2023 State of Cyber Security in Law Report

ALPMA LEXVERITAS AUCLOUD

FOREWORD

In an era defined by digital transformation and technological advancements, Australian law firms are not immune to the evolving landscape of rapid change and global challenges. More connected than ever, the legal industry must navigate digitisation and the intricate web of challenges associated with data protection and cyber security threats. It is increasingly evident that the safeguarding of sensitive data and protecting operational business continuity is paramount.

The **2023 State of Cyber Security in Law Report** is a study of Australian and New Zealand law firms, delving into the tapestry of digital and data security challenges that law firms face, and the complexities that require both strategic foresight and proactive planning.

In an age where information is the currency of the digital realm lies the issue of cyber security, where the imperative to fortify digital defences against ever-evolving threats is non-negotiable. This report reveals the urgency for all firms to have robust cyber security practices; a need accentuated by the 53% of respondents who identified it as their most pressing challenge.

The report also uncovers the dynamic interplay between attracting human resource talent, allocating financial resources for technology infrastructure, and the need to optimise and plan for operational strategies. The intricate dance of securing skilled employees while maintaining robust IT frameworks resonates with 48% and 35% of respondents, respectively, identifying it as their biggest challenge.

A special focus of this report is dedicated to the preparedness of firms for cyber incidents, with attention to in-house expertise, cyber incident planning, and the implementation of cyber security planning and response measures. The diverse strategies to counter cyber threats and the varying degrees of preparedness encapsulate the kaleidoscope of perspectives within the legal sector.

As we navigate this journey through the challenges and aspirations of Australian law firms, it's clear that success lies in the intersection of investment, security, and resilience measures. The findings serve as a compass to guide law firms towards fortifying their digital environments, identifying risks and implementing strategies to ensure they stand strong in the face of a rapidly changing legal landscape and the threat of cyber-crime.

We thank all respondents who took part in the study and encourage you to share the **2023 State of Cyber Security in Law Report** with fellow colleagues.

Peter Maloney
CEO
AUCloud

Emma Elliot
CEO
ALPMA

Duncan Little
CEO
LexVeritas

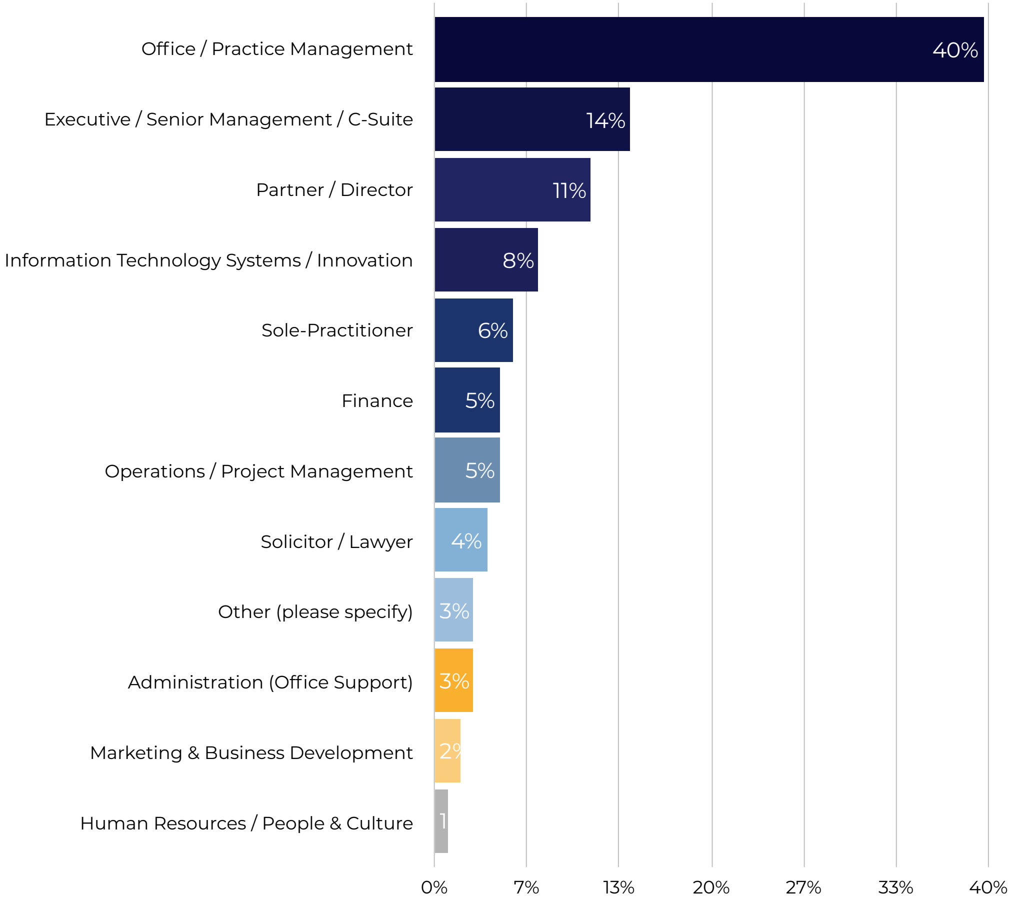
BACKGROUND + RESEARCH METHODOLOGY

The **2023 State of Cyber Security in Law Report** research was undertaken by ASX-listed cyber security and sovereign cloud provider AUCloud, in partnership with managed services provider LexVeritas and in association with the Australasian Legal Practice Management Association (ALPMA). The survey was completed by 106 law firm respondents across Australia (95%) and New Zealand (5%).

