LEXISNEXIS 2019

DECODING CYBERSECURITY:

Clause & Effect

Roadshow Report

LexisNexis®

LEXISNEXIS 2019 ROADSHOW REPORT
DECODING CYBERSECURITY: CLAUSE AND EFFECT

Findings show that the legal industry has a good grasp on the issues and practices required to maintain secure digital systems, but there is still some way to go. There must be an ongoing focus on the people, processes, and technologies of businesses in order to build and maintain good cyber resilience - and this can only be achieved through greater education and awareness-building at all levels of the organisation.

SUMMARY

The legal industry is at the forefront of advances and changes in the cybersecurity arena - acting as a trusted advisor to businesses, but also grappling with these same changes from the perspective of its own cyber resilience. Legal professionals are uniquely positioned to identify the technological, legislative and organisational challenges that are pertinent now, and in the future.

Based on the 2019 Roadshow Cybersecurity Survey ('Survey') of 250 legal practitioners, LexisNexis hosted panel discussions with legal, cybersecurity and data privacy industry thought leaders across Australia to explore the current landscape of cybersecurity and the law. Live polling of attendees was conducted at each event.

Decoding Cybersecurity: Clause and Effect examines the issues around cybersecurity for the Australian legal industry in 2019. It distils quantitative and qualitative data taken from a diverse range of Australian legal professionals on topics including Australia's legislative environment, compliance for businesses, issues specific to the legal industry, as well as recommendations for best practice now and in the future.

INTRODUCTION

It's fair to say that the legal industry is at the forefront of the rapidly-changing practices and threats involved with modern cybersecurity.

Lawyers and law firms play a crucial role in advising businesses on how to manage their digital defences and how to manage their responses if (and when) those defences are breached amidst a complex, and at times ambiguous, domestic legislative environment.

The flip side of this coin is that firms and other legal businesses must also manage these risks for themselves, though it seems that at times lawyers may need to work harder on practicing what they preach.

We explored these issues and more through a survey of 250 Australian lawyers, and six panel events around the country that brought together some of the best legal minds in the cybersecurity space - and I'm pleased present the culmination of that work in our 2019 Roadshow Report, ***Decoding Cybersecurity: Clause and Effect.***

There were a number of fascinating insights garnered throughout this process, but perhaps two that stood out above the crowd.

The first is the role that human error plays in cybersecurity. From mistakenly clicking a phishing link to recklessly transmitting sensitive information through insecure platforms, more often than not there is a human at the start of any data breach.

The second is the absolute importance of incident response planning. Modern businesses are not expected to be immune to data breaches, but it is entirely unacceptable for them not to be prepared.

These points were raised repeatedly throughout the panel discussions, and are issues that Australian businesses are now coming to terms with - helped in no small way by the legal industry.

There was also consensus that current Australian cybersecurity legislation could be described as convoluted, with few laws dedicated specifically to fighting cybercrime, but a number of existing regulations in the data privacy space - which can often cross over each other and cause confusion when deciding which laws are actually applicable.

Looking to the future, there are recommendations for changes to how we treat data under the law and what rights we assign to it, and a call for greater collaboration within the legal industry to share knowledge in order to continue defining and refining best practices for the benefit of all.

One thing seems certain - the legal industry has its work cut out in this space.

We hope you enjoy the report.

Simon Wilkins

Managing Director, LexisNexis Australia

CYBERSECURITY

THE LEGAL LANDSCAPE

CYBERSECURITY

THE LEGAL LANDSCAPE

> **When you're looking at cybersecurity and keeping customer data confidential, it's no longer about fines and embarrassment. It's become a bet-the-company situation.**

John Swinson, Partner, King & Wood Mallesons

The fundamentals of cybersecurity are essentially the same as they were 20 years ago. Hackers (usually State-sponsored, criminal gangs, or hacktivists) seek to find vulnerabilities in an entity's systems in order to acquire data that they can use to their advantage. Most often the greatest vulnerability in an organisation's systems is its people and thus human error - both unwitting and negligent - remains a significant contributor in many data breaches. This can be seen by how prevalent hacks which use human error as an entry point (such as phishing) are today.

