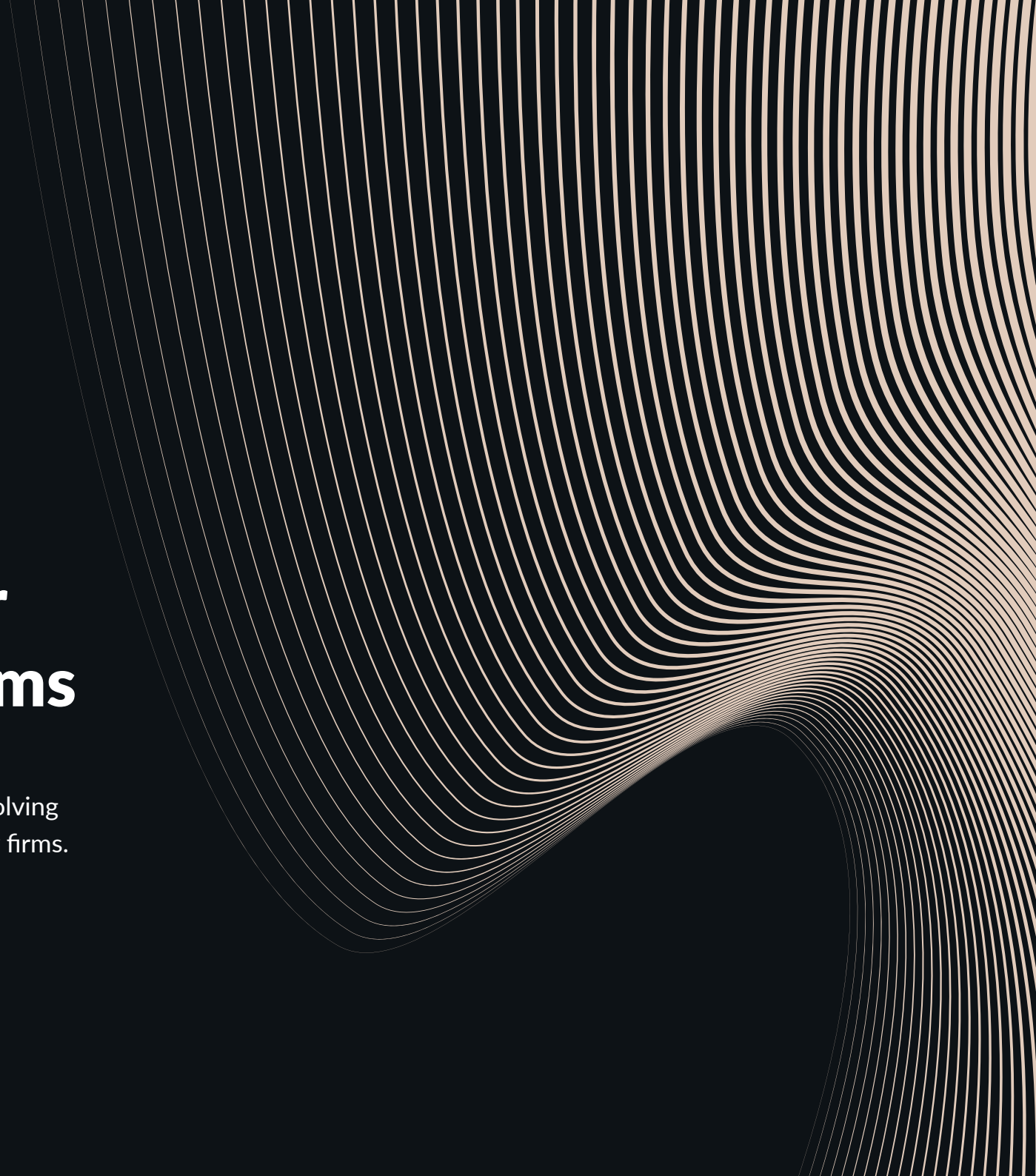
dotSec
dot com security

2023 State of Cyber Maturity for Australian Law Firms

Exploring the opportunities and threats of the evolving cyber security landscape impacting Australian law firms.



Foreword

This report presents the outcomes of a questionnaire presented to 386 businesses in the legal sector. The aim of the questionnaire was to assess the level of cyber security maturity among legal firms and to understand how these businesses perceive the role of cyber security in dealmaking, competitive advantage and operational robustness.

There is a growing body of evidence to suggest that the legal sector is becoming increasingly digitised:

- Increased use of technology in legal practice: Legal firms are increasingly adopting technology tools such as e-discovery software, legal project management tools, and virtual meeting platforms to streamline their operations and improve efficiency.
- Growth of online legal services: The rise of online legal services, such as online document preparation and remote legal consultations, has made it easier for people to access legal services from the comfort of their own homes.
- Increased use of electronic documents: The trend towards paperless offices has led to an increase in the use of electronic documents in the legal sector. This has improved the speed and efficiency of document management, but also presents new challenges for cyber security.
- The growth of e-filing: Many courts are now allowing parties to file documents electronically, which has made it easier and faster for legal professionals to submit their filings.
- These developments demonstrate that the legal sector is becoming increasingly digitised and that technology is playing an increasingly important role in legal practice.

Of course, these online and digital services depend heavily upon a mature approach to cyber security, due to the vast amount of confidential and privileged information, such as personal data, trade secrets, and financial records, that is collected, stored and managed by these online services.

The results of the questionnaire reveal that there is a varied level of cyber security maturity across the legal sector, with some firms demonstrating a high level of understanding and preparedness while others stating that they are yet to get up to speed and admit (with refreshing honesty!) that they manage their cyber security by “dancing around the maypole and drinking from the sacred cup of good luck each month when the moon is full!”

While many (around 30 per cent across the entire questionnaire) show a high level of cyber security maturity, the findings also indicate that there is a significant lack of cyber security awareness among legal firms. Twenty per cent of businesses are unsure about the role of cyber security in dealmaking, and 55 per cent indicated that their clients have never inquired about their cyber security. This suggests that many legal organisations may not understand the importance of cyber security, or do not see it as a priority when engaging with clients. However, the legal firms that use cyber security as an asset tend to attract clients who are concerned about the security of their information. This approach can help to build trust and confidence with clients and demonstrate the firm’s commitment to protecting their data.

Overall, the findings from this report suggest that cyber security remains a critical issue for legal firms. While some organisations have demonstrated a high level of preparedness and understanding, there is a significant gap in cyber security awareness across the sector. Legal firms that prioritise cyber security and take a proactive approach to protect their clients’ data are likely to be more successful in attracting clients and building trust. With cyber threats increasing in sophistication and frequency, it is essential that legal organisations continue to evaluate their level of risk and invest (according to that prioritised risk) in appropriate cyber security maturity-improvement strategies to not only stay ahead of the game but also to be seen by potential clients and partners as an organisation that can be relied upon with confidence.

Dr Tim Redhead
Director,
DotSec – Dot com Security

Introduction

Global threats from cyber attacks are growing with more and more of the Australian public focused on whether their information is safe.

Legal firms are one of the most trusted professions in Australia, but this could be impacted severely with threats of cyber attacks on the horizon.

Dotsec's inaugural *2023 State of Cyber Maturity for Australian Law Firms* report explores these issues within legal firms, with data from a quantitative survey of 386 firms.

The survey has been designed to collect insights across three key areas of a firm's cyber security life cycle, including motivations, maturity and management.

These three areas explore the fundamental elements required to create a safe, secure and successful legal firm in this evolving threat climate.

This is a robust, revealing and insightful report that will give legal practitioners a richer understanding of the current state of the market and the actions they can take to evolve their practice.

