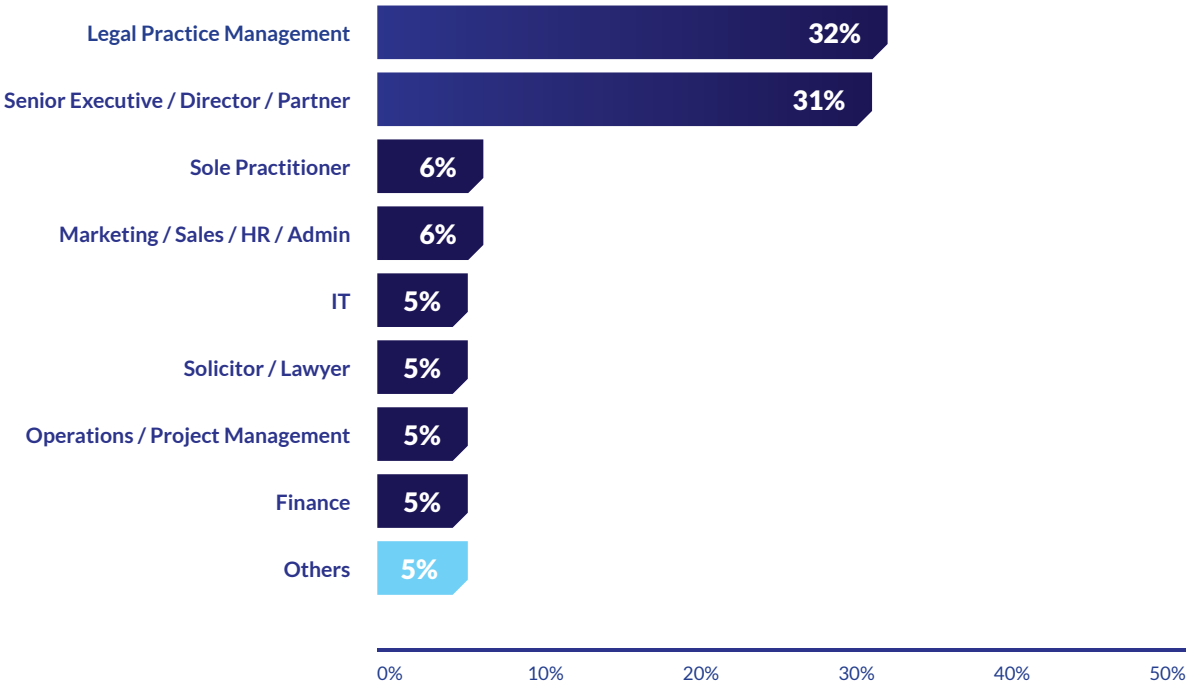
The **2024 State of Cyber Security in Law Report** research was undertaken by ASX-listed cyber security and sovereign cloud provider AUCyber, in partnership with managed services provider LexVeritas and in association with the Australasian Legal Practice Management Association (ALPMA). The survey was completed by **140** law firm respondents across Australia (**95%**), New Zealand (**3%**) and Asia (**2%**).

AUCyber is recognised as the official cyber security partner of ALPMA.

Participant Profile

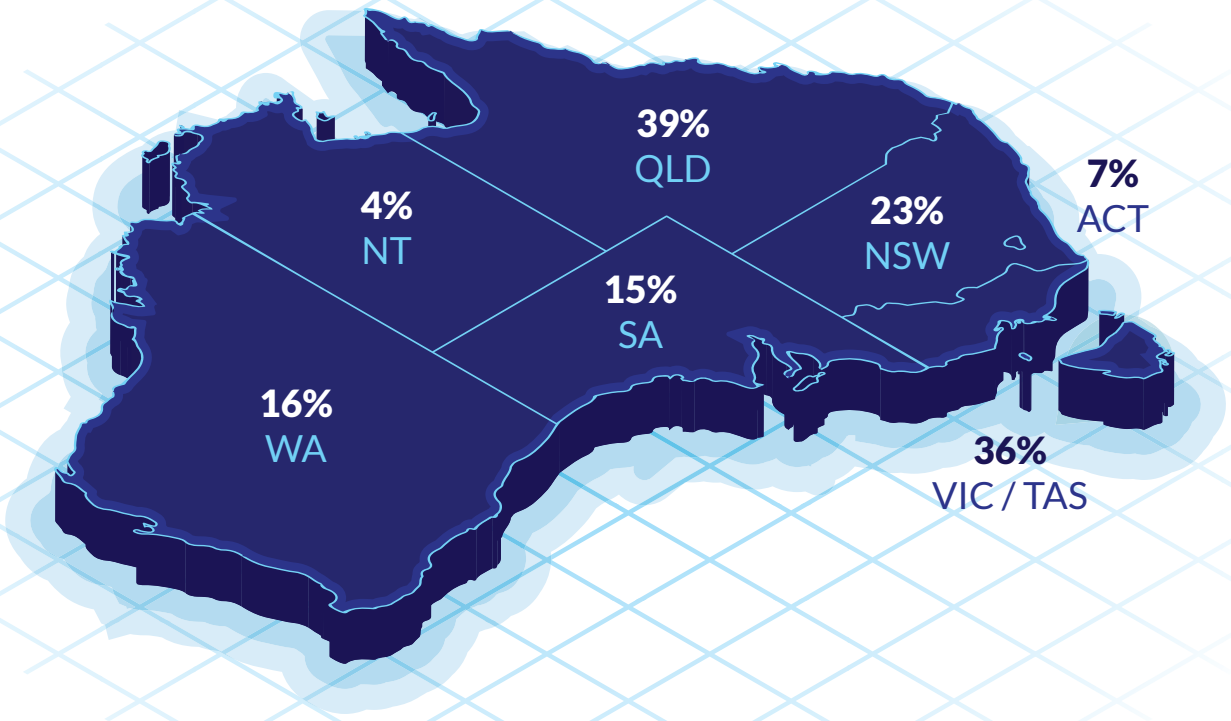
Respondents worked across all practice areas of law firms, with 32% in identifying legal practice management and an additional **31%** of respondents noting themselves as holding senior executive, director or partner level roles.

What is your role or position area within your organisation?