What has changed drastically in the last 20 years is the prevalence of technology and data into every facet of modern life. It's fair to say that almost every modern business can now be classified as a data-driven business, from online platforms to brick-and-mortar retailers, and with this transition has come a much greater appreciation of the value of data.

Data is now one of the most valuable commodities in the world, and solid ability to handle data and maintain robust cybersecurity practices are now viewed as a competitive advantage in the business world. Panellists at the Decoding Cybersecurity: Clause and Effect events reported that digital security has become an integral part of any pitch process, with potential clients routinely asking to see a firm's credentials before making any decision.

> **The majority of businesses these days are actually data-driven whether they realise it or not... so without understanding the value of that data, how can you possibly protect it?**

Yvonne Sears, Director, ISDefence

Thanks in part to a number of high-profile hacks and breaches, the world is truly beginning to understand the value of data. For businesses, this is essential - an understanding of what data the business holds, where it is located, who is responsible for it and what could happen if it falls into the wrong hands is crucial to preparing cyber resilience and incident response strategies.

To this end, there are a number of common issues the Australian legal industry is assisting clients with:

- **Handling of new legislation such as the Notifiable Data Breach (NDB) scheme or the General Data Protection Regulation (GDPR) where applicable.** The NDB is currently having a significant impact on Australian businesses, particularly from a compliance standpoint and dealing with issues like what constitutes a notifiable breach, or what steps need to be taken in notifying the relevant authorities.

- **Responding to regulatory investigations, such as those from the Office of the Australian Information Commissioner (OAIC).** This dovetails with the development and positioning of regulatory strategies for clients, as well as negotiating undertakings on their behalf and achieving the desired outcomes.

- **Navigating the large number of new cyber-focused products - particularly insurance - on the market.** The legal industry is becoming more involved with the procurement of these products and ensuring that they will be fit for purpose and provide the requisite cover when it matters.

- **Increasing capability at board level around cyber risk. Cybersecurity is no longer purely the realm of the IT department - it concerns the whole company.** Directors and administrative staff alike must be well-versed in the regulation and process of cybersecurity in order to be adequately prepared to make decisions.

- **Developing, testing and refining response plans and running drills for clients.** The importance of this will become evident as a key theme throughout this Report.

> **We're much more likely to do a fire drill than a data breach drill. And when I say drill, I don't mean testing if people can spot a phishing email. I mean getting the senior executives in a room and running a ransom demand scenario and seeing how people react.**

David Yates, Partner, Corrs Chambers Westgarth

Hacks and data breaches are becoming more common and more complex. There is broad agreement across the legal industry that these days no business is expected to be invincible against cyber-attack. They are, however, expected to be fully prepared and to be able to respond in a timely and fitting manner.

Whilst best-practice cybersecurity must be observed by businesses of all sizes, the reality is that closing all vulnerabilities in a company's systems is a nigh-on-impossible task. Breaches can come through any gap - from phishing to exploitation of holes in the security of third-party suppliers or contractors. In the court of public opinion, the responsibility for data breaches will ultimately sit with the business that faces the customer and for this reason, the focus in the legal industry (and businesses at large) is on response rather than prevention.

LEGISLATION

AUSTRALIA vs THE WORLD

LEGISLATION

AUSTRALIA vs THE WORLD

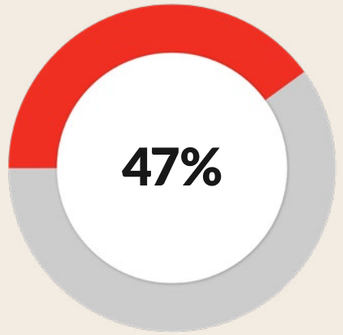
“There have been a number of laws that have been very slowly adapted or have evolved over time, but we don’t have a Lord of the Rings type one piece of legislation which covers it all. We have a series of different laws at both State and Commonwealth level which try and regulate cyber activity together.”