Table of Contents

Research Methodology

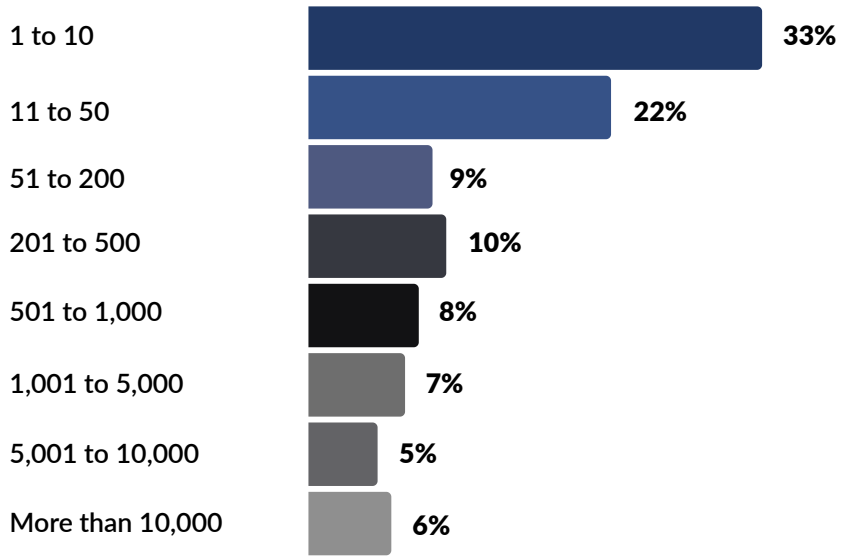
The 2023 State of Cyber Maturity for Australian Law Firms survey invited legal professionals to share their approaches, motivations, decision making, and management towards cyber security.

DotSec commissioned independent market research firm Momentum Intelligence to conduct the survey in collaboration with Lawyers Weekly.

The survey was conducted on behalf of DotSec by Momentum Intelligence between 8 September and 4 October 2022. The survey received a total of 500 responses, including a total usable sample of 384 fully completed submissions.

Therefore, the margin of error for the enclosed results is +/-4.99 per cent. This is an excellent level of accuracy for a study of this nature and provides a robust and rich source of data.

Company size



49% Solicitor/Lawyer

18% Partner

9% Corporate counsel

3% Marketing

2% Compliance manager

1% Human resources

1% Finance

16% Other

Key Findings

1

One in four organisations

are aware of a security breach in the last two years.

These respondents are in the minority, which should be encouraging, except that...

2

Only 48 per cent of legal professionals

are confident that their firm is able to detect and respond to security breaches.

This is less encouraging, so why is this the case?

3

Majority of legal professionals

are unsure of what security frameworks their organisation is compliant to.

4

Well, to start with, most respondents indicated a lack of understanding

of how cyber security can be a competitive advantage.

5

And while most respondents indicate a desire to improve or maintain their level of maturity

more than half of the respondents indicate that they do not undertake security maturity-improvement issues for various reasons.

Read on to see how we can better manage risk, and maybe even increase revenue as a result!

Motivations

This section explores the fundamental motivations for legal firms to invest in cyber security.

It outlines the drivers that are encouraging firms to take action and the opportunity for firms to leverage a mindset shift to turn threats into opportunities.

Respondents have a range of motivations for maintaining or improving their organisational security maturity

Most organisations are motivated to maintain or improve their level of cyber security maturity primarily by the desire to avoid the negative outcomes of a successful attack or data breach. This is the traditional reason for implementing a solid cyber security program, and it makes sense.

As we work our way down the other responses, however, we see an increasing level of cyber security maturity begin to emerge:

a) In the first case, we see respondents who need to satisfy the requirements of insurers, clients and interested or otherwise affiliated third parties. This is becoming an increasingly common motivation, especially with developments in director's liability, insurance and legislative requirements.

b) In the second case, we see highly mature respondents that recognise that having a solid, defensible, standards-based cyber security framework in place will make their practice a more attractive option.

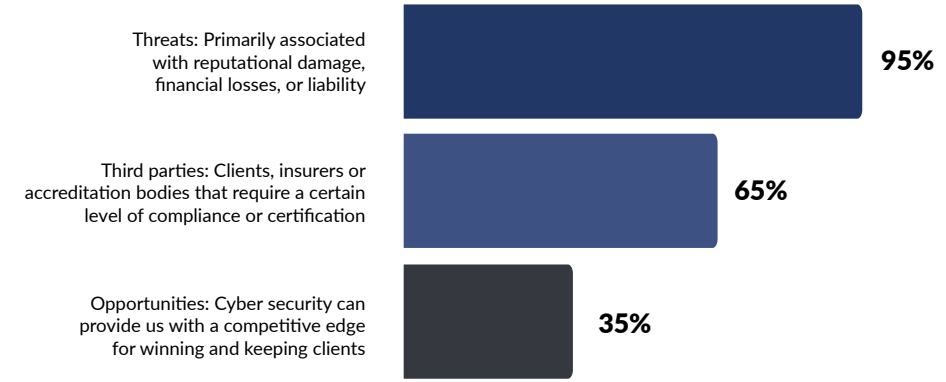
By adopting a standards and risk-based approach and proactively educating clients about cyber security, organisations can help clients understand the benefits of a mature approach to cyber security and increase their confidence in the security of their information.

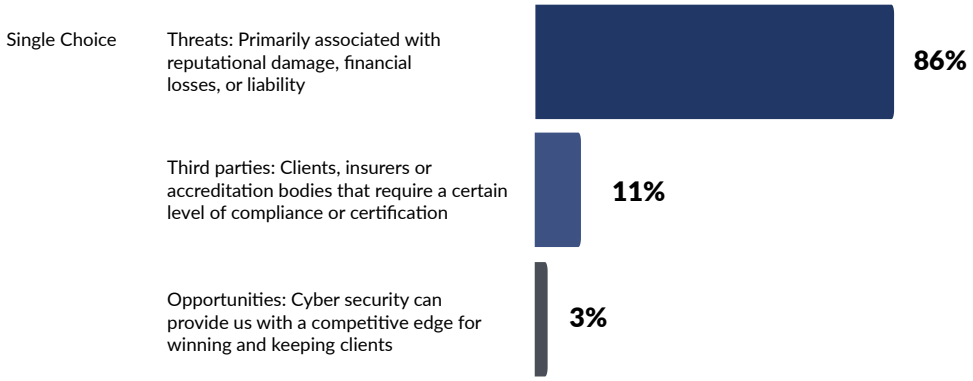
Key insights

- Risk avoidance (reducing the likelihood or consequences of an attack) motivates almost all respondents.
- As the number and severity of data breaches continue to increase, third parties will also increasingly inquire as to how their information is managed and secured.
- Some organisations have decided that competitive and cost advantages are to be had by proactively addressing their cyber security maturity improvement.

What are your organisation's motivations for maintaining or improving cyber security?

Sample size: 384 (All respondents)





Less than half of the surveyed legal firms consider cyber security to be a factor in winning or losing deals

Responses to the previous question (page 7) indicated that 65 per cent of firms have fielded questions from third parties regarding the firm's level of security maturity. In contrast, only around 35 per cent of the respondents to this question indicated that some or all of their clients ask about the firm's level of maturity. The reason for this apparent inconsistency is unclear, unless perhaps the difference (around 30 per cent) of inquiries indicated in the previous question were from non-client third parties such as insurers and compliance bodies.

Whatever the case, the fact that some clients have never inquired about their law firm's level of cyber security does not necessarily mean that clients don't care about or understand the concepts of cyber risk. It could just indicate that clients simply do not know how to ask about cyber, or that they trust the legal firms they are working with to take the necessary measures to secure their information.