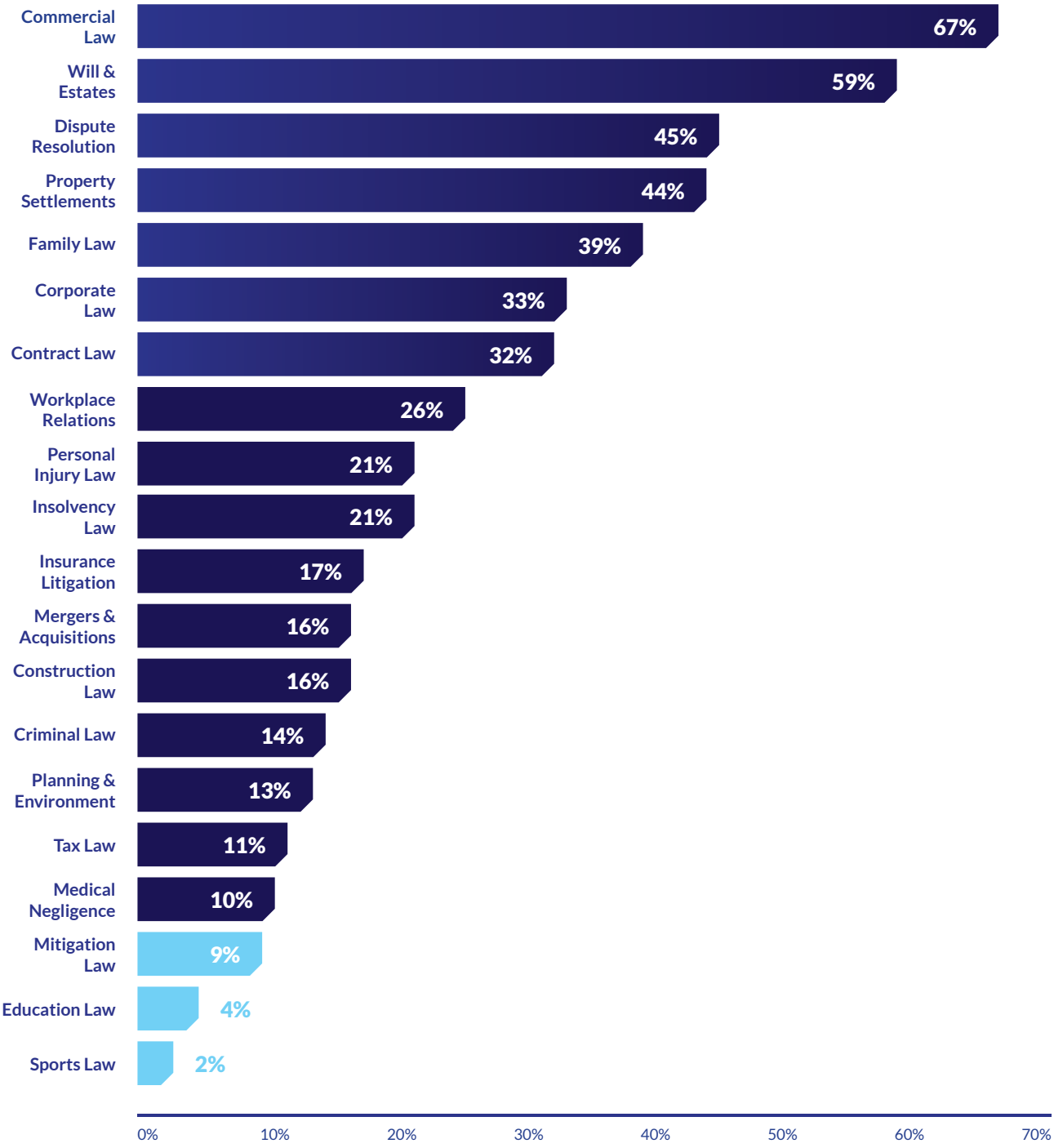
Where does your organisation currently operate?

2%
Others



2%
New Zealand

What are the main areas of law your firm practises?

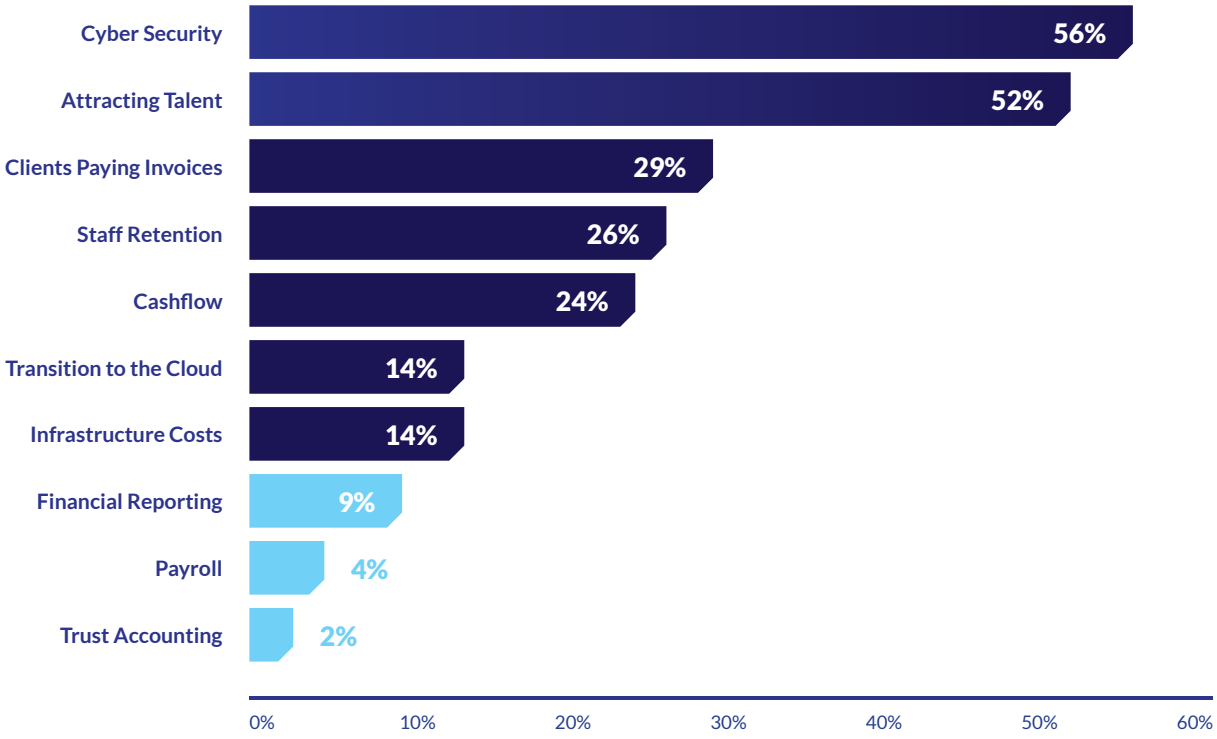


Cyber Security is the Industry's Biggest Challenge

In an effort to identify the key challenges faced by Australian law firms, this survey revealed a wide range of concerns. For the second year in a row, Australian law firms identified **'Cyber Security' as their biggest operational challenge**, with **56%** of respondents citing it as their top concern — growing **3%** from the previous year.

