Shaping the future of insurance law

wotton kearney

A founding member of LEGALIGN GLOBAL

Cyber, Tech & Data Risk Report

W+K's wrap-up of the month's cyber, technology and data risk news for insurers, brokers and their customers doing business in Australia and New Zealand.

SEP22

W+K INSIGHTS

INTERACTIVE PDF

TOP RANKED Chambers Asia-Pacific 2022 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS

Welcome to W+K's Cyber, Tech and Data Risk Report

Issue 3, September 2022

We are delighted to publish Issue 3 of Wotton + Kearney's *Cyber, Tech and Data Risk Report* – our regular wrap-up of relevant news for insurers, brokers and their customers doing business in Australia and New Zealand in the cyber, tech and data fields. We also share some relevant articles from our Legalign Global partners around the world.

In this month's report, we look at a range of cyber issues and developments, including the recent Optus cyber attack and data breach which has purportedly affected a significant percentage of Australia's population, Lloyd's state-backed cyber exclusions, the legality of ransom payments, and the closure of the OPC's first compliance notice. We also provide an update on the National Data Security Action Plan, the prospects of a Takeovers Panel model approach to managing cyber attacks, and the NZ Ministry of Justice's consultation into broadening the notification requirements under the Privacy Act 2020. And, to finish, we provide an update on some interesting IT liability litigation currently ongoing in Singapore.

For more information about any of these stories, please contact a member of our cyber, privacy and data security team or technology liability team.

Contents

Kieran Doyle
Partner, Head of Cyber & Technology
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

Joseph Fitzgerald
Partner, New Zealand Cyber & Tech Leader
T: +64 4 260 4796
joseph.fitzgerald@wottonkearney.com

Australia – Cyber

New security measures to be unveiled after Optus suffers large-scale data breach

Optus (a SingTel subsidiary, and Australia's #2 telco) suffered a highly publicised cyber attack in late September which has, according to media reports, resulted in the potential disclosure of personal data belonging to millions of current and former customers, including driver's licence and passport numbers.

As demonstrated in the strong response by the government, a breach of this reported magnitude by a company of this prominence is likely to trigger significant changes, both to the law and the approach and tolerance of regulators.

The Home Affairs minister has indicated that the government will make material changes to privacy measures and penalties for cyber security incidents. Among these is a proposed requirement for banks and other institutions to be informed earlier of the occurrence of data breaches, in order to prevent compromised personal data being used to access bank accounts and to allow for monitoring of customers' accounts.

The government has also flagged the introduction of significant fines for data breaches of this type to mirror fines available under overseas regimes.

Currently, the maximum fine under the Australian Privacy Act is A$2.2m. This can be contrasted with significantly higher penalties available under parallel legislative regimes for some types of privacy related breaches, as we discussed re the Google case in August.

While the extent and applicability of the changes to the regulatory measures are yet to be determined, changes to the federal Privacy Act have been flagged since 2019 and have remained on the back burner.

In the meantime, the Office of the Australian Information Commissioner (OAIC) has published advice for impacted Optus customers. Those whose identities have been stolen or are being misused are advised to contact IDCare.

“As demonstrated in the strong response by the government, a breach of this reported magnitude by a company of this prominence is likely to trigger significant changes, both to the law and the approach and tolerance of regulators.

Lloyd's state-backed cyber exclusions

In its *Market Bulletin Y5381* of 16 August 2022, Lloyd's announced that from 31 March 2023, all standalone cyber policies it underwrites will need to include exclusions from losses arising from any state-backed cyber attack. This is separate from any existing war exclusions, which are fairly standard in the market, but do not explicitly address the scenario of non-physical warfare. Lloyd's has previously issued 4 alternative draft exclusions for its members to consider, however the Bulletin goes a step further. Lloyd's are, understandably so, looking for mechanisms to help manage the potentially systemic losses and aggregation risks state-backed attacks throw up.

While some have criticised that the change could materially change the utility of cyber policies, we think that view needs to be tempered by reference to the practical reality of cyber attacks and the difficulties associated with attribution – particularly when the burden of proof is on insurers.