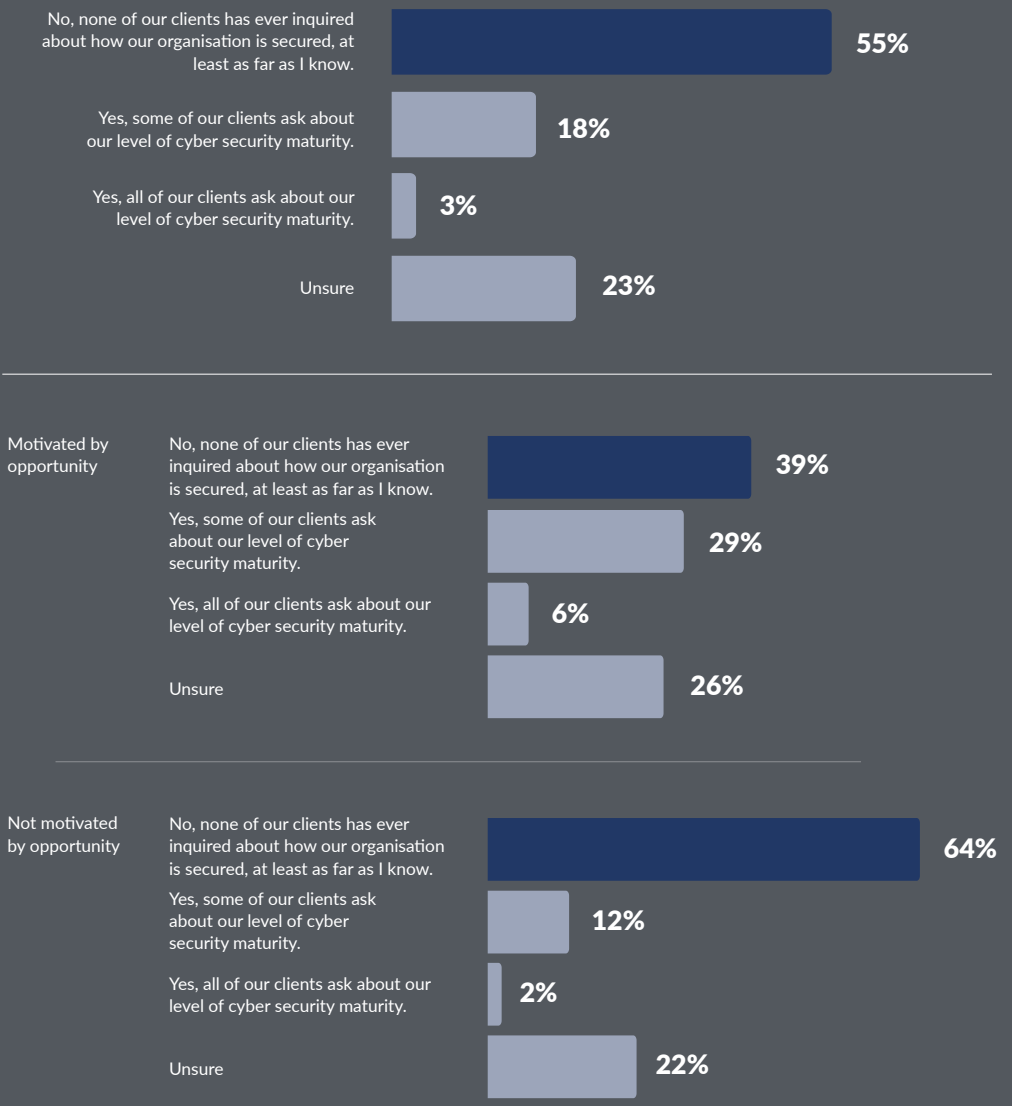
Australian reporting laws are very weak, especially when compared to the US, where most state data breach notification statutes require businesses or agencies to notify federal authorities and victims within 30 to 45 days of the determination of a breach. It seems likely that as Australian reporting laws mature, clients will become more aware of the importance of cyber security and start to actively ask about it.

Key insights

- The majority of respondents indicate that clients do not inquire about how the legal organisation is secured, "at last as far as I know". This uncertainty is somewhat inconsistent with the responses to the previous question, which show that 65 per cent of respondents field compliance questions from third parties.
- Around a quarter of respondents indicated that they were unsure as to whether or not clients inquired about the firm's approach to security. This is unusual as it indicates a lack of process and understanding within the law firm itself.

Has your organisation's cyber security been a factor in winning or losing deals in the last 12 months?

Sample size: 384 (All respondents)



Understanding the opportunity for growth and protection by investing in cyber security

Legal firms that have a culture of investing in cyber security at all levels are able to better articulate their unique proposition to their clients.

In a rapidly evolving threat landscape, there are clear benefits to investing in the protection of your information. However, with a small shift of focus and a clear articulation, alongside accreditation with compliance frameworks, legal firms can position themselves as a leader.

To move effectively on this journey, legal firms need to educate their staff in the importance of cyber security in relation to threats, compliance and opportunity of the investments.

External cyber security consultants can play an important role in these conversations to move the needle among senior decision–makers.

At DotSec, we take a holistic approach to understanding your firm's cyber security maturity and create a technical and cultural pathway for your firm to follow that will enable you to access the benefits of a more secure practice, with the benefits that follow.

3 ways to start a cultural change in cyber security:

1. Educate and influence your internal stakeholders to change the way they see cyber security by referring to risk and opportunity.
2. Encourage your firm to become accredited in standard compliance frameworks, in order to contain costs and overheads.
3. Speak with clients about your understanding of cyber security when articulating your firm's credentials.

Dr Tim Redhead
Director,
DotSec – Dot com Security

Maturity

This section explores the self-assessed cyber maturity of legal firms.

It outlines the level of awareness regarding the risks associated with security breaches, and the methods used to prepare for, detect and respond to security breaches. This section also examines leadership, threat management and overall compliance with best practice standards and frameworks, within legal firms.

1 in 4 organisations are aware of a security breach in the last 2 years

The responses reveal that almost 59 per cent of organisations are unsure if they have experienced a security breach. These law firms that were surveyed selected “not that I know of”, which indicates that these organisations may have limited organisation-wide incident detection and response processes, which enable employees to be knowledgeable in day-to-day actions and identify any risks or vulnerabilities.

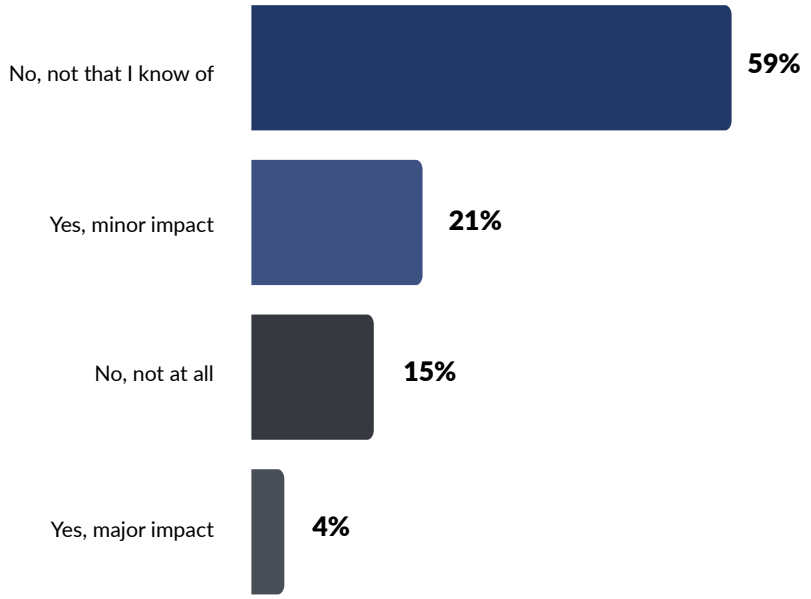
As IBM has shown in its 2022 report, in 2022, it took an average of 277 days — about nine months — to identify and contain a breach. (https://www.ibm.com/au-en/reports/data-breach)

Or as the saying goes, “The absence of evidence is not evidence of absence!”