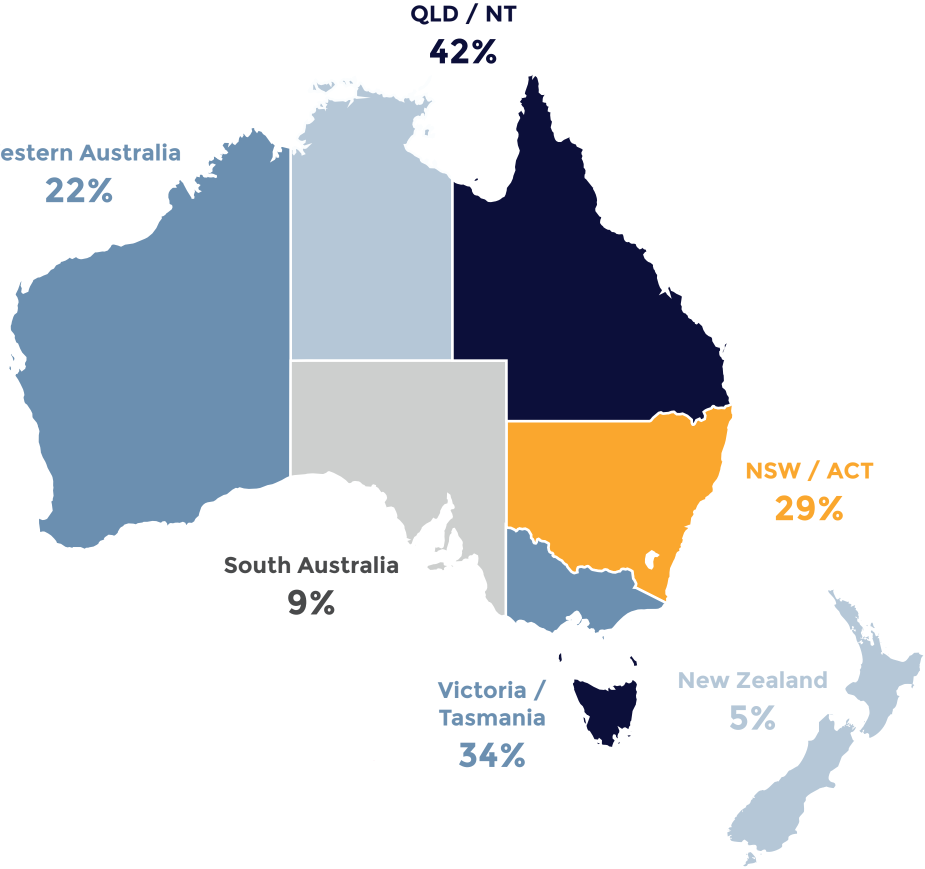
Participant Profile

Many of the respondents (40%) work in legal practice management, with an additional 25% of respondents identifying themselves in senior executive, director or partner level roles.

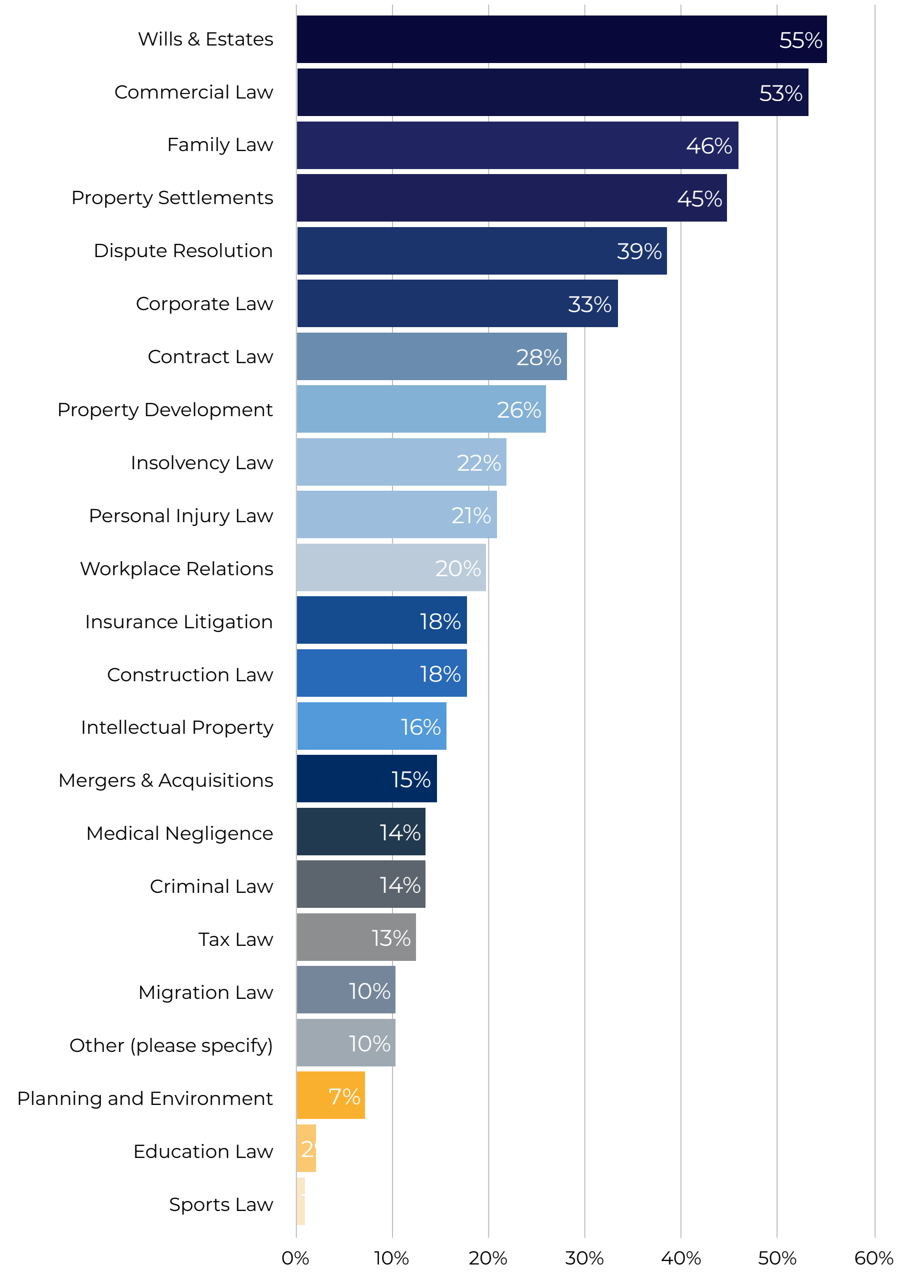
What is your role or position area within your organisation?