The intention behind the war exclusions is to carve out circumstances where:

- the cyber attack can actually be attributed to a state – Lloyd's has proposed a few ways to do this, most of which hinge on a government body declaring attribution, and
- the state-backed cyber attack significantly impairs the ability of a state to function or a state's own security capabilities.

The intention is not to exclude cover for any and all cyber attacks with a suspected state government link or where a threat actor is able to be traced back to a particular nation state. This is clear from the model clauses Lloyd's has previously released, which it has now re-endorsed as part of *Market Bulletin Y5381*.

Cover for ransom payments arising from ransomware and data extortion incidents is one of the heads of loss insureds have in mind when seeking a cyber policy. Under Australian and international law, it is illegal to pay ransom to sanctioned entities or individuals (including certain state-sponsored groups) if attribution is possible. This means any new war exclusions on Lloyd's syndicates' policies will be unlikely to have a material impact on the availability of cover for ransom payments themselves – where a war exclusion was triggered, a sanctions exclusion would likely be triggered too.

The central point is that attribution is very difficult following a cyber attack, and Lloyd's has acknowledged as much in the way the model exclusions have been drafted. Most require a positive declaration from a government that a cyber attack is to be attributed to another nation state. The likelihood of sufficient information being available to make that attribution, and a government to then take that significant step, is very low.

Even if a government did make such a declaration, questions could be raised, subject to the particular policy wording, as to whether that government is a competent and relevant government for the purpose of the exclusion – or if a given declaration goes far enough to truly bed down attribution. To the extent insurers incorporate exclusions that allow for an ability to rely on other evidence as well, and not just a government declaration, those terms will still be very difficult to make out. The likelihood of achieving any level of certainty of attribution via, say, forensic evidence, is nigh on impossible except in the most exceptional circumstances.

While this development with Lloyd's is significant, we expect it will be a long time before an insurer will be in a position to seek to rely upon a war exclusion like this and we will see what the outcome of that will be. In the meantime, attribution will remain an aspect of forensic investigations following cyber attacks, as it always has, and insurers can continue to be cognizant of the potential risks.

Cyber basics: when is paying to get your data back illegal in Australia?

The law around cyber incidents and data breaches continues to become more complex. We will cut through that complexity with a series of 'cyber basics' articles, with this being the first.

Australian law doesn't specifically prohibit paying a ransom following a cyber attack. Australian law also doesn't presently require you to specifically report that ransom has been paid in response to a cyber incident[1].

This doesn't mean you can pay a ransom payment to whoever you like. Unless you have a defence, it could be illegal to pay money to criminals, terrorists, or individuals or entities on a sanctions list, or where that money could end up being used for a criminal purpose. Getting this wrong exposes an organisation to stiff penalties under criminal or sanctions laws. Companies and possibly their directors could also face serious consequences under corporate law.

During a ransomware event, you typically won't be able to identify who you're paying with certainty.

However, to avoid breaching the law, you need to undertake due diligence to seek to ascertain the identity of the threat actor. You will need expert help with this, including to analyse incident indicators against global intel and sanctions lists. You'll also need specialist legal advice.

We expect that Australian law around ransomware payments will change in the next few years. In 2021 and 2022, two separate ransomware bills were proposed (but have since lapsed[2]). Having established a dedicated Minister for Cyber Security (Hon Clare O'Neil MP), and given the recent Optus incident, the Albanese government is expected to undertake a range of reforms across its term.

Consultation on National Data Security Action Plan

The Australian Department of Home Affairs recently undertook consultation on the National Data Security Action Plan (NDSAP) – a government initiative to "define a consistent set of national, whole-of-economy expectations for data security"[3]. The Department's discussion paper on the NDSAP proposed mechanisms to address identified gaps in Australia's data security, and called for views on how the Australian Government could:

- uplift protections for personal information, while balancing the opportunities presented by international data flows and the global economy[4]
- align with international data protection and security frameworks (such as the EU's GDPR), and
- approach data localisation, that is, laws requiring data to be collected, processed and/or stored within Australia.