On the other hand, 15 per cent of organisations have stated “not at all”, giving a clear indication that these organisations are completely aware of risks and are confident they have not been exposed to any risks or attacks in the last two years. These organisations are likely to have a set of policies and processes, combined with regular assessments organisation-wide regarding cyber security, incident detection and response.

To your knowledge, has your organisation been affected by a security breach in the last two years?

Sample size: 384 (All respondents)



Only 49% of attacks have been detected by internal discovery

This page shows that around a quarter of respondents (100 out of 385) indicated that they had detected and responded to a breach in some way. This is very interesting because 59 per cent of the responses to the previous question indicated that their organisation had not been affected by a breach, “at least not that they know of”.

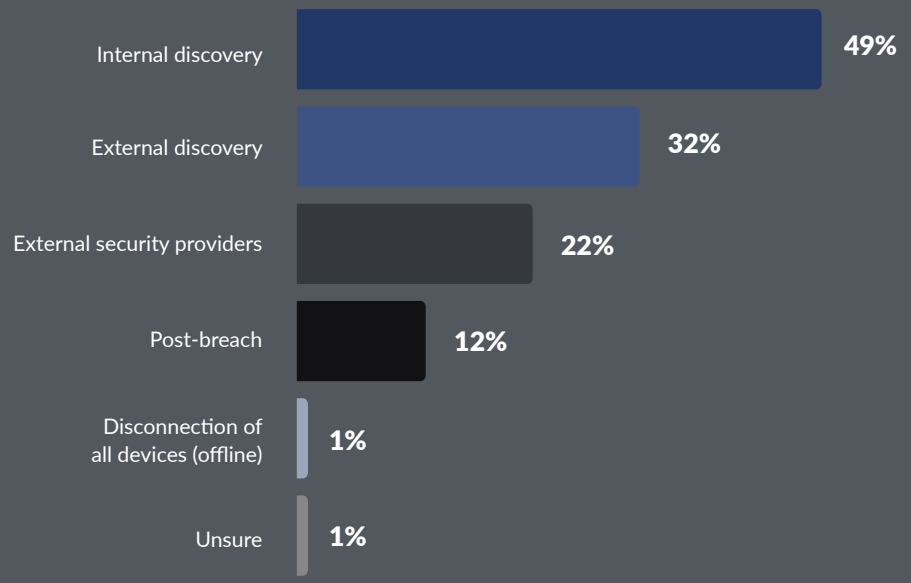
Whatever the case, a third of known breaches were discovered by a third party, such as a client or a bank, that was unrelated to the business’s cyber security function. That indicates that the attackers were at work within the firm, without the firm’s knowledge, and continued with their nefarious activities until the damage was discovered by a third party.

Key insights

- The responses summarised here show that 12 per cent of data breaches were discovered after the event rather than while the attack was taking place, and a third was discovered by a third party that was not a security service provider. This indicates that, despite the confidence indicated in the response to the question on page 15, some law firms need to develop and test more robust incident detection and response systems.
- Incident detection and response is a key component of all well-accepted cyber security standards and frameworks and is a key feature of a mature cyber security infrastructure.
- Organisations can use red team exercises to verify the effectiveness of their incident detection and response systems. The exercises need not be costly or time-consuming, but when conducted by experienced experts, they will always be informative and constructive.

How did you detect the breach?

Sample size: 100 (All respondents)



Your organisation can be impacted by a cyber security attack in 1 of 3 ways:

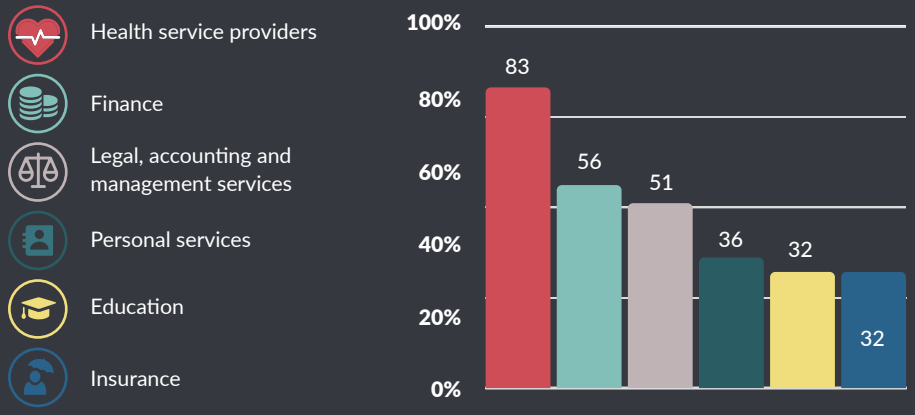
- **Target:** You are the target of an attack
- **Enabler:** You have the channel or medium in which the attacker reaches their target (client data, PII, etc.)
- **Collateral:** You happen to be in the blast radius of an attack when it is taking place; Wrong place. Wrong time.

Legal firms make up the third-most targeted sector

The *Notifiable Data Breaches Report* is a twice-yearly published report (January – June, July – December) by the Office of the Australian Information Commissioner (OAIC) that provides statistical information about data breaches.

Cyber attacks can happen against businesses across all industries and sizes. Unfortunately, law firms are becoming a key target for cyber attack perpetrators. From July to December 2021, legal service firms were one of the top three industries in Australia to report data breaches, with 51 incidents of attacks recorded by the Australian government's *2021 Notifiable Data Breaches Report*[1].

Top industry sectors to notify data breaches



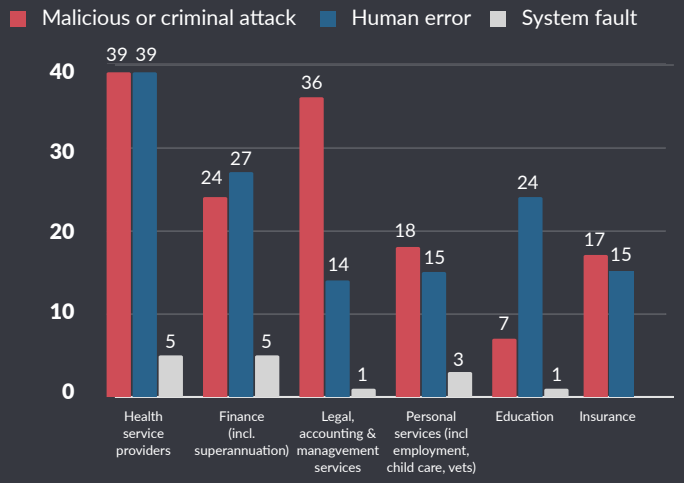
Notifiable Data Breaches Report (OAIC 2022)

[1] Office of the Australian Information Commissioner (OAIC). (2022). *Notifiable Data Breaches Report: July – December 2021*

More than 55% of breaches were due to malicious or criminal attacks.

In the recent reporting period (July – December 2021), the sources of data breaches were categorised by three segments. The majority of breaches (55 per cent) were attributed to malicious or criminal attacks, while 41 per cent of breaches were a result of human error. This was followed by system faults, which only accounted for 4 per cent of breaches[1].

The top three sources of attacks were phishing (compromised emails), which accounted for 32 per cent, stolen credentials, accounting for 28 per cent, followed by ransomware, accounting for 23 per cent[1].