Given the rise of sophisticated cyber-attacks and data breaches, it is clear Australian law firms are highly aware of the need to strengthen their digital defences and prioritise cyber security. Protecting sensitive client data and matter information while ensuring seamless business continuity has become a top priority. These survey results make one thing clear: prioritising cyber security is no longer optional, it's essential for protecting the future and operations of law firms. Implementing robust cyber security measures is crucial to shield sensitive information from cyber criminals and ensure business continuity.

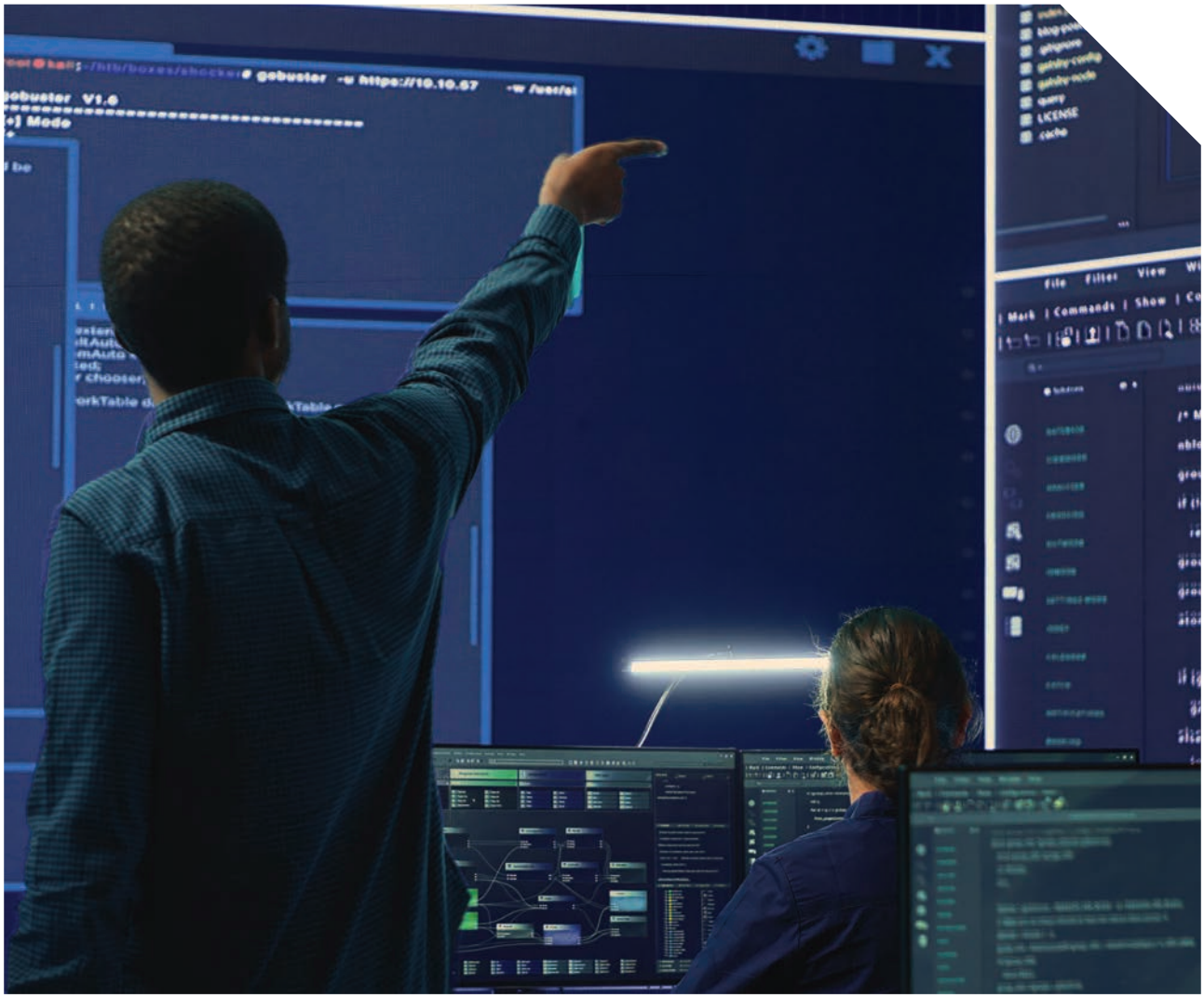
What are the biggest challenges currently facing your firm?



Attracting Talent

Running in close competition, the challenge of 'Attracting Talent' also emerged as a top concern for over half (**52%**) of all participants, highlighting the growing difficulty of recruiting skilled professionals in a competitive market.

This issue is compounded by 'Staff Retention', with **26%** indicating that firms are not only struggling to attract new talent but also to retain their existing workforce. These people-related challenges are further linked to issues like 'Clients Paying Invoices', identified by **29%** of participants, pointing to concerns around cash flow and the current economic conditions facing Australia. Together, these findings suggest that Australian law firms must focus on improving talent acquisition and retention strategies while also strengthening their account receivable practices and cash flow to ensure long-term sustainability of talent and operations.



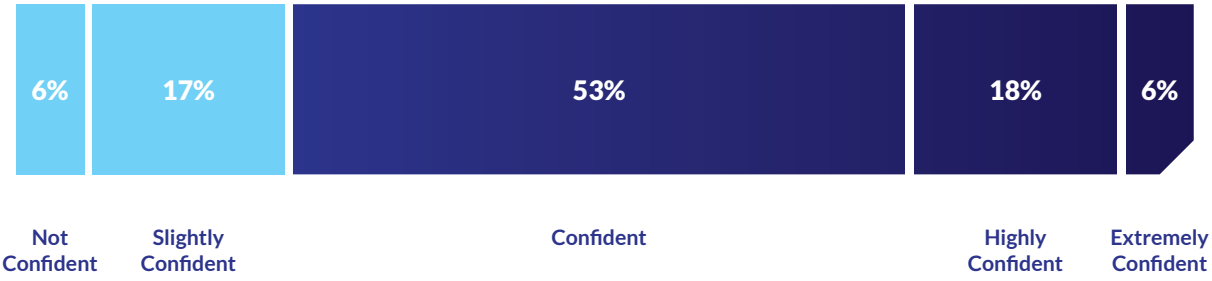
Cyber Security — How Prepared are we?

When assessing the confidence of firms in their cyber security resilience, the findings reveal mixed levels of confidence.

In comparison to 2023 results, where **44%** of law firms reported a high level of confidence in their cyber security resilience, this year's findings indicate a notable decline in confidence. Only **24%** of firms express a high or extremely high level of confidence then it comes to their existing cyber security protocols, a significant decrease from the previous year.

This shift suggests that more firms are now questioning the adequacy of their cyber defences. The fact that **17%** of respondents admit to concerns about their firm's cyber defences and another **6%** lack confidence, indicates a significant portion of firms feel vulnerable to cyber threats. The decline in high confidence levels highlights growing awareness of cyber security challenges and the recognition that existing measures may not be sufficient in an evolving threat landscape. This trend underscores the increasing need for law firms to reassess and strengthen their cyber security response strategies to better protect against potential attacks.