The Department of Home Affairs received 81 submissions, with commentary articulating some key themes including:

- organisations are broadly in favour of Australia aligning its data security framework with the GDPR, particularly the GDPR's guiding principle of 'privacy by design', which emphasises designing data processing procedures with privacy in mind from the outset (rather than retroactively imputing privacy features)[5]
- organisations objected to the 'wholesale importation' of the GDPR as, among other things, the enforcement penalties in the GDPR were widely regarded as excessively punitive (as we mention earlier, the government may be less inclined to heed this view in the wake of the Optus incident), and
- several organisations (particularly VISA and the Australian Banking Association) opposed data localisation, arguing that it would restrict the free flow of data across borders and prevent business from ensuring business continuity by severing connections with key data centres across the world[6].

The submissions are currently being reviewed by the Department, with an updated NDSAP to be developed and implemented to drive digital security in Australia. The key challenge in any resulting privacy and data security legislative reform will be balancing international alignment/consistency (e.g. with the GDPR framework) with strengthening protection for individuals' personal information and accommodating the general preference of public and private organisations to exercise autonomy over data management. Given that previous reforms are still being implemented (e.g. the consumer data right and critical infrastructure cyber security obligations), a key issue to watch will be how the government manages reform in the context of growing regulatory complexity.

[1] Certain entities involved in the payment chain might have reporting obligations to Austrac, although those don't arise merely because a ransom payment is being made by an entity to a threat actor.
[2] The *Ransomware Payments Bill 2021* (Cth) and the *Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022* (Cth)
[3] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security
[4] https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf
[5] https://www.itgovernance.eu/blog/en/the-gdpr-why-you-need-to-adopt-the-principles-of-privacy-by-design
[6] https://www.homeaffairs.gov.au/reports-and-pubs/files/national-data-security-action-plan/visa.pdf

Is a Takeovers Panel model appropriate for managing cyber attacks?

In recent weeks, some industry commentators have called for a Takeovers Panel-styled model to be introduced in the cyber risk context to offer added protection and recourse for directors. The purpose of the panel would be to act as a referral point to make key decisions in the aftermath of a cyber attack. These could include decisions about whether or not a ransomware demand can be paid. The panel would make a decision or give advice to the directors, which they could then safely rely on in the event of scrutiny down the track.

While many boards are looking for more clarity on their obligations regarding cyber security, sending urgent decisions to a third party statutory panel is unlikely to be fit-for-purpose or the answer directors are looking for.

The Takeovers Panel is a statutory body that essentially operates as a peer review of corporate control transactions to resolve takeover disputes. The process in working with the Takeovers Panel usually takes 2-3 weeks until a resolution is reached.

A takeover dispute is not comparable to a cyber event, and they cannot necessarily be addressed in the same way. A cyber event requires assessment of key questions and decisions with urgency and often represents a question of survival for companies. Knowledge of the specific business and circumstances of the cyber event is key – and those circumstances are often evolving day-by-day after a cyber event has been discovered.

Simply put, it is not as easy as sending off a two-page brief to a three-member industry panel to turn around a 24-hour decision on whether it is appropriate or legal for a company to respond to a ransomware demand.

The factors playing into any such decision shift and change even in a matter of hours. Accordingly, even if an urgent panel was able to be convened, that decision could be out of date within a matter of hours.

In the current landscape, particularly with the uptake of cyber insurance growing, companies obtain advice on legal and cyber security issues after a cyber event from their dedicated appointed specialist vendors, including lawyers, forensic investigators and others. Those vendors can be appointed immediately after an incident has been discovered, and work with the organisation hand-in-hand and day-by-day. The vendors will have access to the most up to date information with which to inform their advice and can update that advice on an ad hoc basis as circumstances change. As is the case for any other business risk, directors and companies can rely on expert advice they receive about what the risk is and how it ought to be managed or remediated.

The ability to defer decisions to a third party panel is also no replacement for board members achieving a basic level of cyber literacy, with which they can make appropriate decisions about investing in cyber risk management and governance. A director does not need to be a cyber security expert – they simply need the level of knowledge to understand what the key issues and risks are, and to seek the appropriate expert advice.

Having regulatory guidelines and benchmarks in place for cyber security standards makes logical sense and would be a helpful starting point, particularly as this would give directors a greater level of comfort and push them in the right direction to improve their cyber hygiene. However, this does not mean the next logical step is to involve statutory bodies in business' urgent decision-making in the aftermath of cyber attacks.