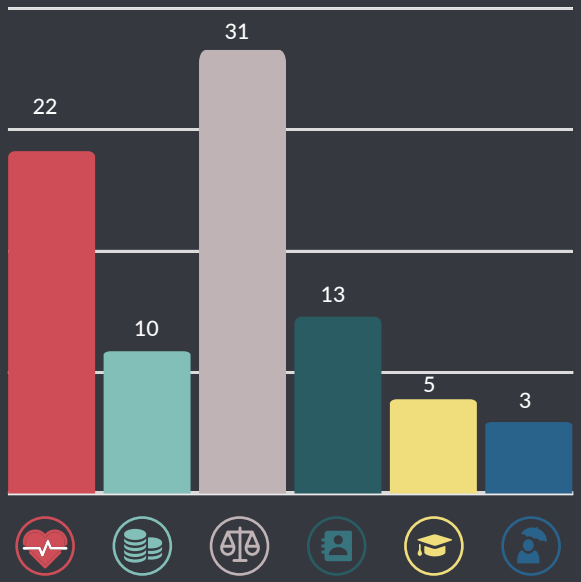


Notifiable Data Breaches Report (OAIC 2022)

The top industry sectors by sources of breach reveal that legal services are a heavily targeted sector, with malicious or criminal attacks being the leading source of breaches.

Legal services are the leading sector for cyber incidents

While health service providers have accounted for a larger volume of breaches, which include human error and system faults, legal services were by far the most targeted in terms of cyber incidents, accounting for 31 notifications of targeting breaches.



Notifiable Data Breaches Report (OAIC 2022)

Of the 31 breaches, phishing accounted for 10 breaches, followed by ransomware (9) and hacking (4). Legal services have surpassed all sectors regarding phishing, ransomware and hacking attacks. Some of the lesser methods of cyber incidents include malware, brute force attacks, and unknown methods of stolen credentials.

Phishing tips / how to build employee awareness:

It is an accepted fact that general security-awareness training is the cornerstone of any effective information security practice, and security awareness training is a key requirement in almost every security compliance framework and cyber insurance policy.

Educated personnel who are well-trained, engaged and alert to threats are less likely to be duped by clever attackers, meaning that your business is less likely to be caught up in reputational, clean-up and liability costs.

Dr Tim Redhead
Director,
DotSec – Dot com Security

Legal services account for the highest number of breaches across all sectors, which come from phishing attacks, ransomware, and hacking.

DotSec will work collaboratively to get the right training material to suit your needs. Don't make your users sit through hours of boring classes with irrelevant, overseas-based content.

DotSec delivers online (SCORM 1.2 or hosted) security awareness training, with local, Australian content providing your users with customised, online training program that provides regular reinforcement of your information security policies and procedures.

Back that up with regular testing (social engineering and phishing, for example) and refresher updates, and you have the cyber game sewn up!

51% of legal firms are not confident in their ability to detect and respond to security breaches

As with many of the responses in this survey, the responses to this question are split more or less down the middle: Slightly less than half of the respondents are sure that their detection and response capabilities are solid and tested, while more than half of the respondents are unsure of their incident detection and response capabilities.

Interestingly, 60 per cent of respondents (see page 11) are unsure if they have experienced a security breach; in light of that response, it would be expected that around 60 per cent of the responses to this question showed a lack of confidence in the organisation's incident detection and response capabilities, instead of the 51 per cent shown here.

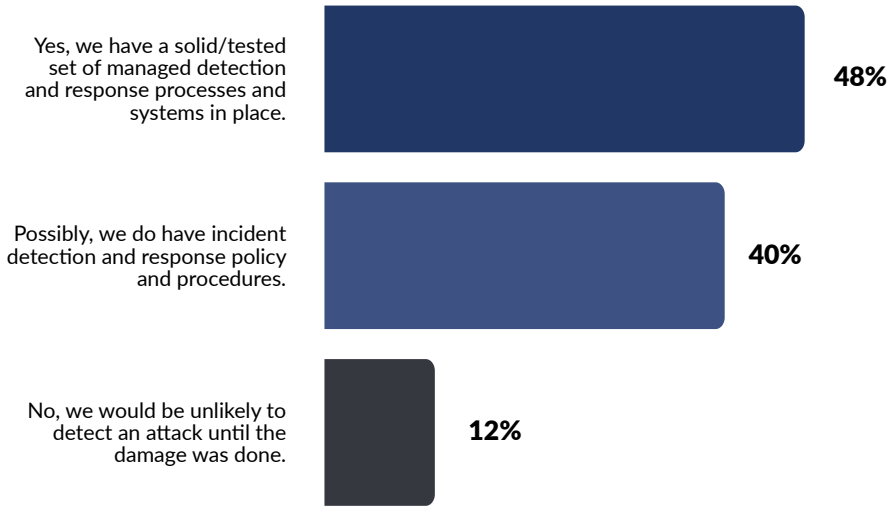
As IBM has shown in its 2022 report, in 2022, it took an average of 277 days — about nine months — to identify and contain a breach. (https://www.ibm.com/au-en/reports/data-breach). Or as the saying goes, "The absence of evidence is not evidence of absence!"

Key insights

- One in 10 legal organisations is confident that they could NOT detect an attack until after the damage was done. That is consistent with IBM's reporting, which has shown in 2022, a breach affecting 10 per cent of the respondents will likely see the attackers at work for almost a year before they are discovered.
- Insurance providers are likely to ask for evidence of a documented and tested incident detection and response, in the event that a claim is made for a cyber incident. This response indicates that between 11 per cent and 51 per cent of the respondents would be unable to provide such evidence. This shortcoming is likely to adversely affect the firm's ability to obtain reasonably priced coverage, especially following a breach claim.

Is your organisation able to detect and respond to a security incident?

Sample size: 384 (All respondents)



Three-quarters of the legal firms indicated that they are unsure of their compliance status, or are certainly not compliant

Security frameworks and standards exist to provide a common point of reference, allowing an organisation to be confident of its own security maturity while also being able to demonstrate that maturity to a client, partner, insurer or other third party. Only 30 per cent of respondents were confident that they were compliant with an external security framework or standard, such as ISO/IEC 27001:2022 or the CIS Essential Controls, but 75 per cent were either unsure or were certain that they complied with no well-accepted standard or framework.

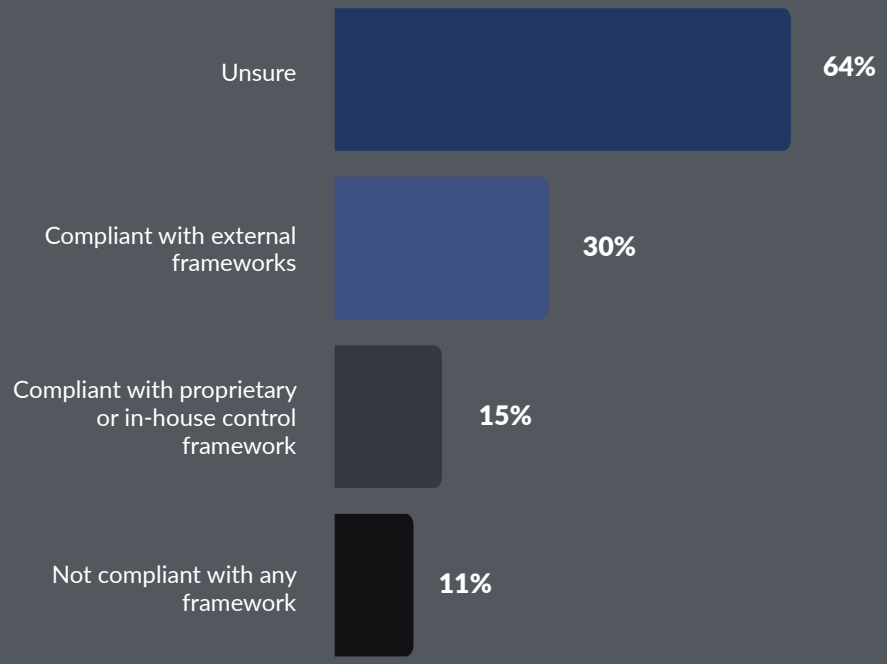
An organisation that fails to comply with a well-accepted, national or international standard or framework will almost certainly fail to have a holistic set of cyber security policies, procedures and controls in place. This, in turn, makes the attackers' job unnecessarily easy, and may also open the organisation up to accusations of failure to meet best practices, especially in the event of a security breach.