Dudley Kneller, Partner, Gadens

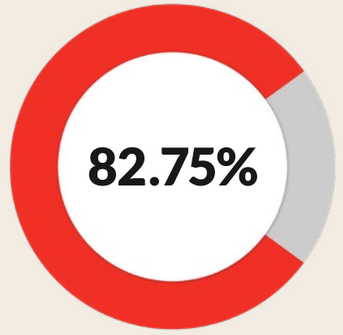
“The reality is that there are actually quite a lot of data laws, but there is a gap in the sense that there is no harmonised or clear cybersecurity law in Australia.”

Raavi de Fonseka, Partner, Johnson Winter & Slattery

WE NEED BETTER LAWS



THEY ARE INSUFFICIENT



When asked whether Australia’s cybersecurity laws provide adequate protections, results were greatly different between event attendees (82.75% of whom think they are insufficient) and Survey respondents (47% saying we need better laws). There was, however, agreement amongst panellists that a lack of harmonised or dedicated cybersecurity laws in Australia means that there is now a poorly aligned patchwork of legislation that is used to govern actions in the digital space. For example:

- Existing criminal codes can be used to cover digital offences. The crime ‘Receipt of stolen goods’ was notably used by the Australian Federal Police in June 2019 as the basis for a raid on ABC headquarters - the ‘goods’ in that case being digital files received by journalists.
- Sector-specific legislation such as the Telecommunications Act 1997 (Cth) or the Security of Critical Infrastructure Act 2018 (Cth) imposes guidelines and obligations around reporting of security incidents that are reasonably extended to digital activities.
- Directors who do not exercise due care and diligence in ensuring the cybersecurity of the Company could be in breach of their statutory obligations under the Corporations Act 2001 (Cth).
- There is growing pressure from regulators such as ASIC, APRA and the ACCC, who now include cyber resilience as part of the risk management and disclosure obligations for entities in their respective sectors.

“So, is it more laws, is it better designed laws, is it just more creative applications of what we have? I think that’s the real question.”

Alex Hutchens, Head of Technology, Media and Communications, McCullough Robertson

The Privacy Act 1988 (Cth) could be described as the 'go-to' piece of legislation when people consider Australian cybersecurity law. The recent inclusion of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) has made it the most comprehensive piece of legislation relating to data-handling in Australia, and is considered by many as Australia's answer to Europe's General Data Protection Regulation (GDPR).

The GDPR is currently hailed as the gold standard of international data protection law, and whilst the Notifiable Data Breach (NDB) scheme has been hailed as a step in the right direction, there is agreement in the legal industry that the legislation has some shortcomings, namely:

- As an amendment to the Privacy Act, the NDB scheme does not apply to State or Territory-based authorities, businesses with an annual turnover of less than $3 million or registered political parties (with some exceptions). There is currently no similar legislation governing data-handling obligations for these entities.
- The NDB does not contain provisions for the 'right to be forgotten' - or the right of an individual to have all personal data deleted by an organisation on request. This was a key right in the GDPR and there are calls for the same protection to be applied in Australia.
- The potential fines outlined in the NDB have been criticised as too small to be of serious concern to some larger organisations. Currently the maximum fine is $2.1m, which pales in comparison with the 4% of turnover outlined in the GDPR (currently the maximum fine suggested under the GDPR is £183m for British Airways).
- There is question around the subjectivity of what constitutes a 'significant' breach. If businesses were to treat all breaches as significant they would run the risk of inducing 'notification fatigue' in their customers, but if they fall the other way they risk infringing their obligations under the NDB.

Australia is also finding the balance between issues of national security and principles of individual privacy in the cybersphere. This has perhaps been most notable in the debate over the recently passed Telecommunications and Other Legislation (Assistance and Access) Act 2018 (Cth), commonly known as the Encryption Act.

Results from both live polling (85% agreement) and the Survey (72% agreement) found that the Australian legal community is heavily of the opinion that the Encryption Act potentially opens the door to privacy breaches, focusing mainly on two areas: encryption busting and law enforcement secrecy.