Where does your organisation currently operate?



What are the main areas of law your firm practices?

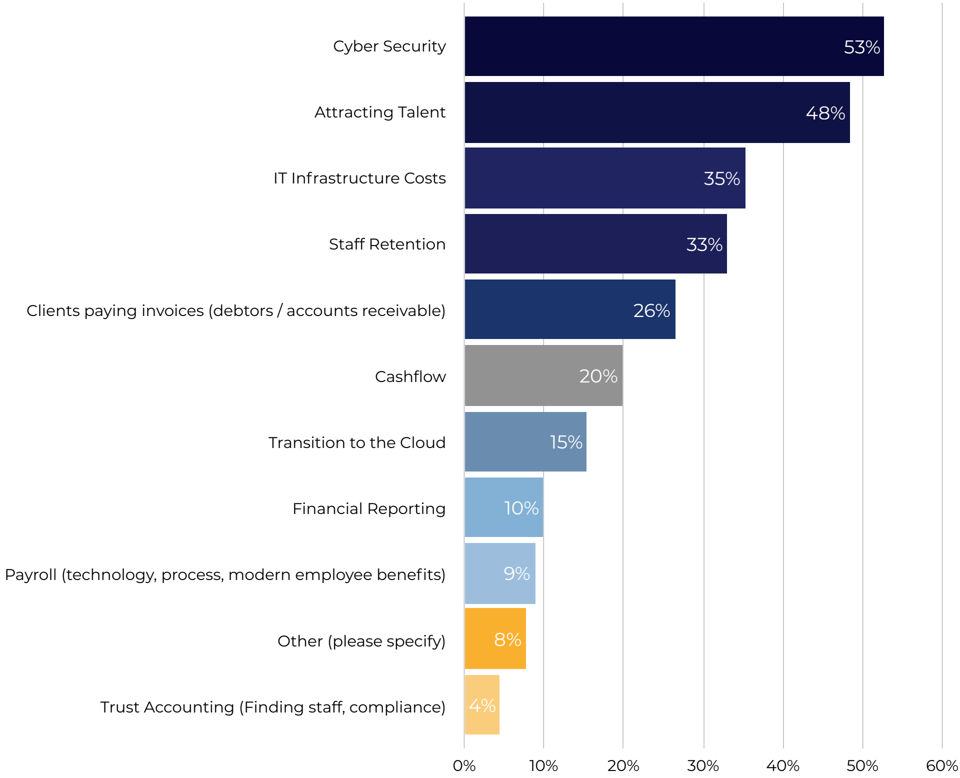


CYBER SECURITY – AUSTRALIAN LAW'S BIGGEST CHALLENGE

In the pursuit of understanding the primary challenges encountered by Australian and New Zealand law firms, this survey yielded a spectrum of concerns from participants. Notably, 'Cyber Security' emerged as the challenge, with more than half of respondents nominating it as one of the biggest operational challenge facing their firm.

The result highlights the escalating awareness of the intricate and ever-evolving cyber threat landscape that modern businesses, particularly law firms, must navigate. Given the proliferation of sophisticated cyber-attacks and data breaches, Australian law firms are aware of the need to fortify their digital defences and to protect their firm and client information. This involves prioritising cyber security measures to shield sensitive data to ensure continuity of business operations.

What are the biggest operational challenges facing your firm?



PEOPLE & SYSTEMS

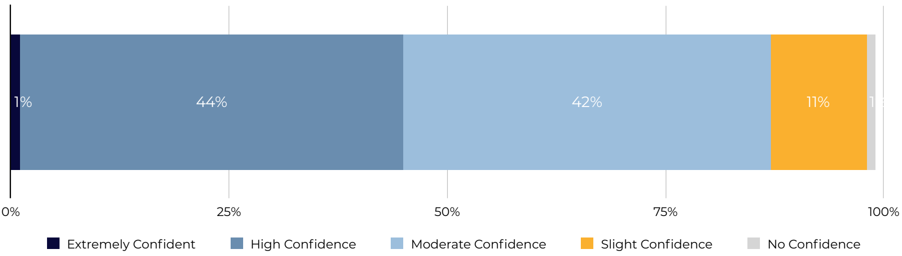
The second most significant operational challenge cited by Australian and New Zealand law firms (48%) was 'Attracting Talent'. A third (33%) of all respondents also identified 'Staff Retention' as one of their biggest challenges. This focal point underscores the ongoing struggle that many law firms face in securing and retaining skilled employees capable of driving innovation, productivity and elevating the overall competitiveness of the firm.