How confident are you that your firm is secure against a cyber-attack?

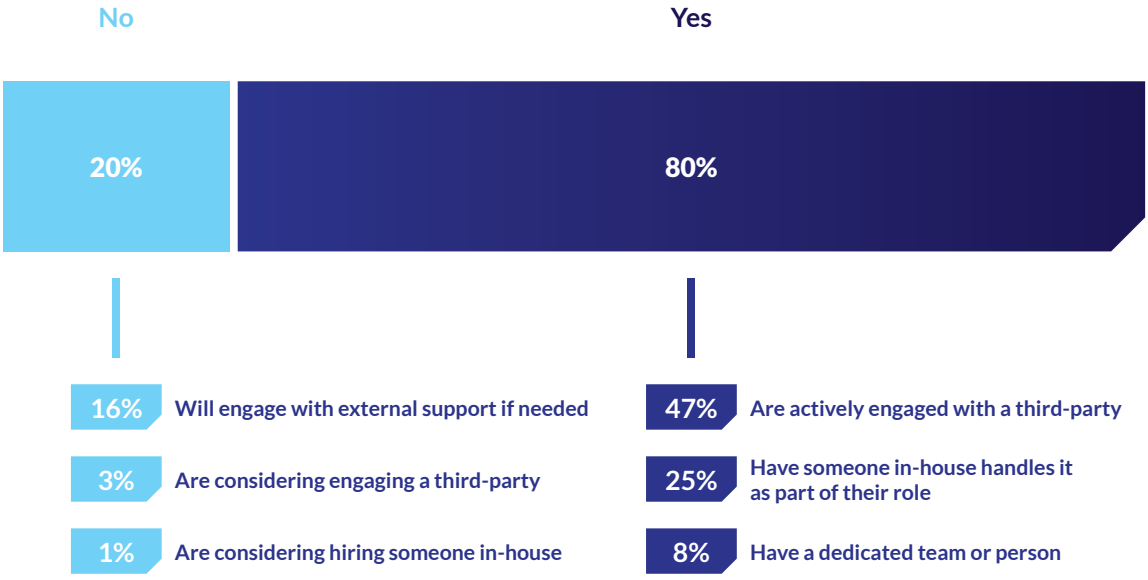


Cyber Security Planning & Incident Response

The allocation of responsibilities for managing and addressing cyber security risks within law firms reveals a range of strategies and maturity. A significant **47%** of firms surveyed collaborate with third-party entities, leveraging external IT and cyber expertise and assistance.

Meanwhile, **25%** rely on dedicated in-house personnel to handle these concerns, demonstrating an internal directive for the management of cyber planning, detection and response strategies. Additionally, **12%** of firms plan to seek external support as needed, reflecting a flexible approach to cyber security challenges. Notably, **16%** are actively exploring external support options, indicating a proactive stance toward enhancing their cyber security measures.

Do you have a designated individual or team responsible for managing and addressing cyber security risks and incidents for your firm?

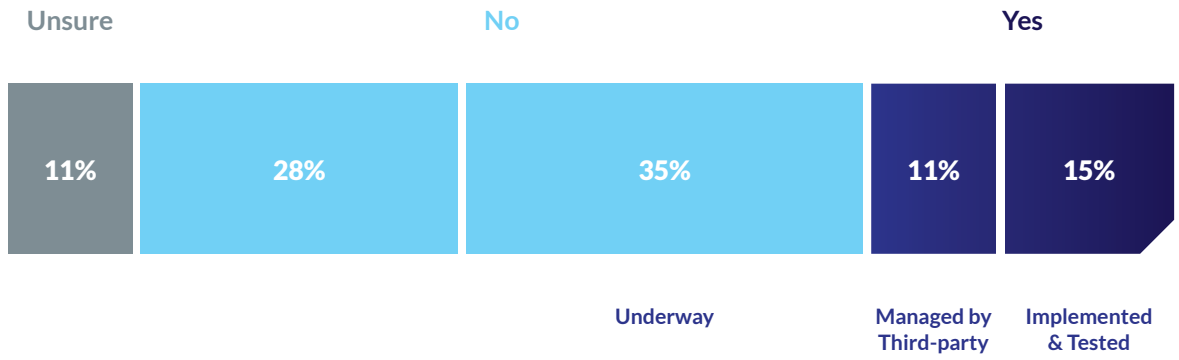


Cyber Incident Planning

The response data on the existence of formal 'Cyber Incident Plans' reveals significant variation in cyber preparedness among Australian law firms. Notably, **28%** of respondents reported the absence of such plans, exposing a critical gap in their ability to manage and respond to cyber threats in the most efficient and effective manner. In contrast, just over one-third (**35%**) of firms are actively developing these plans, signaling ongoing efforts to bolster their cyber security measures.

Disappointingly, only **15%** of firms have implemented and tested internal cyber incident plans, while **11%** rely on third-party entities to manage their incident response. Additionally, **11%** of respondents are unsure about the status of their firm's plans. These findings collectively underscore the urgent need for comprehensive, well-documented cyber incident plans. They highlight varying levels of preparedness across the industry and emphasize the importance of having robust strategies in place to protect against, detect and respond to cyber incidents effectively.

Do your firm have a published cyber incident plan that is well understood by your staff and recently tested?



Cyber Security Detection, Prevention & Protection

The responses regarding the implementation of effective cyber security measures reveal a troublingly mixed landscape among law firms. Just over half (**56%**) of firms believe they have established cyber security measures to protect themselves against cyber-attacks, reflecting a proactive stance on safeguarding their operations, the overall picture remains concerning. Notably, **26%** of respondents are unsure about the extent or effectiveness of their cyber security measures, pointing to potential gaps in their security posture and suggesting a lack of confidence or clarity in their current protections.

More alarmingly, **18%** of respondents believed their firm was not doing enough to protect itself against a cyber-attack, representing a critical vulnerability that leaves them highly susceptible to cyber threats. This lack of foundational security measures not only exposes firms to significant risks but also undermines their ability to respond effectively to potential incidents. To address these issues and bolster cyber security defences, firms should consider conducting regular and thorough security assessments to identify and remediate vulnerabilities. Additionally, comprehensive training for all employees is crucial to enhancing overall awareness and preparedness, ensuring that everyone within the organisation is equipped to recognise and respond to cyber security threats.

Without the implementation of robust cyber security solutions and a thorough understanding of their effectiveness, firms expose themselves to severe risks, including the compromise of sensitive client data. This negligence can lead to profound operational disruptions, substantial reputational damage, and significant legal exposure. In the event of a cyber incident, the consequences could be devastating, undermining client trust, inflicting financial losses and potentially resulting in serious legal liabilities. The failure to address these vulnerabilities not only jeopardises the integrity of client relationships but also threatens the very survival and credibility of the firm itself.