Encryption

The Encryption Act contains provisions that could require tech operators or service providers to de-encrypt certain communications, but draws a line at what it calls 'systemic vulnerabilities' - backdoors that would compromise wider encryption. There are concerns that any encryption busting would necessarily exploit weaknesses in existing software which, if put in the wrong hands, could be easily replicated on a large scale. Comparisons were drawn to the 2017 NotPetya malware attack - a piece of malicious software which originally started as a security exploit designed by the National Security Agency in the United States. It was leaked online, weaponised by Ukrainian hackers and went on to become the most costly malware attack in history.

Secrecy

There is concern amongst the legal industry around the transparency of the Encryption Act. Previously, intercepting a telecommunication involved a robust process including probable cause, warrants, and clear judicial oversight to prevent overreach. The general consensus from the legal industry is that as this new legislation applies largely to Australia's intelligence organisations this oversight is unclear, and in some cases, lacking entirely.

Without doubt, legislation such as this must tread a thin line between the individual right to privacy and national security, but there are questions as to whether this particular Act has got it right.

COMPLIANCE

THE BALANCING ACT

COMPLIANCE

THE BALANCING ACT

“Cyber threat is very high. The World Economic Forum released the Global Risks Report for 2019 … and rated cyber attacks as the 5th biggest risk to the world in terms of likelihood and 7th biggest risk in terms of impact.”

Marco Marcello, Manager of Information Systems, Lavan

Domestically, compliance in the cybersphere is an ongoing and complex issue for businesses. The rapid pace of change in technology means that companies must treat compliance as a constantly evolving part of their business, not something that can be fixed and forgotten. The statutory penalties for non-compliance can be severe, but the subsequent reputational damage can be worse. There are a number of compliance issues being faced by businesses, and a number of common recommendations from across the legal industry, but two core themes in the compliance space: preparation and communication.

Staying compliant and minimising reputational damage following a breach is a complex, time consuming and resource-intensive process, but it all essentially boils down to one thing: planning. Adequate preparation isn’t about prevention anymore - it’s about being ready for a breach to happen and knowing what steps to take afterwards.

There are key steps that all businesses should be taking to ensure their compliance:

- Build a detailed and prescriptive response plan detailing all actions that will need to be taken following an incident, and exactly who is responsible for each. In the hours and days after a breach it can be very difficult to ascertain what has happened and on what scale, so this level of preparation is essential.
- Run full-scale incident drills on a regular basis. This means not only reviewing the plan, but getting all relevant personnel to run the scenario as it would happen. It’s only through simulating the real time-sensitivities and pressures of an actual breach that the points of weakness in a response plan will become evident. 34% of Survey respondents reported that their businesses engage in cyber-attack drills only once a year or less, so this is a lesson that the Australian legal industry must heed.

“[Responding well means] you’ve written down what you’re going to do in the event of a breach, and you’ve already practised how to do it.”

Katrina Avila, Senior Manager, Cybersecurity & Financial Services, Ernst & Young

- As data breaches are becoming more common and more complex, training must be frequent, regular and continuous. Human error such as clicking suspicious links or transmitting sensitive information over insecure channels is one of the main threats for every business and it’s only through continuing education that this risk can be mitigated.

“They say there are two types of firms, those that have been breached and those who aren’t aware that they have been breached. That’s the truth.”

Zahn Nel, Director, CT Group Solutions

Communication with consumers (and getting it right) is crucial to minimising reputational damage following a breach. During a recent data breach, online design platform Canva simultaneously became an example of what to do, and what not to do, when communicating a breach to users.

Following their detection of a beach on Friday May 24, 2019, Canva sent an email to 140 million users the following day. The email’s first paragraph contained general information about the company and its platform updates, with no mention of the breach until the second paragraph and no mention of what users should do until the fourth paragraph. This misstep was roundly criticised online and cause the brand huge reputational damage.

Three key lessons for businesses here are:

- **Keep the consumer front of mind: it’s your system that has been breached but it’s your customers’ data that has been stolen.**
- **Be clear and concise: If you are notifying customers of a breach, that should be the sole purpose of your communication.**
- **Time the communication well: Canva’s email was sent on a Saturday; and while the speed of the communication should be applauded, there is broad agreement that a serious communication of this nature is best sent during the working week.**

Following the initial misstep, Canva set up an FAQ page on their website which has been regularly updated in the months following the breach. It includes information that is relevant to the more tech-minded, as well as the average Canva user, on what happened, what was compromised, and what users should do to protect their data. This is a highly-recommended step in continuing consumer communication following a breach and should be recognised as best practice.