Key insights

- Thirty per cent of organisations are confident that they comply with an external security framework or standard, such as ISO/IEC 27001:2022 or the CIS Essential Controls,
- The response to this question is interesting when compared to other responses such as those summarised on page 18, which indicated that nearly 50 per cent of businesses felt that they had a strong risk-management system in place: Without reference to a national or international security framework or standard, it may be difficult for some organisations to justify that level of confidence to an interested third party.

Is your organisation currently compliant with any of the following?

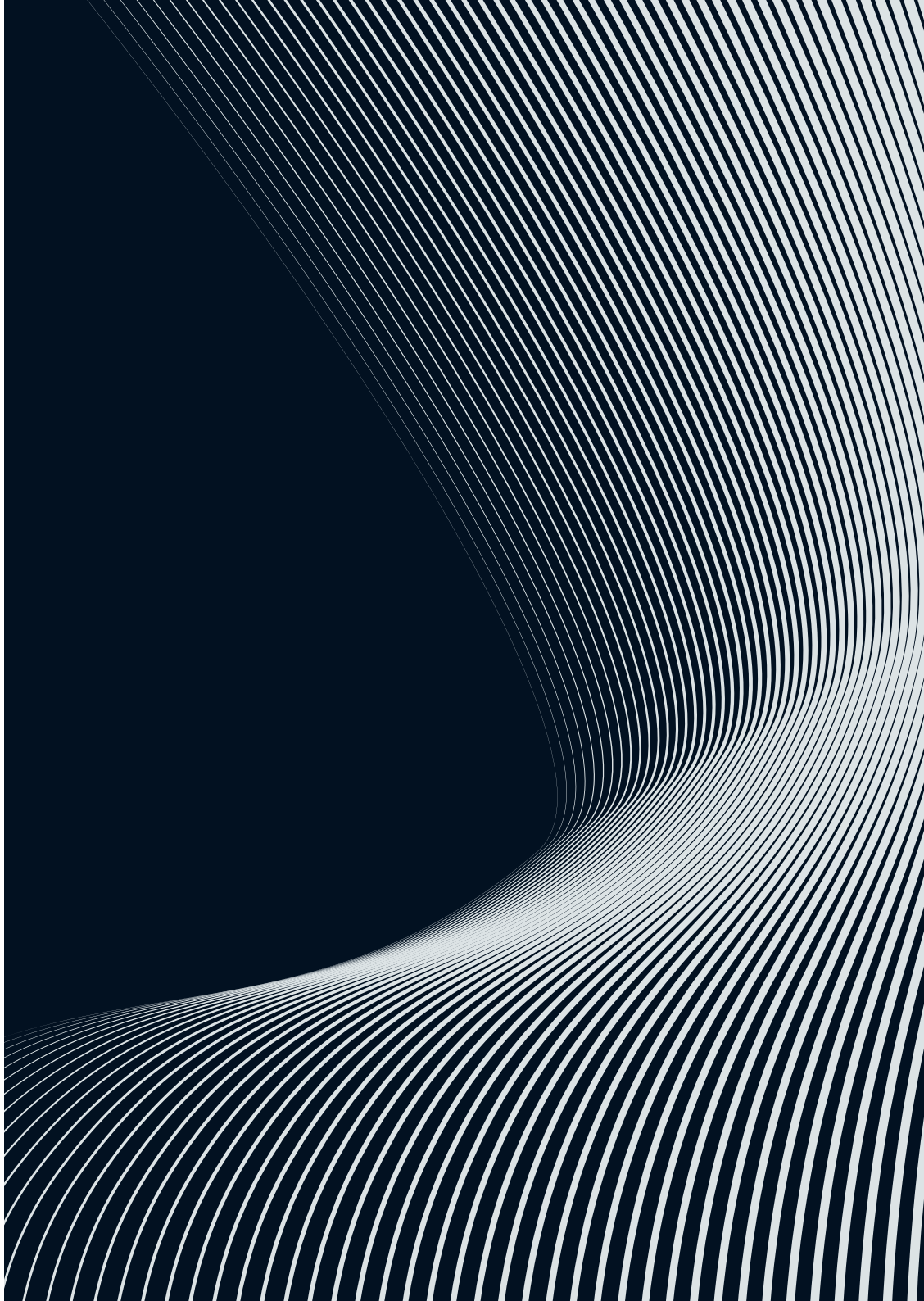
Sample size: 384 (All respondents)



Management

This section explores the management towards dealing with cyber security in legal firms.

It outlines the management approach to deal with cyber security risks in legal firms, the level of investment and obstacles regarding cyber security, and the key primary persons who are responsible for leading security in legal firms.



Most respondents are unsure of how to facilitate cyber improvements in a cost-effective way

Once again, the numbers are split more or less down the centre, with just under half the surveyed firms indicating that their investment in cyber security is in line with risk.

The remaining 52 per cent of respondents indicate that they do not undertake security maturity-improvement issues for one of three reasons:

1. A lack of understanding of options
2. A lack of a clear business case; or
3. A lack of affordable staff and consultants.

Issues associated with (1) or (2) can be addressed by undertaking a formula assessment of risk against a well-accepted national or international standard or framework. Security improvements should address risk in a cost-effective manner with reference to best practice; otherwise, money will be spent with no tangible maturity gain.

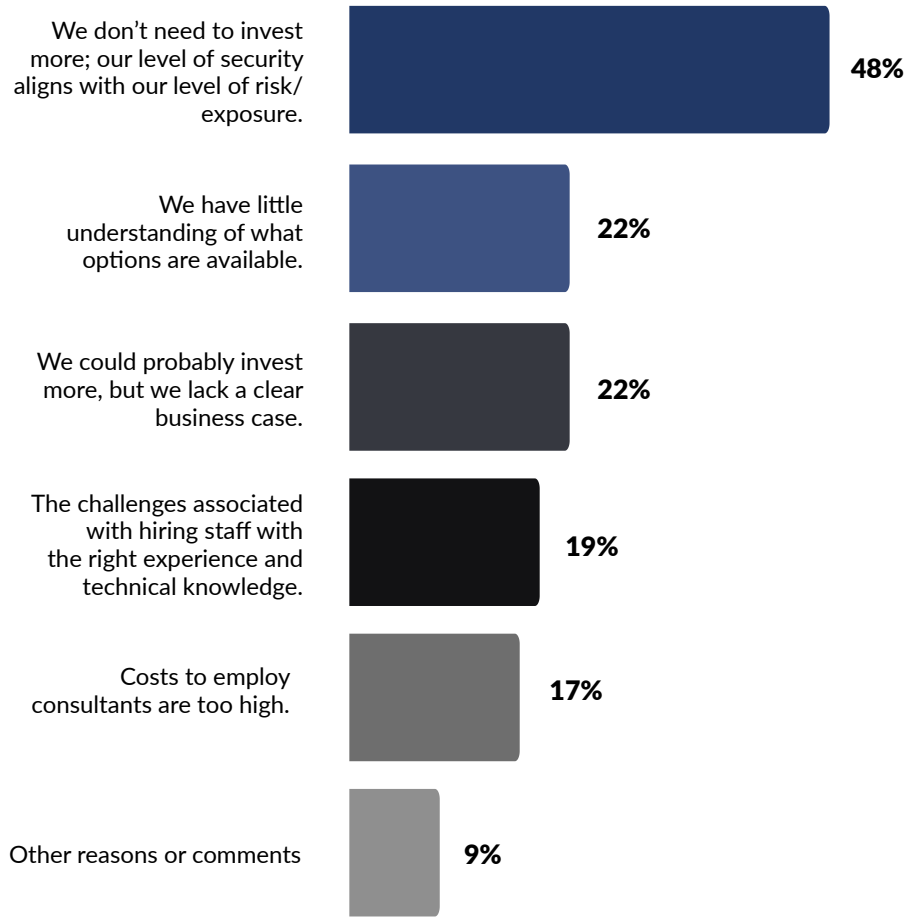
Issues associated with the cost or staff and consultants can be addressed by having a clear understanding of what the staff or consultants are to achieve, and that, in turn, will be based on the clear understanding of risk described above.