Further, more than a third (35%) of respondents identified 'Information Technology (IT) Infrastructure Costs' as a significant operational challenge. This acknowledgement accentuates the pivotal role of technology and systems in underpinning day-to-day operations of firms, supporting operational efficiency, and securing client matter and data management. It's evident that Australian and New Zealand law firms are challenged when it comes to optimising, upgrading, and maintaining their complex IT infrastructure to maintain seamless connectivity, efficient processes, and the agility to adapt to evolving technological landscapes.

CYBER SECURITY PREPAREDNESS

When assessing the confidence of firms in their cyber security resilience, the findings uncovered a diverse panorama of sentiments. Only 1% conveyed an extremely high level of confidence, while a robust 44% expressed a high level of confidence in their cyber security protocols. This was followed closely by 42% indicating a moderate level of confidence, reflecting a balanced outlook on their security measures. A smaller fraction, accounting for 11%, admitted to a degree of trepidation regarding their firm's cyber defences. Interestingly, 1% conceded an absence of confidence in their current cyber security posture.

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

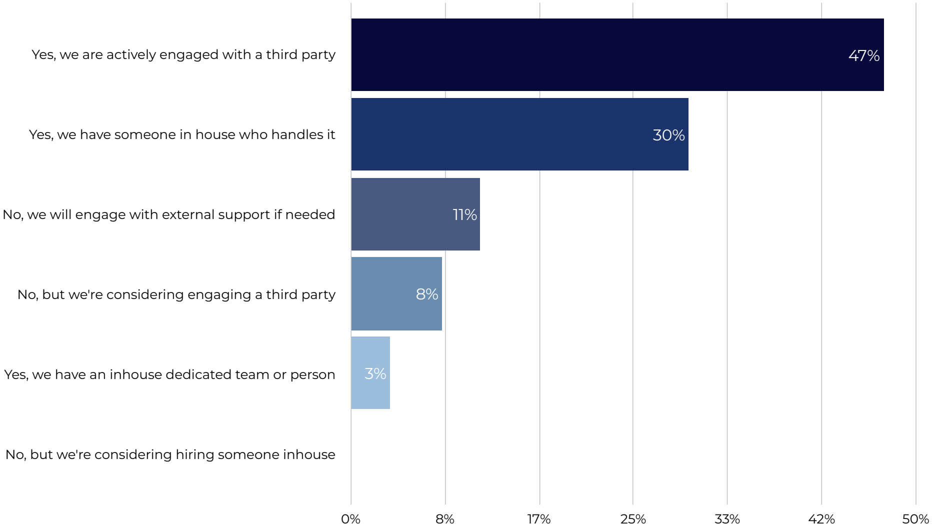


PLANNING & INCIDENT RESPONSE

The allocation of responsibilities for managing and addressing cyber security risks and incidents within law firms yielded insightful results. A substantial 47% of respondents disclosed active collaboration with third-party entities, acknowledging the expertise external specialists provide in this intricate field.

Meanwhile, 30% highlighted their firms' reliance on dedicated in-house personnel to oversee these concerns. Additionally, 12% indicated an intention to seek external support when required, reflecting a flexible strategy towards cyber challenges. With 8% proactively exploring external support to enhance cyber security measures. A smaller cohort of 3% proudly detailed an in-house dedicated team or individual, emblematic of a robust commitment to cyber security.

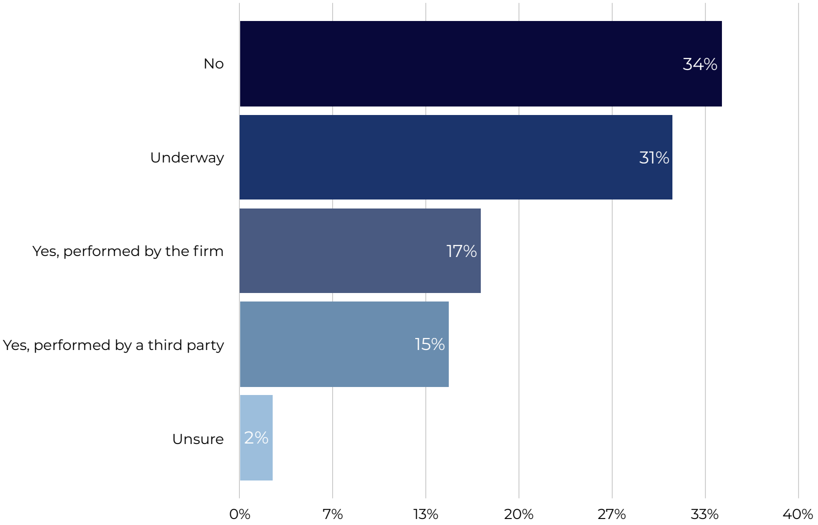
Do you have a designated individual or team responsible for managing and addressing cyber security risks and incidents for your firm?



FORTIFYING PREPAREDNESS & RESPONSE

Regarding published 'Cyber Incident Plans', one third (34%) noted their absence and underlined the need for staff comprehension. A commendable 31% were in the process of formulating such plans, evidencing ongoing endeavours to elevate cyber security. Encouragingly, 17% boasted executed and tested internal plans, while another 15% entrusted third-party entities with executing their cyber incident plans. A smaller fraction of 2% remained unsure of their firm's cyber incident plan. These insights highlight the diverse stages of preparedness, spotlighting the vitality of comprehending cyber incident planning and routinely testing these strategies for swift, effective responses.

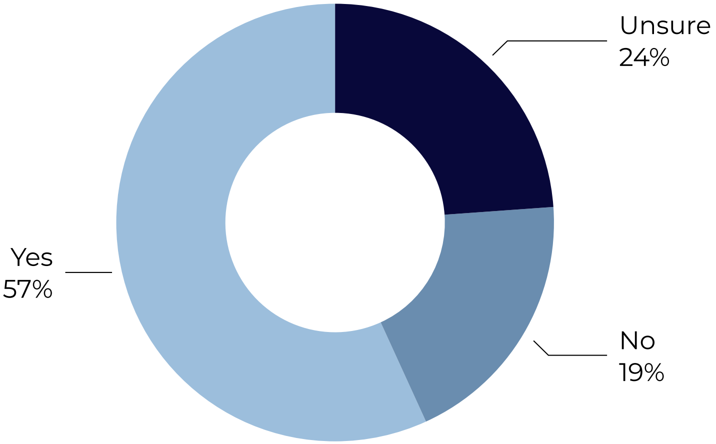
Does your firm have a published cyber incident plan that is well understood by your staff and recently tested?



CYBER SECURITY MEASURES

The survey's enquiry into perceptions about cyber security measures revealed varied perceptions a spectrum of viewpoints. A minority of 19% expressed scepticism, while a significant 57% affirmed their belief in their firm's robust safeguards. Of those surveyed, 24% remained undecided, suggesting a measure of uncertainty or unfamiliarity with the firm's cyber security protocols. These varied responses reflect the range of preparedness and awareness levels among legal professionals concerning the efficacy of cyber security measures.

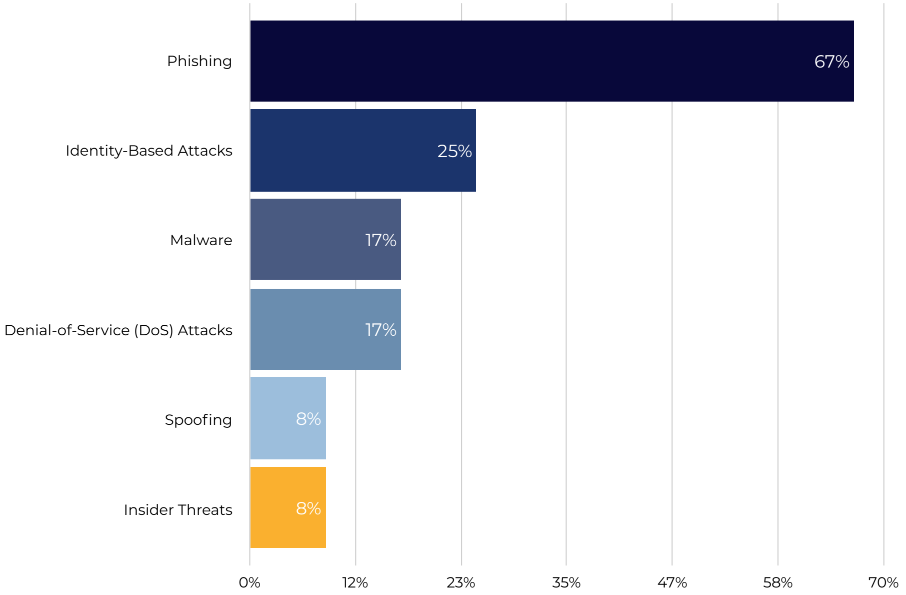
Do you believe your firm is doing enough to protect itself against a cyber attack?



CYBER ATTACKS ON LAW FIRMS

Over the last year, 14% of respondents shared an experience of cyber-attack attempts, while 86% remained untouched. Conversely, 86% remained untouched by such attempts, illustrating a commendable cyber security stance. Delving deeper, 67% fell prey to phishing attacks, while 25% were targeted by identity-based assaults. 'Malware' and 'Denial of Service (DoS)' attacks affected 17%, exemplifying the breadth of cyber threats. Spoofing attacks targeted 8% and 'Insider Threats' were reported by 8%. These insights stress the importance of multifaceted security strategies in countering an evolving array of threats.

What type of cyber-attack did your firm suffer?

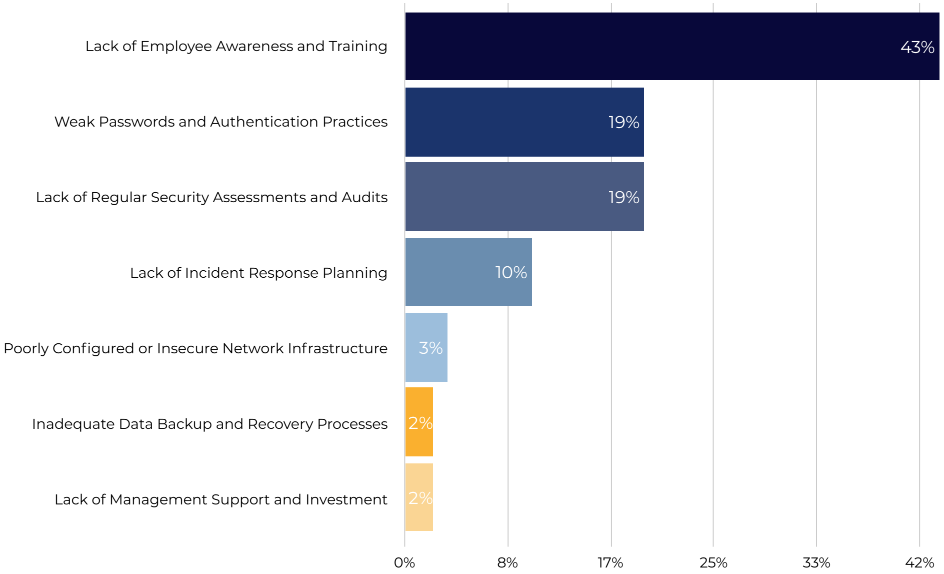


Code Injection Attacks, Supply Chain Attacks, DNS Tunnelling, IoT-Based Attacks, Other all 0%

IMPEDIMENTS TO BEING CYBER RESILIENT

Insights into the primary obstacles thwarting robust cyber security implementation uncovered diverse challenges. Notably, 43% identified 'Lack of Employee Awareness and Training' as a prominent hindrance. 'Weak Passwords and Authentication Practices' and 'Lack of Regular Security Assessments and Audits' concerned 19% of respondents respectively. 10% noted the absence of incident response planning, while 3% cited poorly configured network infrastructure. Inadequate data backup and recovery processes were flagged by 2%. An 8% minority pointed to a lack of management support and investment. These responses demonstrate the multifaceted nature of cyber security challenges and the need for comprehensive, proactive approaches.

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



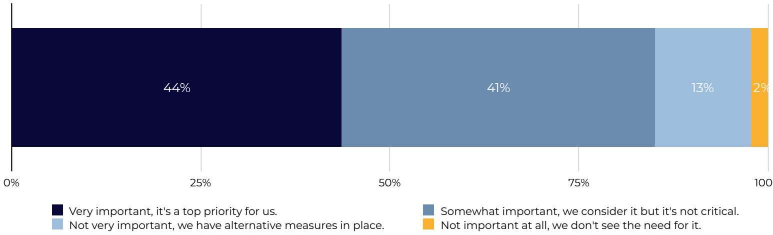
APPREHENSION ABOUT CYBER ATTACK IMPACTS

Conclusions regarding the potential consequences of cyber-attacks spanned a number of sentiments. A mere 1% conveyed minimal concern, while 17% exhibited modest levels of concern. Majority (46%) registered moderate apprehension. Crucially, 36% articulated profound concern, emphasising potential impacts on operations, reputation, and data security. These responses mirror a broad spectrum of readiness and awareness levels among legal professionals concerning the potential ramifications of cyber incidents.

DATA RESILIENCE & SOVEREIGN CLOUD INFRASTRUCTURE

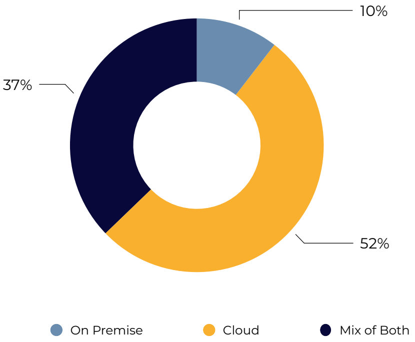
Addressing the importance of sensitive data storage within a sovereign cloud infrastructure, responses reflected diverse perspectives. A slender 2% deemed it unimportant, while 13% indicated alternate measures. 41% considered it somewhat important but not critical, and majority 44% elevated its importance, making it a top priority. The majority of respondents further indicated their firm data was hosted in the cloud (52%), with 37% indicating a hybrid of on premise and cloud. A minority 10% stated they stored data solely on premises.

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



LACK OF EMPLOYEE AWARENESS AND TRAINING

Is the majority of your firm data hosted on premise or in the cloud?

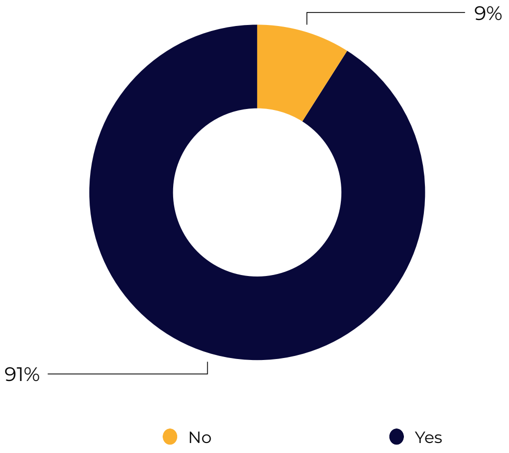


DATA & SYSTEM BACKUP

The survey results reveal a reassuring commitment to data security within law firms, with a resounding 91% affirming that they indeed back up their data and systems. This strong majority underscores the recognition within the legal profession of the importance of data backups. In an industry where the confidentiality and integrity of sensitive client information are paramount, data loss or system failure can have profound repercussions, both legally and reputationally.

It is heartening to see that the majority of law firms prioritise proactive measures to safeguard their digital assets. Nonetheless, the 9% who do not currently engage in data backups acknowledge of the potential risks involved and consider implementing robust backup strategies to protect their clients' interests and their own professional integrity. In today's digital age, data backups are not merely a precaution but a fundamental necessity in preserving the trust and reliability that clients place in legal practitioners.

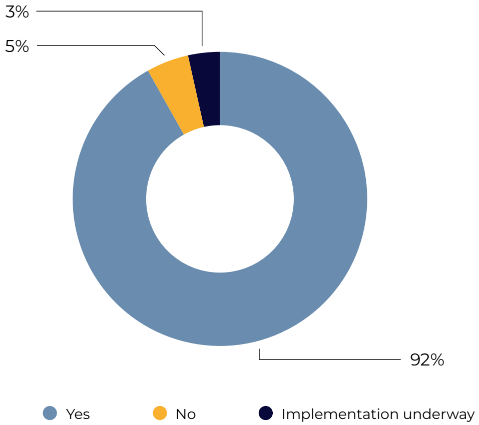
Does your firm backup your systems and data?



MULTI-FACTOR AUTHENTICATION

The high adoption rate of two-factor authentication (2FA or MFA) at 92% demonstrates its critical role in enhancing online security. By necessitating two forms of verification, 2FA provides an essential extra layer of protection beyond passwords, increasing the difficulty for unauthorised individuals to access sensitive accounts and information, thereby bolstering overall cybersecurity.

Do you use two-factor authentication (2FA or MFA) for your important online accounts, such as email or banking?

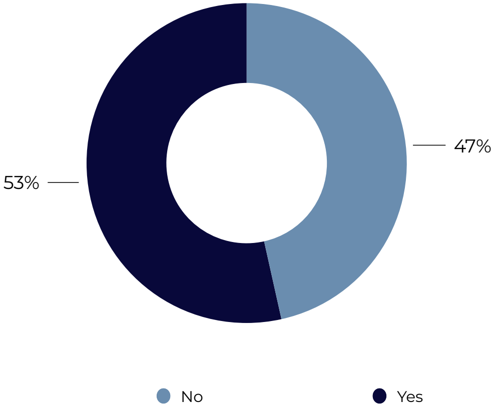


CYBER SECURITY FRAMEWORKS

Familiarity with the Australian Cyber Security Centre (ACSC) Cyber security baseline, Essential Eight was observed in 53% of respondents. The Australian Signals Directorate has developed prioritised mitigation strategies, to mitigate cyber security incidents and help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies is the Essential Eight.

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks. While the principles behind the Essential Eight may be applied to cloud services, and enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate in these environments.

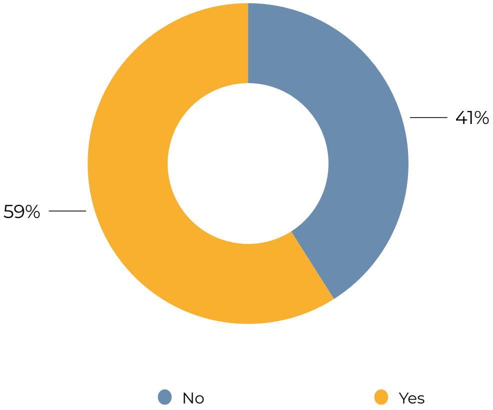
Are you familiar with the Australian Cyber Security Centre (ACSC) cybersecurity baseline, Essential 8?



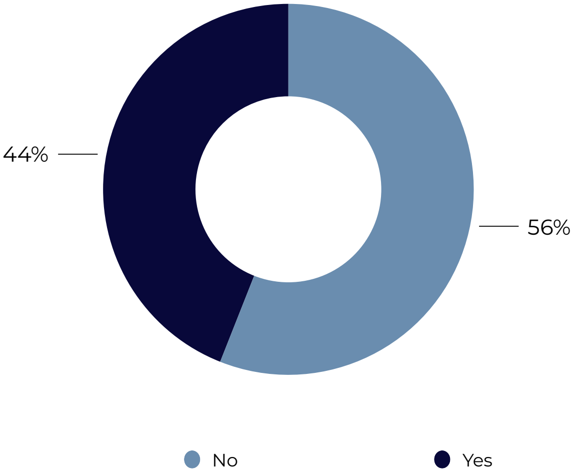
BUSINESS CONTINUITY PLANNING (BCP) & TESTING

The majority of firms (59%) responded positively to having a Business Continuity Planning (BCP) in place at their organisation. In the realm of cyber security practices, 44% engaged in regular penetration testing, while 84% conducted cyber security training. The significance of certifications such as ISO 27001 or SOC 2 varied: 9% found them not very important due to alternative measures, 20% prioritised them, 63% considered them somewhat important, and 8% dismissed them.

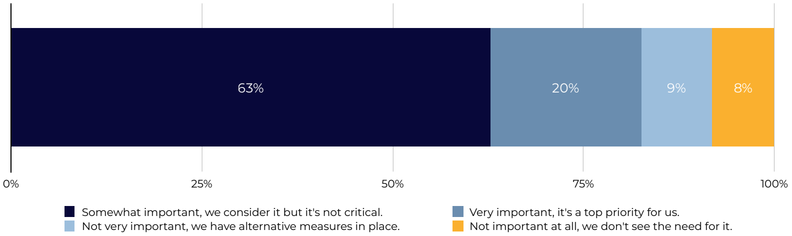
Does your firm have a business continuity plan (BCP)?



Does your firm conduct penetration testing?



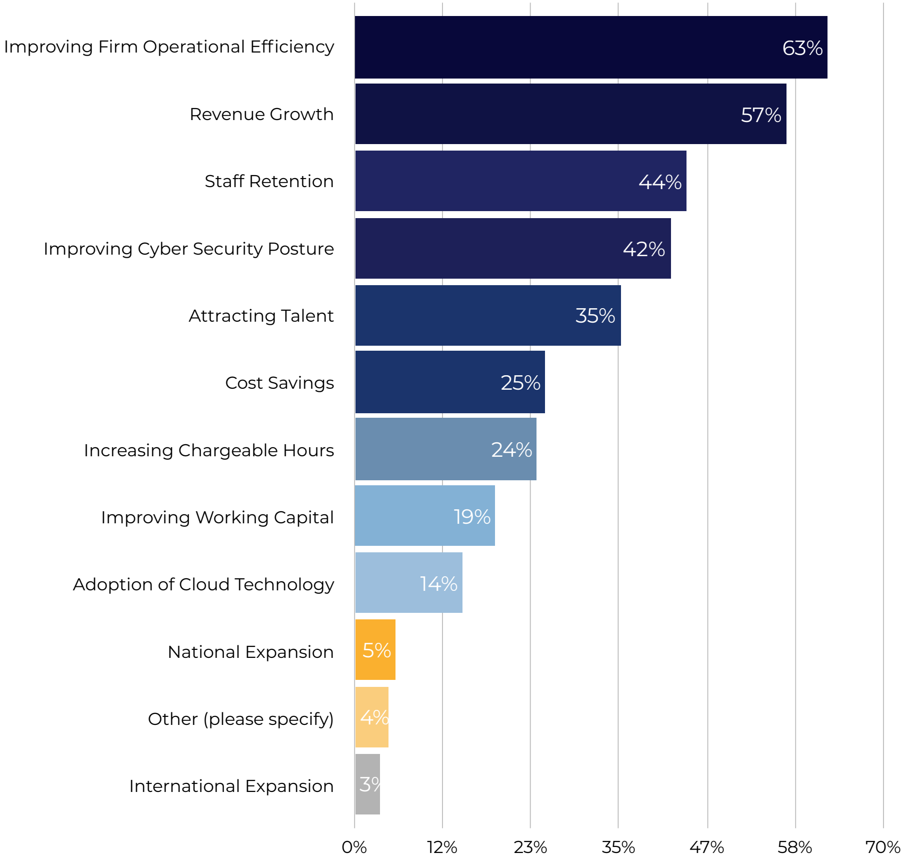
How important do you consider certifications, such as ISO 27001 or SOC 2, in ensuring the security of your business's data and systems?



FUTURE STRATEGIC PRIORITIES FY24

Respondents' priorities for financial year FY24 focuses on 'Improving Firm Operational Efficiency' (63%), followed by 'Improving Revenue Growth' (57%), 'Staff Retention' (44%) with 42% of respondents noting 'Improving Cyber Security Posture'. Over one third of respondents (35%) noted 'Attracting Talent' as a main strategic propriety for the year.

What are your firm's main strategic priorities for FY24?



CONCLUSION

Investing in cyber security for law firms in today's digital age, as highlighted by the findings of The 2023 State of Cyber Security in Law Report. The fact that more than half of respondents identified "Cyber Security" as their top operational challenge identifies the need for robust cyber defences within the legal sector. The evolving cyber threat landscape poses a significant risk, and law firms must take proactive measures to protect sensitive client data and maintain business continuity.

Furthermore, the challenges related to "Attracting Talent" and "Staff Retention," are closely tied to cybersecurity. Skilled professionals are crucial for implementing and managing effective cybersecurity measures. By investing in cybersecurity, law firms not only protect their clients' interests but also enhance their ability to attract and retain top talent in an increasingly competitive landscape.

The emphasis on "Information Technology (IT) Infrastructure Costs," underscores the critical role of technology in supporting law firm operations. Investing in cybersecurity is an integral part of maintaining a secure and efficient IT infrastructure. Firms must allocate resources to optimise, upgrade, and maintain their IT systems to ensure seamless connectivity, efficient processes, and adaptability in the face of evolving technological challenges.

This report revealed diverse levels of confidence in cybersecurity preparedness, with only 1% extremely confident and 44% highly confident in their security protocols. This variance in confidence emphasises the need for continuous investment in cybersecurity measures. With cyberattacks affecting approximately 14% of law firms in the past year, there is a clear need to fortify security strategies to mitigate risks and protect against potential disruptions, reputational damage, and data breaches.

In conclusion, the findings of this report highlight the imperative for law firms to invest in cybersecurity. The challenges and risks identified, coupled with the concerns about cyberattack impacts, emphasise the need for a comprehensive and proactive approach to cybersecurity. By prioritising cybersecurity measures, law firms can safeguard their operations, maintain client trust, and position themselves competitively in an increasingly digital and interconnected world.

AUCLOUD

AUCloud is an Australian owned and operated Cyber Security Managed Security Service Provider (MSSP) and Sovereign Cloud Service (IaaS) specialist that supports Australia's Legal industry, Governments, Critical National Industries (CNIs) and secure enterprise organisations with the latest sovereign cloud infrastructure, backup and cyber security threat defence and response services. AUCloud's Sovereign Cloud Service (IaaS) and Cyber Security Solutions are underpinned by a range of security certifications, including "Certified Strategic" on Digital Transformation Agency's Hosting Certification Framework (HCF), assessed to the PROTECTED controls of the Australian Signals Directorate's (ASD) Information Security Manual (ISM) through to the Australian Cyber Security Centre's Cloud Assessment and Authorisation Framework (CAAF), inclusive of the Information Security Registered Assessors Program (IRAP) certification and ISO 27001.

aucloud.com.au

LEXVERITAS

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

ALPMA

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

ALPMA

LEXVERITAS

AUCLOUD