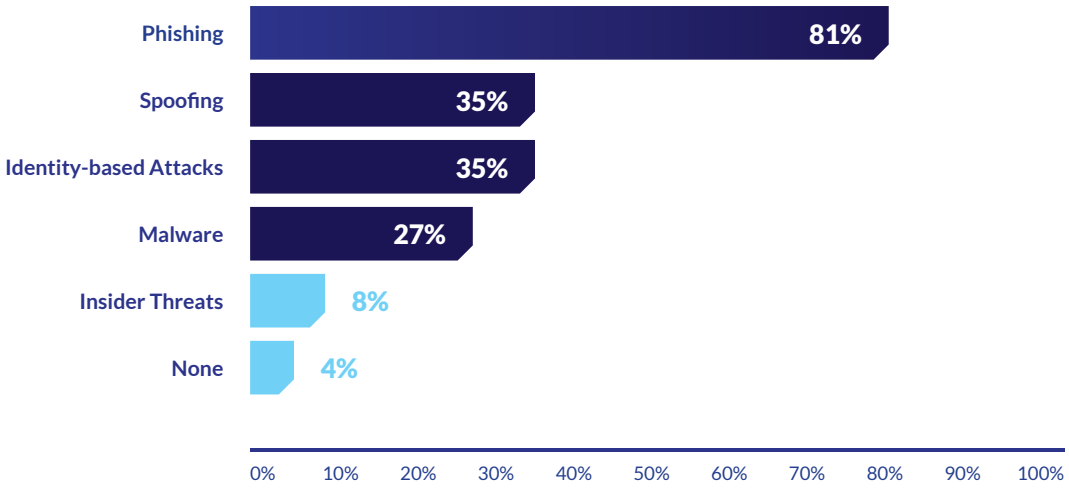
Do you believe your firm is doing enough to protect itself against a cyber-attack?

Cyber-attacks on Law Firms are Increasing

Over the past 12 months, **21%** reported experiencing cyber-attack attempts, highlighting a significant vulnerability within law firms. This marks a **7%** increase from the previous year, suggesting that cyber criminals are employing increasingly sophisticated techniques to breach operational systems and access sensitive data. Despite this, **79%** of firms reported no such attempts, reflecting a generally strong cyber security posture among the majority.

Phishing remains the most prevalent form of attack, with **81%** of respondents falling victim to these schemes. Additionally, 35% encountered identity-based assaults and spoofing, while **27%** were affected by malware attacks, illustrating the wide range of cyber threats faced. Insider threats, although less common, were reported by **8%** of firms. These insights underscore the need for law firms to bolster their defences against phishing and other prevalent threats, enhance employee training to recognise and mitigate attacks, and continuously update their security protocols to stay ahead of evolving cyber risks.

What type of cyber-attack did your firm suffer?

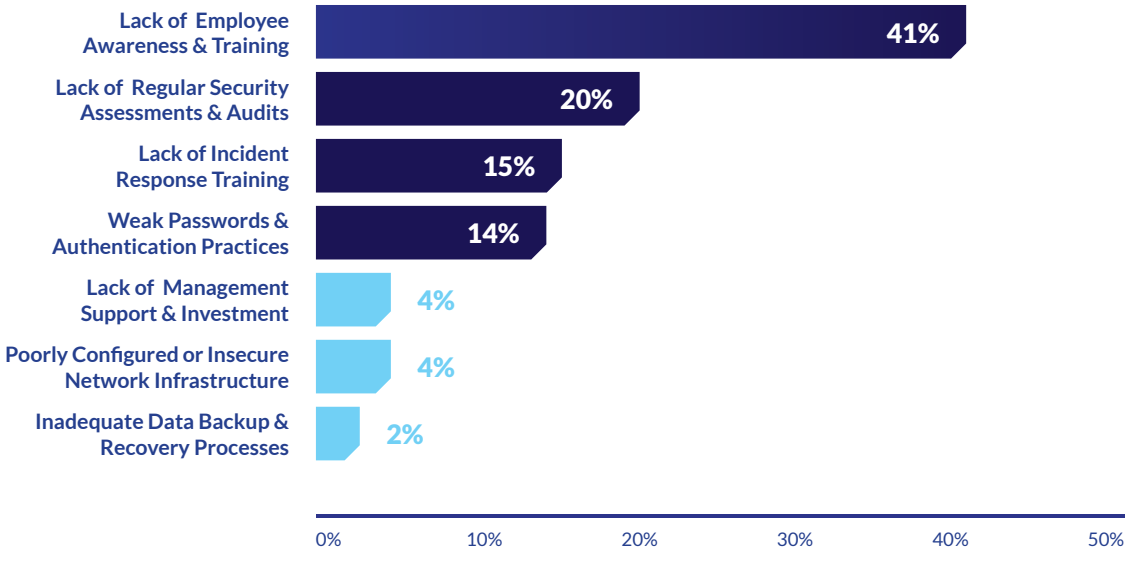


Challenges to being Cyber Resilient

Insights into the primary obstacles to achieving robust cyber security reveal a range of challenges faced by law firms. A significant **41%** of respondents cited a lack of employee awareness and training as the most prominent barrier, underscoring the crucial role that knowledgeable boards, management and frontline staff play in maintaining cyber security resilience. Additionally, **20%** highlighted the absence of regular security assessments and audits, emphasising the need for continuous governance, risk and compliance evaluation and improvement of security measures to effectively address and mitigate evolving threats.

Further concerns include the absence of incident response planning, noted by **15%** of respondents, which highlights the need preparedness for potential breaches. Weak passwords and authentication practices were flagged by **13%** of respondents, indicating vulnerabilities in basic security protocols. A smaller percentage, **4%**, cited insufficient management support and investment, along with poorly configured or insecure network infrastructure as key issues. Lastly, inadequate data backup and recovery processes were identified by **2%** of respondents, highlighting gaps in preparedness for data loss or system failures.

What do you believe is the biggest impediment to being more cyber secure?



Concern about Cyber-attacks' Impact

Responses regarding the potential impact of a cyber security breach reveal varying levels of concern among law firms. Interestingly **20%** of respondents said they were not very concerned as they believed they were doing enough, the majority (**54%**) displayed moderate apprehension about the potential consequences. Over a quarter (**26%**) expressed profound concern, highlighting their awareness of the severe impacts a breach could have on operations, reputation and data security.