Key insights

- Any business can more effectively manage its cyber security costs if staffing and consultant milestones are tied clearly to risk-reduction goals, which in turn reference best practice standards and guidelines.
- Similarly, a business can better understand and prioritise its cyber improvement options if it identifies risks and then prioritises the management of those risks with reference to best practice standards and guidelines.

What is stopping your organisation from investing more in cyber security?

Sample size: 384 (All respondents)



Legal firms have varying levels of confidence in their ability to address and manage risks

The response to this question shows that the majority of surveyed organisations are adopting a comprehensive and proactive approach to cyber risk management, which is essential for effectively managing and improving the organisation's level of cyber maturity.

The response to this question may seem to be at odds with the responses to the previous question, which indicated that 70 per cent of organisations do not invest more in cyber security because they don't have a clear business case, they don't understand what options are available, and/or the costs of improvement are too high.

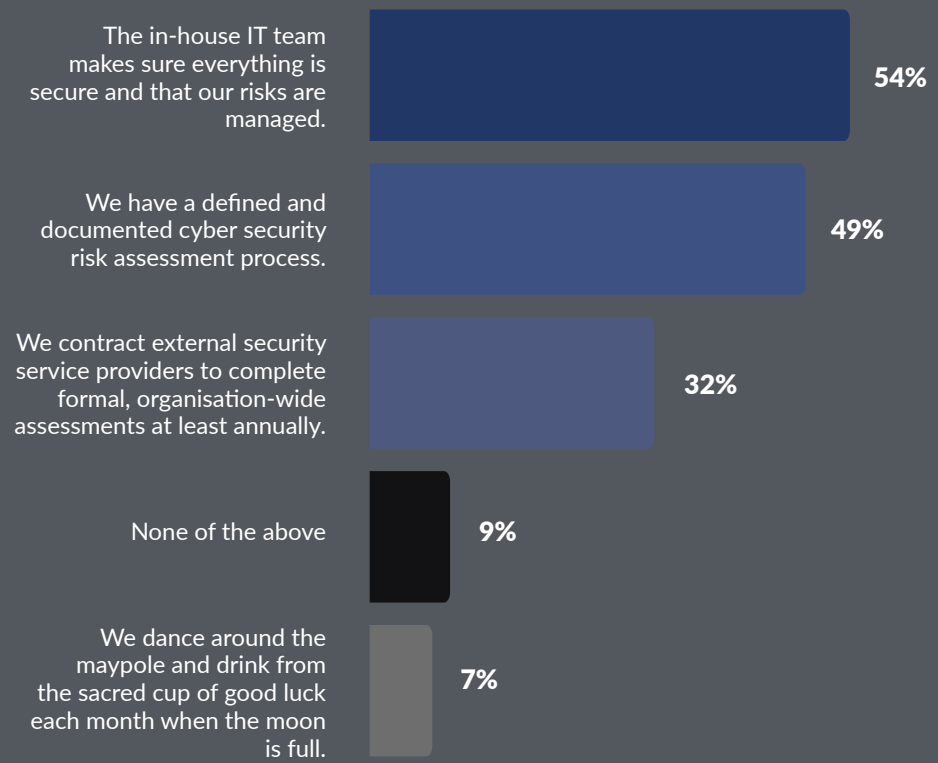
However, it seems more likely that the responses are consistent: Respondents have a management team that is committed to improving its level of security maturity, but that may not have a full understanding of the threat landscape or the latest technology and best practices that are available to address those threats. They may have taken steps to define roles and create policies, but may still struggle with the challenge of making a clear business case for further investment in cyber security.

Key insights

- Having clear roles, policies and procedures, and committed leadership all play important roles in ensuring that an organisation is protected against cyber threats.
- Organisations may be facing constraints such as budget constraints or limited knowledge of the options available to them, which may make it difficult for them to invest more in cyber security. This would explain the 16 per cent of respondents who have no formal risk management in place.

How does your organisation manage risks associated with cyber attacks?

Sample size: 384 (All respondents)



Legal firms have varying levels of maturity when it comes to assigning key roles, teams, policies and procedures

These statistics show a range of attitudes towards risk management within surveyed businesses, from those that are proactive and confident in their abilities to manage risks to those that may be neglecting the issue altogether.

The majority of businesses have some level of confidence in their internal risk management capabilities, an observation that is supported by the fact that around half the respondents have well-defined and documented procedures for assessing risks is a key component of effective risk management, indicating that they are taking the issue seriously.

Furthermore, 32 percent of businesses employ third-party contractors to verify their risk management efforts, highlighting the importance that some businesses place on having an external perspective and validation of their risk management processes.

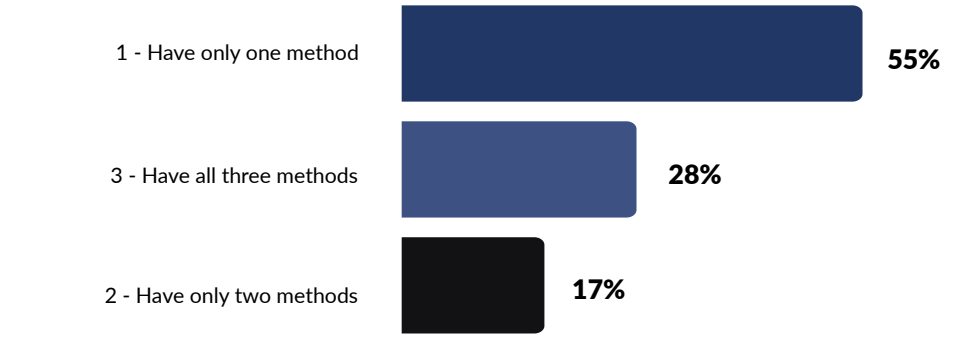
It should be noted that relying solely on the IT team to manage cyber risks can have its limitations. Cyber attacks are often multifaceted and can come from a variety of sources, including internal as well as external actors. This means that a comprehensive approach to risk management is needed, one that involves not just the IT team but also C-level leadership and the involvement of other departments and stakeholders within the organisation.

Key insights

- It is encouraging to see that 54 per cent of surveyed organisations have formally assigned risk management to either an internal team or a third party.
- It is also important to remember that (as shown in standards like ISO 27001) risk management is not a purely technical issue. Organisations should consider the limitations of relying solely on the IT team and to adopt a comprehensive and cross-functional approach to risk management.