Australia – Technology Liability

Case update

In the first issue of our *Cyber, Tech and Data Risk Report*, we discussed recent trends in claims against managed service providers (MSPs) and cloud service providers (CSPs). Developments in the trial between American-Singaporean gaming hardware manufacturer Razer and IT vendor Capgemini over a 2020 data breach (being an admission of responsibility by a key witness for Capgemini) illustrate the importance of IT providers ensuring (as best possible) that their employees are appropriately skilled and qualified to perform the work that they are responsible for. The admission of culpability means that there are unfortunately no broader principles to be gleaned from this litigation, which might inform the liability landscape for Australian IT providers.

The litigation arises from a mass leak of Razer customers' data in June 2020. No sensitive data, such as credit card information or passwords, was leaked. Rather, the breach involved orders details, customer and shipping information.

Razer alleges that Capgemini:

- breached its contractual obligations, and
- was negligent, by failing to ensure that its IT systems were secure and that its personnel had appropriate and adequate skills, qualifications and experience.

Razer had engaged Capgemini to implement the ELK Stack platform on its internal IT systems. The ELK Stack platform collects and processes large volumes of data from multiple sources and stores it in one centralised location.

Both parties' experts agreed that the breach was caused by the security settings in ELK Stack having been manually disabled[7].

The trial, which commenced on 13 July 2022, was cut short on 22 July 2022 after a former employee conceded that he caused the security breach that led to the data leak after being shown material from Razer's independent expert.

Following the admission by the former employee, the High Court stated that it was no longer necessary for expert evidence to be heard. Instead, the case was adjourned for written submissions to be filed by 30 August 2022, following which the High Court would rule on damages[8].

Razer seeks damages of at least US$7 million for loss of profits, forensic investigation costs and legal/breach response costs.

While the admission of culpability reduces the insight into how an Australian court might approach liability issues in a similar matter, the case does illustrate the need for IT providers to ensure that their employees are appropriately skilled and qualified to perform the work that they are responsible for. It also highlights the evidentiary risks present in any litigation, which should be factored into any decision to defend a case to trial rather than attempt to resolve it commercially before that point.

> The case illustrates the need for IT providers to ensure that their employees are appropriately skilled and qualified to perform the work that they are responsible for.

Cyber security awareness and training

Due to the ever-growing threat of cyber attacks globally, companies are increasingly outsourcing systems management to MSPs and CSPs. It is becoming increasingly important for MSPs and CSPs to provide cyber security awareness training to their own employees, and to include managed security training as part of their service offering.

Research suggests that human error is involved in more than 90% of security breaches. Security awareness training helps to minimise risk and prevent the loss of PII, IP, money or brand reputation[9]. For this reason, MSPs should consider delivering high-quality training content frequently. The training should reflect the latest threats and entertain users to keep them engaged.

MSPs should also offer education and training opportunities for their own employees, including simulated cyber attacks, which help train and familiarise employees with post-incident remediation actions and crisis control.

[7] https://www.todayonline.com/singapore/admission-early-end-razer-trial-it-vendor-data-breach-1950936
[8] https://www.straitstimes.com/singapore/courts-crime/trial-of-razers-us7m-suit-over-data-leak-cut-short-after-it-vendors-ex-employee-concedes-causing-breach
[9] https://expertinsights.com/insights/security-awareness-training-for-msps-a-comprehensive-guide

New Zealand

Ministry of Justice considers changes to notification requirements under the Privacy Act 2020

The Ministry of Justice has opened a consultation into broadening the notification requirements under the Privacy Act 2020.[10]

Information Privacy Principle 3 requires that, where an agency collects information about an individual, the agency directly must take reasonable steps to provide notice to that individual. This includes the purposes of collection, the intended recipients, and the various access and correction rights available under the Act.

The Ministry of Justice has proposed changes to the Act that would broaden notification requirements to include circumstances where an agency collects information indirectly through a third party. The recommendation is designed to promote transparency and informed choice. The consultation document published by the Ministry of Justice seeks feedback on seven questions, including what the advantages and disadvantages of expanding notification requirements may be and the practical implications of any expansion.

The proposed changes are designed to bring New Zealand's notification requirements in line with those found in the EU's GDPR and Australia's Privacy Act 1988.