“These notification laws are there so people can take steps to protect themselves. You need to be really open, clear and transparent about what has happened, and what people need to do. You can’t mix the message or add it on to a good news story, that’s not what it’s about.”

Sonia Sharma, Special Counsel, Maddocks

An example of clear and transparent communication was when the Australian Red Cross Blood Service suffered a data leak in 2016. The leak was caused by a contractor who had errantly placed a large data file somewhere that was easily accessible to the public. The Service was notified by an ethical hacker who discovered the files, and immediately triggered its response plan. At the time it was one of the biggest data security incidents that had occurred in Australia, but is now regarded as an example of best practice in dealing with this type of event. Amongst the actions undertaken were:

- Communicate clearly and openly about exactly what had occurred, taking full responsibility for the leak and informing the public about how the problem was being fixed.
- Notify potentially affected users directly - in this case through email and SMS.
- Open direct channels of communication for adversely affected users to seek support through the organisation.

Through meticulous planning, the Red Cross Blood Service was able to not only minimise reputational damage following the leak, but more importantly, to reduce the potential damage to blood service patrons who had their highly sensitive personal information compromised.

FIRM SECURITY

ONE MISTAKE IS ALL IT TAKES

FIRM SECURITY

ONE MISTAKE IS ALL IT TAKES

“We sent a phishing simulation email to 150 staff members - and only one person actually failed. If you look at the statistics, that’s fantastic - it’s a 99.3% success rate. But one failure is all that’s required.”

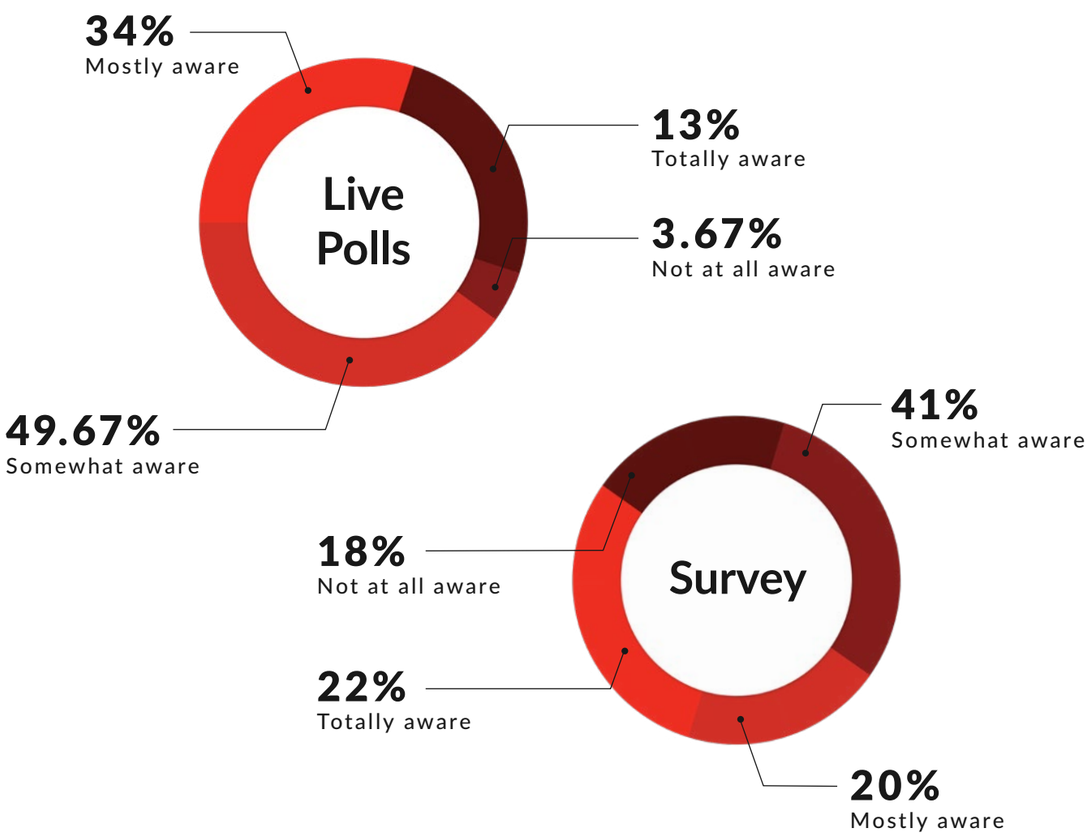
Marco Marcello, Manager of Information Systems, Lavan