Does your organisation have one or more of the following?

Sample size: 384 (All respondents)



There is a wide range of views as to which role is responsible for cyber security

The responses to this question are somewhat at odds with the responses to the question on page 19, which indicated that 54 per cent of the surveyed businesses relied on the IT team to "make sure everything is secure and our risks are managed". By contrast, the responses shown here paint a picture where only 37 per cent of businesses believe that the IT department is the primary driver for cyber security maintenance, reporting and improvement. There are a few ways to interpret this:

a. Around 54 per cent of organisations are mature and have a well-coordinated and effective approach to cyber security. In these organisations, business owners, partners, and C-level roles provide guidance and direction on cyber security strategy (53 per cent), while the IT teams are responsible for ensuring the strategy is implemented effectively and that all risks are addressed (54 per cent).

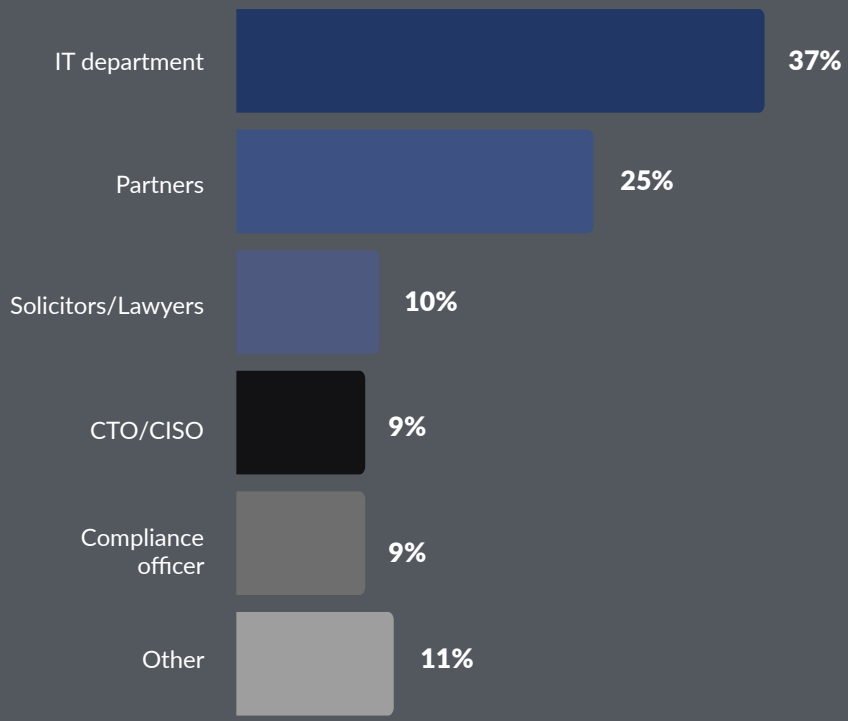
b. There is a lack of consensus and clarity on who is responsible for the organisation's security and risk management. According to this interpretation, there may be confusion, overlap, or gaps in responsibilities, leading to a fragmented and less effective approach to cyber security. This interpretation would be supported by the response on page 16, which showed that only 30 per cent of respondents were confident that they were compliant with an external security framework or standard.

Key insights

- In most cases, business owners, partners, and C-level roles are the primary drivers for cyber security, placing a greater emphasis on overall leadership and direction. This is a good thing!
- In some cases, there is a lack of consensus and clarity on who is responsible for the organisation's security and risk management. The use of national or international security frameworks or standards would help improve that situation.

What role in your organisation is the primary driver for maintaining, reporting on, and/or improving cyber security?

Sample size: 384 (All respondents)



Partnering with the same legal firms for up to 20 years: DotSec's collaborative approach to cyber security

Firewalls, anti-malware, cloud, data-leakage prevention, endpoint protection, SIEM/SOAR/SOC… this list of cyber silver bullets is endless, and there's always a new silver bullet to be sold. But to what end?

Evidence shows (more often now with the increasing number and severity of breaches) that sales-based cyber security doesn't work, at least not for the customer. Why? Because when products and services are sold without reference to a holistic, risk-based strategy, each one becomes just another solution, looking for a stand-alone problem to address.

But it doesn't have to be so: Instead of a sales-focused approach, DotSec has holistic, customer-focused, risk-based cyber security services to legal firms (as well as most other industry sectors and all tiers of government) for 23 years, and we started working with our oldest, ongoing legal client (a multinational business) in 2002.

A customer-focused, risk-based approach to cyber security improvement requires a significant investment of time and resources, as well as a deep understanding of the customer's specific needs and requirements. While such an approach might be seen as more challenging, we have found the customer-focused, risk-based approach to cyber security to be ultimately more rewarding, both in terms of the financial and reputation benefits that it can bring to both parties.

By framing people, processes and technology within an organisation's overall organisational and security strategy, DotSec has been able to effectively address the long-term security of our customers' businesses for over two decades.

DotSec — Do more business, more securely!

Options when looking to review or improve your firm's cyber security maturity

Respondents to this survey sometimes indicated that there were areas in which they might like to improve their organisation's information security maturity, but that they were uncertain how to proceed in a cost-effective way. Here are some ideas to consider:

a) There are no silver bullets! Cyber security is BIG business at the moment, and vendors, agents and resellers are on a feeding frenzy of *Jaws*-like proportions! But don't be seduced by the salesperson that offers you the next and greatest silver bullet: WAF, XDR, EDR, cloud, vulnerability management, NDR, SOC, NOC, SIEM, and everything else that you can buy is likely going to be a waste of money if you buy it as a silver bullet, a solution looking for a problem. Hang on to your cash until you've considered the next few points!

b) What do you want from me now? That is the question you should hear from anyone who purports to be able to increase your organisation's level of cyber security maturity. No two legal firms are the same; similar, perhaps, but not the same, and so there is no one product, solution or approach that is suitable for all would-be clients. The first thing for the would-be supplier to do is to understand (deeply) the particular requirements and operational details and constraints of the business in question. Only then is it possible to understand and prioritise risks, and only (ONLY!) then is it possible to agree on a plan (perhaps involving products, procedures and/or services) that will meet the client's requirements by addressing risk to an acceptable level, within an agreed time and budget.

c) He who represents himself has a fool for a client. It's a saying taken from law, but it holds just as true in cyber security. So many "specialists" are so confident in themselves that they'll recommend an approach because that's what they feel (probably honestly, but whatever) is right, because a vendor taught them (in pre-sales engineering training) that was right, or that they think it's the approach that XYZ company used and no one has ever complained about it before. Just because Tim from DotSec says that log collection and monitoring are important, who cares? And who even is Tim from DotSec, anyhow? Look for an approach that aims to improve your organisation's level of cyber security maturity by prioritising and addressing risk with reference to a reputable, national or international, preferably vendor-neutral, standard or framework. We've listed a few good examples in this report so you have a head start!

Cyber security is, in some ways, a rapidly evolving field, and many commentaries seem to be designed to achieve little more than hype up the FUD*. It's good for sales but doesn't really help. So consider the above points, stand firm in the swirling panic, and set your own course. And have fun with it!

*Fear, uncertainty and doubt.

About DotSec

DotSec is a professional cyber security organisation that works with national and international clients across most industry sectors and all tiers of government. DotSec offers a wide variety of cyber security services, which include security testing, managed security, integrated security, and also cyber security training for governments and organisations.

Book a consultation call today by visiting
https://www.dotsec.com

dotSec
dot com security

2023 State of Cyber Maturity for Australian Law Firms

Exploring the opportunities and threats of the evolving cyber security landscape impacting Australian law firms.