That said, insurers and insureds may want to consider the increased administrative burden and compliance cost associated with the need to notify individuals of indirect collection. Provision of a typical insurance product involves information passing through multiple parties. The requirement to provide notice at each point along this process may dramatically increase the cost for collecting agencies and the 'notification fatigue' for individuals.

Feedback on the Ministry of Justice's proposal closed on Friday, 30 September 2022. If you would like to discuss the Ministry of Justice's consultation, please contact a member of our cyber, privacy and data security team.

Office of the Privacy Commissioner (OPC) closes first compliance notice

On 1 September, the OPC closed its first compliance notice one year after it was issued to the Reserve Bank of New Zealand – Te Pūtea Matua (RBNZ).

Under section 123 of the Privacy Act 2020, the Commissioner has the power to issue a compliance notice where an agency has breached the Act, committed an act that may be treated as an interference of privacy under another Act, or breached a code of practice.

A compliance notice must identify the breach in question, require that the agency remedy the breach, and may identify particular steps to be taken by the agency.

RBNZ was issued with a compliance notice following a data breach of a third party file sharing software application in late 2020 (reported in January 2021). Following the breach, RBNZ appointed KPMG and Deloitte to undertake reviews of the incident and information-handling practices. RBNZ reports that the response to the breach cost approximately $3.5m. The compliance notice set out a range of improvements the OPC required RBNZ to implement following the incident. The OPC reports that RBNZ has now made all of the required changes and that the notice has been closed.

The OPC's response to the RBNZ's breach highlights the potential for the regulator to compel organisations to act and incur costs via a compliance notice. It also highlights the value of notifying early and working with regulators where possible. The Privacy Commissioner, Michael Webster, noted: "The Reserve Bank did everything right in responding to this breach. They notified us immediately, they worked with us throughout the process and they have taken on board the improvements we advised through our compliance notice."[11]

[10] https://www.justice.govt.nz/justice-sector-policy/key-initiatives/broadening-the-privacy-acts-notification-rules
[11] https://privacy.org.nz/publications/statements-media-releases/first-privacy-act-compliance-notice-successfully-closed

Global

New emerging threats challenge insureds and insurers

Insurers are facing more threats to their ability to operate and remain aligned with their customers' values than ever before. ESG-washing, supply chain issues, cyber attacks and ransomware are all part of this potent mix.

Many emerging threats are critical operational issues, but they must also be nailed into the strategic planning by businesses. This means having the expertise to identify the issues, analyse the threats they pose, create plans and put in place robust operational responses. For insurers, these present important challenges that they need to face in order to continue to deliver for their clients and for society. For more detail on the challenges these emerging threats present for insurers, read our Legalign Global colleague DAC Beachcroft's article here.

Ransoms – to pay or not to pay, that is the question

Our Legalign Global colleague DAC Beachcroft set out the key takeaways from the ICO and NCSC's recently published joint letter to the Law Society and Bar Council in respect of paying ransom demands in this article.

Legalign Global insights

For recent international developments, please see our Legalign Global colleagues' recent updates below:

- Alexander Holburn (Canada)
- BLD Bach Langheid Dallmayr (Germany)
- DAC Beachcroft (UK)
- Wilson Elser (US)

> Insurers are facing more threats to their ability to operate and remain aligned with their customers' values than ever before. ESG-washing, supply chain issues, cyber attacks and ransomware are all part of this potent mix.

Australian cyber, privacy + data security contacts

Kieran Doyle
Head of Cyber + Technology (Sydney)
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

Nicole Gabryk
Special Counsel (Sydney)
T: +61 2 9064 1811
nicole.gabryk@wottonkearney.com.au

Magdalena Blanch-de Wilt
Special Counsel (Melbourne)
T: +61 3 9116 7843
magdalena.blanch-dewilt
@wottonkearney.com.au

Jessica Chapman
Senior Associate (Sydney)
T: +61 2 8273 9876
jessica.chapman@wottonkearney.com.au

Zoe Bennett
Senior Associate (Sydney)
T: +61 2 9071 1946
zoe.bennett@wottonkearney.com.au