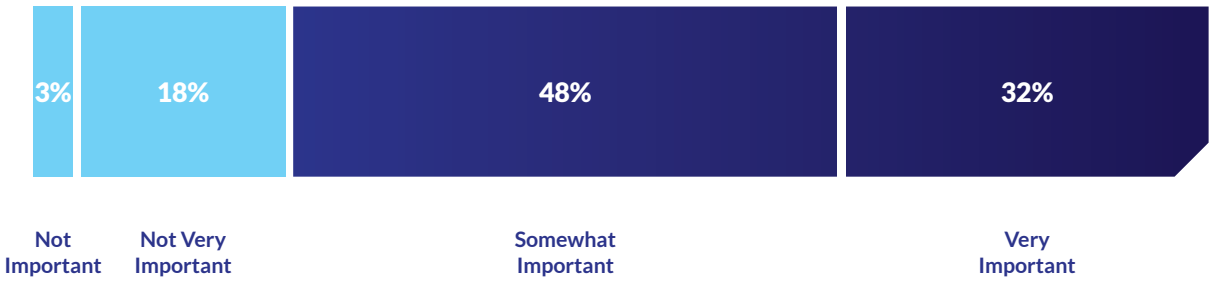
Overall, the sentiment levels of concern when it comes to impact vary across the sector, highlighting a critical need for comprehensive education, training and strategic advice to help firms better understand, manage and mitigate their cyber security risk profile.

Data Management, Storage & Cloud Modernisation

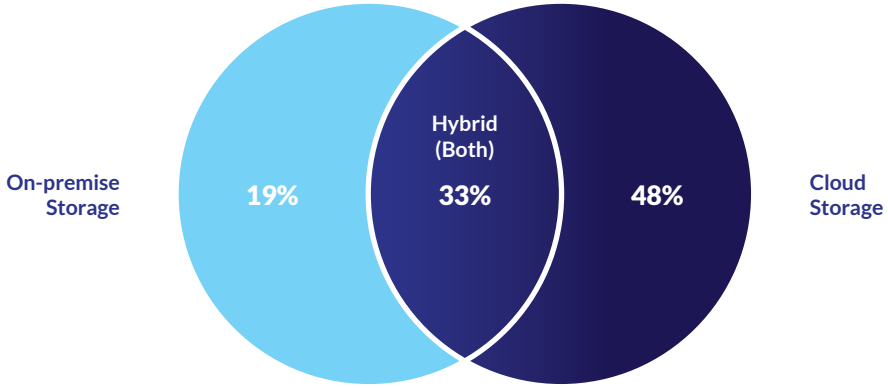
Responses regarding the importance of storing sensitive data within Australian (sovereign) cloud environments revealed a range of perspectives. A small **3%** viewed it as unimportant, while **18%** preferred alternative measures. Notably, **48%** considered it important but not critical, whereas **31%** regarded it as a top priority. Best practice sovereign cloud storage includes ensuring that data is stored and managed in the confines of Australian data centres, by security cleared personnel on behalf of Australian owned and operated providers.

When it comes to data hosting, **48%** of respondents reported that their firm's data is primarily stored in the cloud, with an additional **33%** utilising a hybrid approach of both on-premise and cloud storage, and **19%** noted they rely solely on traditional on-premise data storage.

How important is it for your firm to store and process sensitive data within a sovereign cloud infrastructure?



Is this majority of your firm's data hosted on-premise or in the cloud?

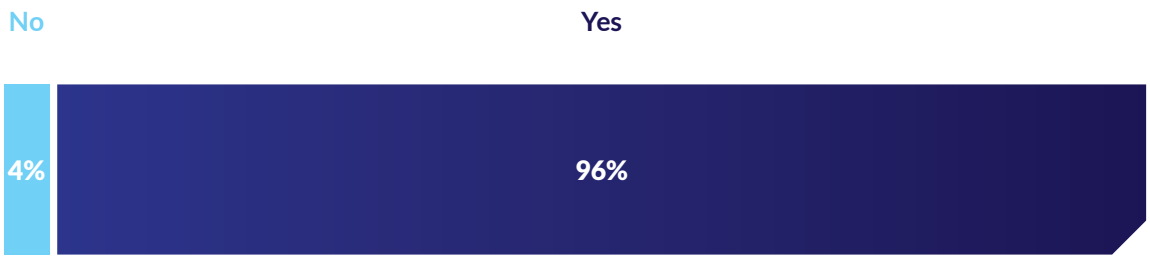


Data Backup & System Continuity

The survey results highlight a strong commitment to data backup and resilience within law firms, with **96%** affirming that they back up their data and systems. This high percentage reflects a widespread recognition of the critical importance of data backups in the legal profession, where the confidentiality and integrity of sensitive client information are essential.

However, **4%** of firms do not currently implement data backups and should be mindful of the significant risks they face. It is crucial for these firms to adopt comprehensive backup strategies to protect their clients' interests and their own professional integrity. Data backups are not just a precaution but a fundamental necessity for maintaining business continuity in the event of a major operational issue or cyber-attack.

Does your firm backup your systems and data?

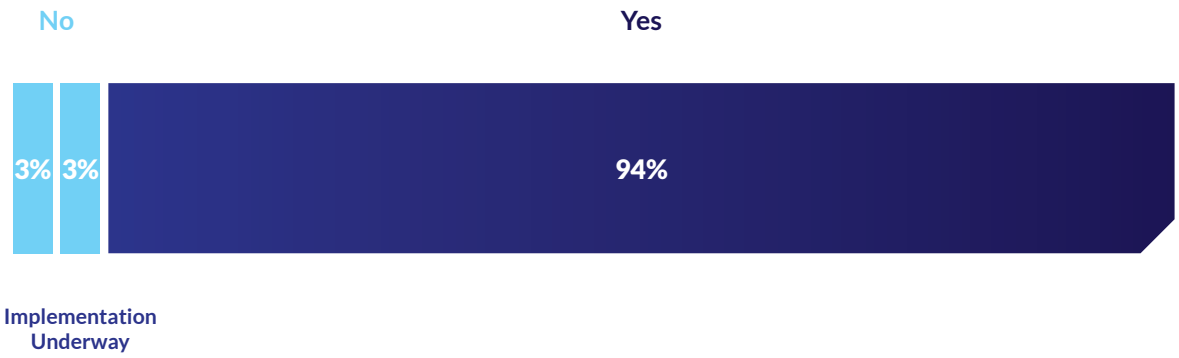


Multi-factor Authentication

The widespread adoption of multi-factor authentication (2FA or MFA) at **94%** highlights its essential role in strengthening online security. The research reveals that **3%** of firms are in the process of implementing 2FA for their systems and applications, while another **3%** have yet to adopt this security measure.

By requiring two forms of verification, 2FA adds a crucial layer of protection beyond traditional passwords, significantly enhancing security and making it more challenging for unauthorised individuals to gain access to sensitive accounts and information. This high adoption rate among law firms reflects a strong commitment to improving overall cyber security.

Do you use multi-factor authentication for your important online accounts, such as email or banking?



Cyber Security Frameworks

Familiarity with the Australian Cyber Security Centre (ACSC) Cyber security baseline, ***Essential Eight***, was observed in **56%** of respondents, reflecting a considerable level of awareness about critical cyber security frameworks within the industry. This indicates that more than half of the firms recognise the importance of following established guidelines to enhance their cyber security posture. However, it also highlights that a significant portion — **44%** — may not be familiar with these essential guidelines, pointing to potential gaps.

The Australian Signals Directorate has developed prioritised mitigation strategies to mitigate cyber security incidents, helping organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the *Essential Eight*. To bolster overall cyber security, law firms should strive to increase awareness and adherence to the *Essential Eight*, ensuring that all firms are equipped with the knowledge and practices necessary to defend against cyber threats effectively.

While the *Essential Eight* is widely adopted across the industry, it is also important to recognise that other cyber security guidelines and frameworks also exist. These varied approaches complement the *Essential Eight*, offering additional layers of protection and guidance for enhancing cyber security practices.

Are you familiar with the Australian Cyber Security Centre (ACSC) cyber security baseline, Essential 8?

Business Continuity Planning (BCP) & Testing

Having a Business Continuity Plan (BCP) is crucial in the event of a cyber-attack, as it ensures that firms can quickly recover operations, protect client data and maintain their reputation. While **68%** of firms have a BCP in place, the remaining firms should prioritise developing one to mitigate potential financial losses, minimise operational downtime and uphold client trust in the face of cyber threats.

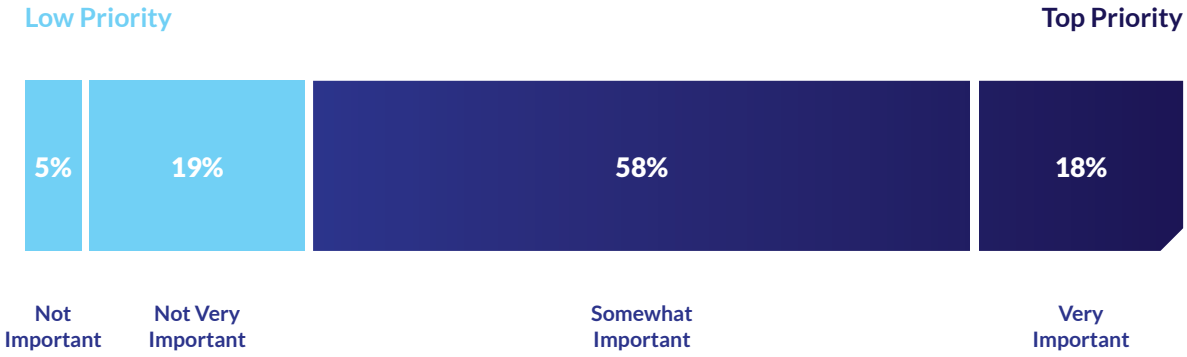
Does your firm have a Business Continuity Plan (BCP)?

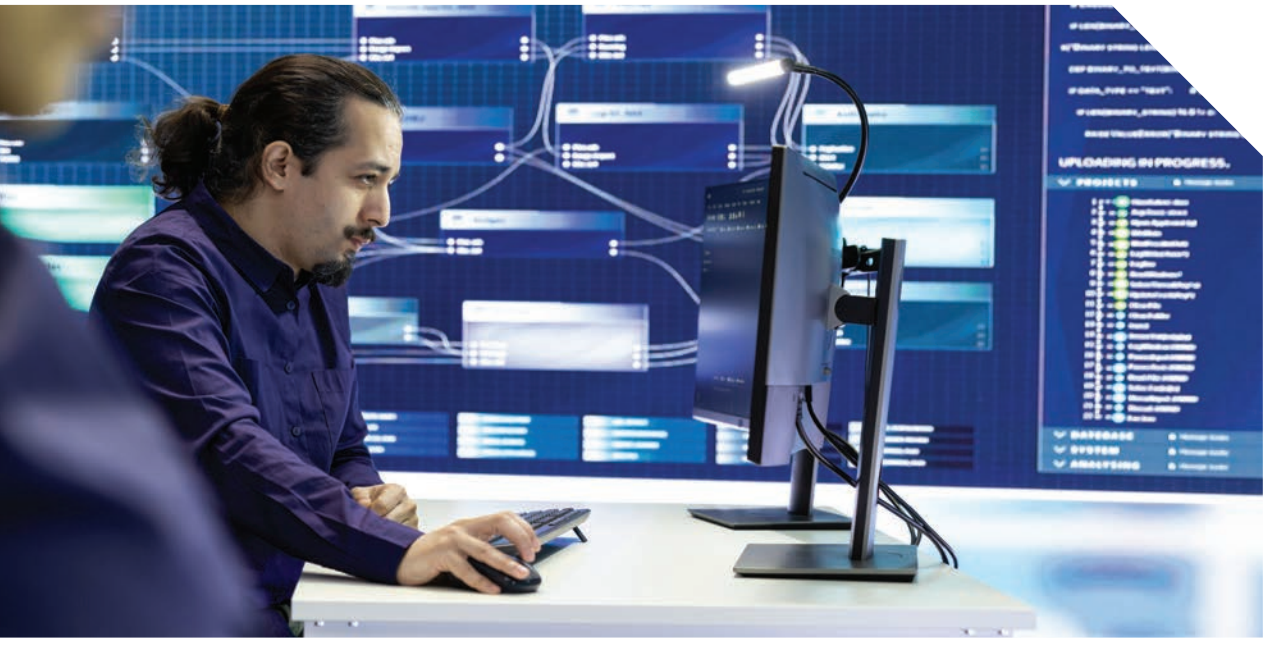
In terms of cyber security testing and assurance, only **46%** regularly conduct penetration testing, while **81%** provide cyber security awareness training for their teams. In an era where cyber criminals are increasingly adept at penetrating systems firms must continually enhance their security measures through education and testing to stay ahead of threat actors.

When it comes to having implemented security certifications such as ISO 27001 or SOC 2, opinions varied across law firms: **19%** viewed them as less important due to alternative measures in place, only **18%** considered them a priority, **58%** regarded them as somewhat important and **5%** did not find them relevant.

Does your firm conduct Penetration Testing?

How important do you consider certifications, such as ISO 27001 or SOC 2, in ensuring the security of your business's data and systems?



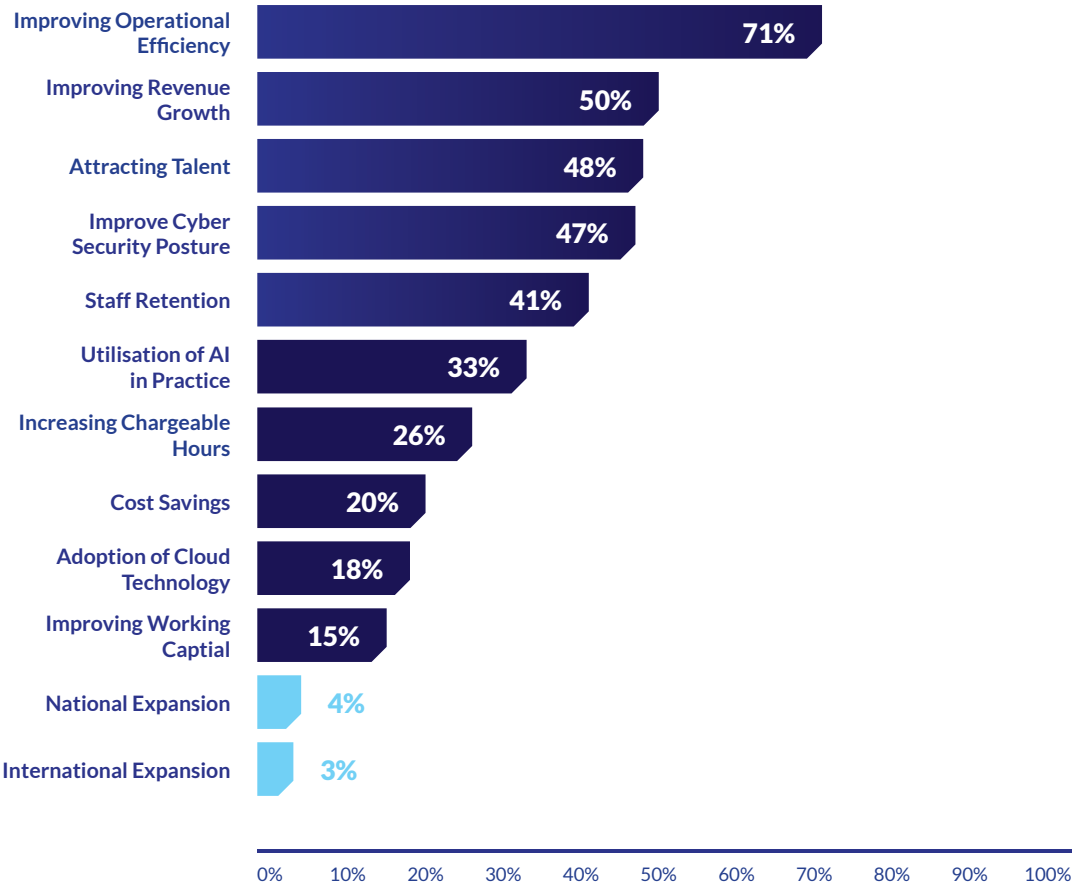


Future Priorities

Respondents identified several key strategic priorities for FY24, with a strong emphasis on enhancing firm operations and growth. The top priority is 'Improving Firm Operational Efficiency', cited by **71%** of firms, reflecting a widespread focus on streamlining processes and optimising resources. This is closely followed by 'Improving Revenue Growth' (**50%**) and 'Attracting Talent' (**48%**), highlighting the ongoing importance of financial performance and talent acquisition in a competitive market.

Additionally, 'Improving Cyber Security Posture' is a significant focus for **47%** of firms, underscoring the critical need to strengthen defences against increasing cyber threats. 'Staff Retention' is also a priority for **42%** of respondents, indicating the value placed on maintaining a stable and experienced workforce. Interestingly, **33%** of firms are prioritising the 'Utilisation of AI in Practice', demonstrating a growing interest in leveraging AI to enhance legal services and operational capabilities.

What are your firm's main strategic priorities this financial year?



Conclusion

This report highlights the increasing recognition within Australian law firms of the importance of cyber security in today's rapidly evolving digital landscape. Cyber security has emerged as the top operational challenge for **56%** of respondents, marking a **3%** increase from the previous year. This growing concern reflects the escalating sophistication of cyber-attacks and the need for robust multifaceted technology solutions, planning and investment. A decline over the past year in cyber resilience confidence has been witnessed with only **24%** expressing high confidence, necessitating the need for law firms to reassess their security strategies.

The survey further revealed a diverse range of preparedness and response strategies, with **47%** of firms collaborating with third-party entities for cyber security management and **35%** actively developing cyber incident plans. However, the **28%** of firms lacking published cyber incident plans and **18%** believed their firms was not doing enough highlight potential critical vulnerabilities that need to be addressed.

While **96%** of firms demonstrate a strong commitment to protecting business continuity with regular backups, the **4%** that do not engage in this practice must recognise the severe risks involved. Moreover, the high adoption of multi-factor authentication (**95%**) is encouraging, but the existence of firms still in the process of implementation points to areas for further improvement.

Overall, the findings indicate that while many Australian law firms are taking significant steps towards cyber security, there remains considerable room for improvement. The increasing frequency of cyber-attacks, coupled with the evolving threat landscape driven by AI and other technologies, demands continuous awareness and enhancement of cyber security measures.

Moving forward, law firms must prioritise the development of comprehensive cyber security frameworks, including Business Continuity Plans, to safeguard their operations, protect sensitive client data and maintain their reputation in an increasingly digital world.

AUCyber serves as the official cyber security partner for the Australasian Legal Practice Management Association (ALPMA). Recognised for its award-winning managed cyber security, cloud services, and IT support, AUCyber focuses on providing tailored solutions for Australian law firms to protect data, secure systems and ensure business continuity. Australian-owned and operated company, AUCyber is accredited and certified to the highest standards, guaranteeing best practices in security and data protection. With a strong track record of serving leading organisations across corporate Australia and Government, AUCyber is committed to delivering reliable and effective cyber security solutions.

Discover award-winning cyber security today.

aucyber.com.au

LexVeritas is a national Australian Managed Services Provider (MSP) that provides bespoke finance, IT and HR services tailored to mid-tier and boutique law firms. By using new-world innovation and technology, LexVeritas empowers law firms to free themselves of the daily challenges of effectively managing the finance, IT, and HR functions. Our specialist staff and integrated solutions allow our clients to focus on what they do best – provide legal services to their clients.

LexVeritas and AUCloud have partnered to create a sovereign cloud solution LexCloud, for Australian law firms offering unrivalled data storage, backup and data protection.

lexveritas.com.au

The Australasian Legal Practice Management Association (ALPMA) is the peak body representing managers and lawyers with a legal practice management role. ALPMA provides an authoritative voice on issues relevant to legal practice management.

Members of ALPMA provide professional management services to legal practices in areas of financial management, strategic management, technology, human resources, facilities and operational management, marketing and information services and technology. ALPMA offers members a wide range of learning and development resources which include webinars, in-person events, on-demand resources, formal training programs and a network of like-minded legal business professionals.

ALPMA adding value to the business of law.

alpma.com.au

AUCYBER LEXVERITAS ALPMA Australasian Legal Practice Management Association