As part of the Survey, events and live polling conducted for Decoding Cybersecurity: Clause and Effect, participants identified steps that law firms should be taking in order to heighten their cybersecurity. Whilst the discussion was legal-centric, the responses hold great value for businesses of all kinds and centre around one crucial theme: minimising human error through greater awareness.

What do you perceive as the biggest security threat to your firm / business?		
	Live Poll	**Survey**
Phishing	24.50%	15%
Hacking by outside operators	3.25%	40%
Undetected data breaches	7.75%	23%
Mobile breach	0.00%	3%
Human error/data mismanagement	63.75%	19%

Looking at the data from live event polling (the Poll) and the Survey, it's interesting to note that Survey respondents strongly felt that malicious hacks from external sources were the most significant threat to their businesses, contrasting sharply with the Poll where respondents felt that human error was the biggest danger. Looking further at the Poll results, and taking into consideration that phishing necessarily requires a human error of judgement to succeed, about 90% of respondents felt that a major point of weakness in their business' security was human in nature.

In your experience, how aware are lawyers about what is required to maintain robust cybersecurity?



Across both polling and the Survey, however, there is agreement that lawyers are 'somewhat aware' of what is required to maintain robust cybersecurity. Roughly 40% of Survey respondents also responded that, in their opinions, lawyers 'mostly' maintain good cybersecurity practices. This highlights is a clear need for better education of what is required to keep data secure and the importance of consistency in doing so.

> **"Most of the vulnerabilities within legal firms could be attributed to lack of awareness and lack of understanding, not only about the type of information you hold or the value of that information to a potentially malicious third party, but also the protections that need to be put in place around the many systems used to access, store and back up this information, and also the protections around how that information is transmitted."**
>
> *Rochelle Fleming, Business Manager, Sapien Cyber*

To this end, there are three fronts on which firms should be protecting themselves: people, process and technology.

People

- People must be educated on the business' cybersecurity controls and empowered to speak up if they feel that these are lacking, or suspect anything untoward.
- People must be continuously trained in how to spot breaches through bi-weekly exercises, phishing tests and incident responses.

Process

- Businesses must implement, communicate and enforce clear procedures and rules around the use of technology and data transmission. At a minimum these should include guidelines around working from home, use of third party platforms such as Gmail or Dropbox and use of mobile phones.
- Cyber resilience and incident response strategies must be developed, continually updated, and rehearsed so that they are up to date and ready for when they're needed.

Technology

- Businesses must remain vigilant in ensuring that all technology is automatically updated, servers patched, and ensure that any are vulnerabilities are closed as soon as they become evident.
- As much as possible, keep sensitive data in-house as much to minimise potential exploits in transmission, and to cut out the supply-chain issues that can arise from weak security on the part of contractors or third parties.

THE FUTURE

ITERATE, EDUCATE & COLLABORATE

THE FUTURE

ITERATE, EDUCATE & COLLABORATE

“The future for lawyers and law firms is education. It is getting informed. Technology will be there, but the technology is only as good as the people who are using it.”

Ben Cornish, Professional Services Manager (Security and Risk), Saab Australia

There were a number of emerging recommendations for improvement in both the legislative space and for businesses. There were two areas identified as key areas for legislative change in the future.

- The first is in offering greater civil recourse to individuals who have their data rights infringed. Currently almost all legislation is focused on reprimanding businesses for data mismanagement, but there is very little providing for a private right of action in relation to damages caused by a data breach. There have been recommendations from regulators and other bodies that a tort of invasion of privacy should be created - so far this has not happened, but this area will likely remain in focus over the coming years.

- The second is the recognition of data as property. Data is currently not recognised as property under Australian law and thus lacks the legislative protections that it would otherwise be afforded. For businesses this means that there is currently no adequate recognition under law of the value of company data, despite it now being widely regarded as among the most valuable assets of any company. For individuals, assigning property rights to data would also serve to strengthen control over how businesses and other entities use their personal information.

From a business standpoint, the recommendations for the future essentially act as a bullet-point summation of the solutions discussed throughout this Report - with the focus squarely on increasing awareness throughout the organisation.

Planning

- Organisations must have a functional and actionable cyber resilience strategy. Not to do so could be considered negligence on the part of both board and business.
- Develop, maintain and update a breach / incident response plan. A well-rehearsed response plan is essential for minimising reputational and functional damage.

Training and Education

- Staff training for culture of cyber awareness. From phishing tests to involvement in drill scenarios, awareness of best practice must be engrained throughout the business.
- Boards must be more involved in resourcing and training. Businesses have reported difficulties in getting directors to fully appreciate the seriousness of cybersecurity and allocate the resources required to get it right. A suggestion from panellists in this regard was engaging ethical or 'white hat' hackers to hack the company and report back on the vulnerabilities and potential ramifications if such a breach was carried out by malicious actors.

Continuous Improvement

- Ongoing privacy impact and security assessments are essential to ensure plans remain relevant amidst an environment of rapidly-shifting threats.
- Greater collaboration and knowledge sharing between firms and businesses in order to adopt and maintain best practice.

Across all consultations in preparation of this report, one point became clear: the cybersecurity space is moving quickly, and will continue to move quickly and the legal industry (as with all businesses) must continue to adapt its approaches in order to achieve the best outcomes for firms and clients alike. Planning, awareness-building and education should be focused on the people, process and technology of the organisation in order to maximise cyber resilience and minimise the damage from incidents in the future.

> **"I think the key takeaway is to really understand your obligations and improve the awareness of cybersecurity as an issue in your organisation. No one expects you to be invulnerable, but you do have to do the absolute best you can, and then be able to respond gold standard as and when you do you suffer a breach. Be aware, and educate."**

Ravi de Fonseka, Partner, Johnson Winter & Slattery

PANELISTS

MELBOURNE, VIC

CHENG LIM
King & Wood Mallesons

DR SUELETTE DREYFUS
University of Melbourne

DUDLEY KNELLER
Gadens

PAUL KALLENBACH
Minter Ellison

SYDNEY, NSW

RAVI DE FONSEKA
Johnson Winter & Slattery

REBECCA DUNN
Gilbert + Tobin

SUSAN BENNETT
Sibenco Legal & Advisory

SONIA SHERMA
Maddocks

KATRINA AVILA
EY Cybersecurity &
Financial Services

PERTH, WA

DAVID YATES
Corrs Chambers Westgarth

ROCHELLE FLEMING
Sapien Cyber

MARCO MARCELLO
Lavan

ZAHN NEL
CT Group Solutions

ADELAIDE, SA

BEN CORNISH
SAAB Security

YVONNE SEARS
ISDefence / Australian Women in Security

DANIEL KILEY
HWL Ebsworth

JOHN MACPHAIL
Lynch Meyer

CANBERRA, ACT

EDWINA MORRIS
Vocus Group

TIM DINGWALL
Griffin Legal

RAVI DE FONSEKA
Johnson Winter & Slattery

BRISBANE, QLD

DR GUIDO GOVERNATORI
Data61

ALEX HUTCHENS
McCullough Robertson

JOHN SWINSON
King & Wood Mallesons

LexisNexis®

About LexisNexis®

LexisNexis is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries. LexisNexis helps customers to achieve their goals in more than 175 countries, across six continents, with over 10,000 employees.

If you would like to find out more about how we can help you with your cybersecurity needs, please contact us at:

Phone: 1 800 772 772
E-mail: customersupport@lexisnexis.com.au