Ellie Brooks
Senior Associate (Melbourne)
T: +61 3 9604 7987
ellie.brooks@wottonkearney.com.au

Ryan Loney
Senior Associate (Melbourne)
T: +61 3 9116 7817
ryan.loney@wottonkearney.com.au

Matt O'Donnell
Senior Associate (Brisbane)
T: +61 7 3236 8736
matt.odonnell@wottonkearney.com.au

Kaila Hart
Associate (Sydney)
T: +61 2 8273 9838
kaila.hart@wottonkearney.com.au

Ronny Raychaudhuri
Associate (Sydney)
T: +61 2 9064 1833
ronny.raychaudhuri@wottonkearney.com.au

Carmen Yong
Solicitor (Sydney)
T: +61 2 8273 9824
carmen.yong@wottonkearney.com.au

Jorge Nicholas
Solicitor (Melbourne)
T: +61 3 9604 7995
jorge.nicholas@wottonkearney.com.au

Maxine Betty
Paralegal (Sydney)
T: +61 2 9064 1842
maxine.betty@wottonkearney.com.au

Cecilia Askvik
Business Development Manager (Sydney)
T: +61 2 9064 1839
cecilia.askvik@wottonkearney.com.au

Avram Lum
eDiscovery + Cyber Forensic Manager (Sydney)
T: +61 2 8273 9875
avram.lum@wottonkearney.com.au

New Zealand cyber, privacy + data security contacts

Joseph Fitzgerald
New Zealand Cyber Leader (Wellington)
T: +64 4 260 4796
joseph.fitzgerald@wottonkearney.com

Laura Bain
Senior Associate (Wellington)
T: +64 4 974 0464
laura.bain@wottonkearney.com

David Smith
Associate (Auckland)
T: +64 9 377 1881
david.smith@wottonkearney.com

Keely Gage
Solicitor (Wellington)
T: +64 4 280 7921
keely.gage@wottonkearney.com

Mathew Harty
Solicitor (Auckland)
T: +64 22 162 1582
mathew.harty@wottonkearney.com

To learn more about our cyber, privacy and data security expertise, click here.

Technology liability contacts

Kieran Doyle
Head of Cyber + Technology (Sydney)
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

Joseph Fitzgerald
New Zealand Cyber Leader (Wellington)
T: +64 4 260 4796
joseph.fitzgerald@wottonkearney.com

Nick Lux
Partner (Melbourne)
T: +61 3 9604 7902
nick.lux@wottonkearney.com.au

Stephen Morrissey
Special Counsel (Sydney)
T: +61 2 8273 9817
stephen.morrissey@wottonkearney.com.au

Magdalena Blanch-de Wilt
Special Counsel (Melbourne)
T: +61 3 9116 7843
magdalena.blanch-dewilt
@wottonkearney.com.au

Brigid Allen
Special Counsel (Melbourne)
T: +61 3 9116 7810
brigid.allen@wottonkearney.com.au

Karren Mo
Special Counsel (Melbourne)
T: +61 3 9116 7869
karren.mo@wottonkearney.com.au

To learn more about our technology liability expertise, click here.

Australian offices

Adelaide
Hub Adelaide, 89 Pirie Street
Adelaide, SA 5000
T: +61 8 8473 8000

Brisbane
Level 23, 111 Eagle Street
Brisbane, QLD 4000
T: +61 7 3236 8700

Canberra
Suite 4.01, 17 Moore Street
Canberra, ACT 2601
T: +61 2 5114 2300

Melbourne
Level 15, 600 Bourke Street
Melbourne, VIC 3000
T: +61 3 9604 7900

Perth
Level 49, 108 St Georges Terrace
Perth, WA 6000
T: +61 8 9222 6900

Sydney
Level 26, 85 Castlereagh Street
Sydney, NSW 2000
T: +61 2 8273 9900

New Zealand offices

Auckland
Level 18, Crombie Lockwood Tower
191 Queen Street, Auckland 1010
T: +64 9 377 1854

Wellington
Level 13, Harbour Tower
2 Hunter Street, Wellington 6011
T: +64 4 499 5589

www.wottonkearney.com.au

wotton kearney

A founding member of LEGALIGN GLOBAL

TOP RANKED Chambers Asia-Pacific 2022 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS