CYBER SECURITY & RISK MANAGEMENT

ANNUAL REVIEW **2018**

FINANCIER WORLDWIDE corporatefinanceintelligence

Published by
Financier Worldwide
23rd Floor, Alpha Tower
Suffolk Street, Queensway
Birmingham B1 1TT
United Kingdom

Telephone: +44 (0)845 345 0456
Fax: +44 (0)121 600 5911
Email: info@financierworldwide.com

www.financierworldwide.com

Annual Review • July 2018
Cyber Security & Risk Management

CYBER SECURITY & RISK MANAGEMENT

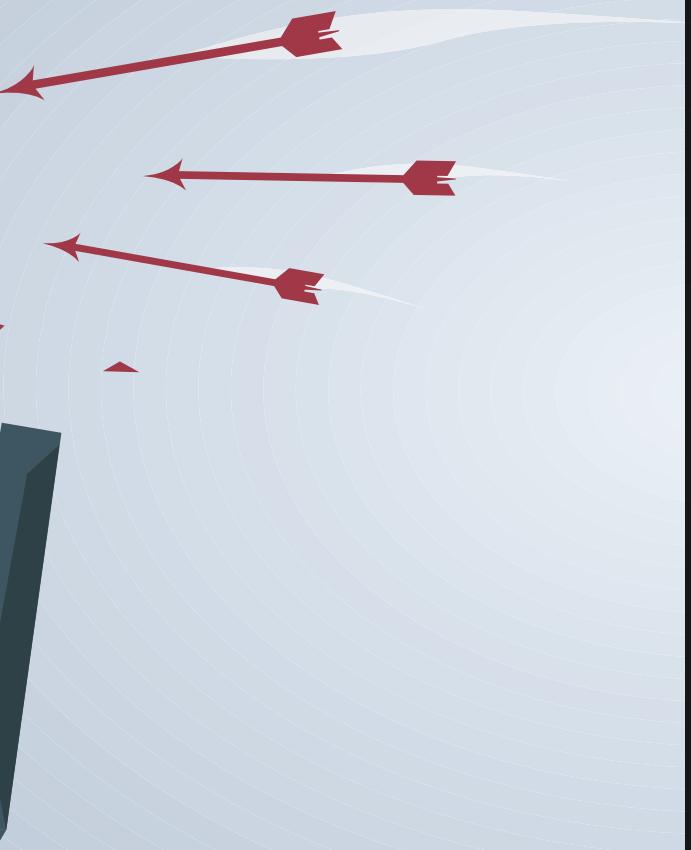
JULY 2018 • ANNUAL REVIEW

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in cyber security & risk management.

Contents

www.financierworldwide.com

Contents



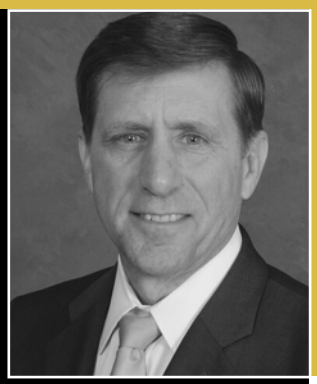
INTRODUCTION

Cyber security has become one of the most pressing issues of our time. The rapid rise of new technologies and practices, such as automation, digitalisation, artificial intelligence (AI), Big Data and the Internet of Things, has meant that many companies and industries are navigating new risks. Companies must ensure that they are fully cognisant of both the risks and rewards of utilising technology solutions. This awareness must form part of each organisation's wider risk management strategy.

Companies are creating and storing an unprecedented amount of data. As that data continues to accumulate, it is crucial that efforts are made to protect it. Regulations such as the EU's General Data Protection Regulation (GDPR) require organisations to be aware of weaknesses in their data security processes and establish effective data governance procedures.

Not only must companies have the right policies and processes in place, they must also appoint sufficiently qualified cyber security personnel. But this issue is increasingly problematic as the cyber security skills gap continues to widen. As a result, existing cyber security staff are grappling with a mounting workload, diverting attention away from much needed planning, strategising and training.

Technology is a double-edged sword. Though it presents companies with exciting ways to do business, it is also the means through which criminals and state actors are able to launch crippling attacks. Companies need to enhance their weaponry in the fight against cyber criminality.



United States

THOMAS FUHRMAN
Marsh Risk Consulting
Managing Director,
Cybersecurity Consulting and
Advisory Services
+1 (202) 263 7827
thomas.fuhrman@marsh.com

Thomas Fuhrman is managing director, cybersecurity consulting and advisory services, at Marsh Risk Consulting (MRC). He leads MRC's cyber risk consulting practice in North America and in international markets and works across Marsh & McLennan's operating companies on a broad range of cyber initiatives. He is an experienced cyber security consultant with over 20 years in the business. He was an active contributor to the development of the NIST Cybersecurity Framework and has advised clients and boards on its implementation. He is a strong advocate of the strategic management of cyber risk at the enterprise level through cyber risk quantification.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

FUHRMAN: Today's cyber risks arise from the shared reliance on ubiquitous and vulnerable technologies. In the past several years, cyber attacks have become more sophisticated, more destructive and more common. Some of this sophistication comes from the availability of attack techniques and methods, which reportedly originated from sources, such as nation-state military intelligence and services and advanced cyber crime syndicates. The 'WannaCry' ransomware attacks and the destructive 'NotPetya' attacks of 2017 are prime examples, and we expect many more. NotPetya, which disabled and effectively destroyed large numbers of servers and desktop computers worldwide, was disastrous for two reasons. First, it targeted specific un-patched configurations of Windows's operating systems. Second, the malware code was aggressively self-propagating and designed to disable functioning systems. Once inside a network, it rapidly installed itself in all the machines it could find. These two characteristics will likely be part of many future cyber events.

Q. What demands are data privacy laws in the US placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

FUHRMAN: The European Union's General Data Protection Regulation (GDPR) requires all firms, including US ones, holding data on persons in Europe to establish more effective data governance policies and procedures in relation to data classification, storage, protection and lifecycle management. A major GDPR challenge for companies is implementing the data rights it defines, including the consumer's right to access one's data, to be forgotten and to data portability.In many cases, technology transformations are needed to provide the functionality these rights imply. Articles 25 and 32 to 34 outline data protection requirements, and Article 42 encourages the establishment of "data protection certification mechanisms" issued by certification bodies. These provisions may present substantial cyber security requirements. GDPR is seen as the harbinger of data protection regimes to be implemented in the US and beyond. Already, every US state has data breach laws governing disclosure and other requirements, which often intersect with GDPR's requirements. We should anticipate a convergence over time of legal requirements for personal information protection and data owners' rights, likely at the US federal level.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

FUHRMAN: Today's detection technology requires intricate setup and integration, as well as trained operators to configure, manage, monitor and react to its alerts. Finding qualified cyber security professional staff to do this work is a major challenge unto itself. Additionally, the frequency of false positives sends analysts down blind alleys and distracts them from analysing true threats. This is a key area in cyber security where artificial intelligence (AI) and automation may reduce time consuming and error prone cyber event analysis by human operators. Various kinds of machine learning are in place in today's cyber sensors and analytical platforms, but this is just the beginning. Systems like these need to grow in capability and sophistication to not only relieve the burden of human operators, but also improve real-time automated analysis and responses to cyber alerts and anomalies. Hackers are using AI; defenders need to do the same.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

FUHRMAN: Companies should adopt a structured approach to cyber security governance. That means establishing the structure for decision making in cyber security, identifying compliance requirements, defining and aligning roles, responsibilities and organisations for managing cyber risk; selecting a cyber programme development framework, such as the NIST Cybersecurity Framework or ISO 27000 and defining the process linkage between key stakeholders and operations for the identification, measurement and management of cyber risk. With these elements in place, it is then time to review, refresh or create enterprise

IT and cyber security policy documentation. This may focus on enterprise-wide cyber security, employee cyber security responsibilities, awareness and IT acceptable use, identity and access management, data classification, cyber risk management, third-party or vendor management, incident response and escalation, and mobile device security. Once the governance and policy frameworks are designed, an integrated set of operational procedures should be developed.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

FUHRMAN: The biggest change in insurance has been the shift in buyers' focus from coverage for data and privacy breaches to business interruption (BI) and contingent business interruption (CBI) risks – especially economic losses caused by operational, system and supply chain disruptions. With many non-traditional buyers of cyber insurance, including manufacturing, energy and pharmaceutical companies, increasingly seeking BI coverage, underwriters are responding with broader terms and higher limits. New market entrants are keeping pricing competitive while increasing overall capacity. Key BI innovations include CBI and supply chain coverage, coverage triggers beyond security breaches and coverage that responds to losses incurred from the start of waiting periods. Insurers are also focusing on tailoring coverage to small and medium size firms' needs and simplifying the underwriting process. Finally, insurers continue to provide services aimed at improving policyholders' risk profile, such as cyber risk education programmes and risk mitigation tools that assist with prevention and recovery from cyber attacks.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

FUHRMAN: While pricing is always a factor in purchasing insurance, it should be secondary to obtaining the appropriate breadth of coverage. Companies should work with a qualified broker to better understand their cyber risk profile, evaluate marketplace offerings and design an optimal insurance programme. The first step is an accurate assessment of the company's cyber risks. What are the external and internal vulnerabilities, and how susceptible is the firm to cyber attack? Secondly, what would a cyber event cost the company? Quantifying cyber risk is critical for driving informed decision making around cyber security investment and risk transfer planning. Another consideration is risk appetite; how much risk is the firm willing and able to bear? These metrics help determine the company's cyber insurance needs. A broker can model maximum potential losses and analyse the firm's current risk transfer portfolio to evaluate policies and limits, identify gaps, overlaps or coverage needs, and design a coverage solution.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

FUHRMAN: Cyber is one of the greatest risks that organisations face and management of this risk is essential. Boards know this and are increasingly aware of their fiduciary and risk

“While pricing is always a factor in purchasing insurance, it should be secondary to obtaining the appropriate breadth of coverage.”

oversight responsibilities. Additionally, the Securities and Exchange Commission (SEC) recently released guidance on understanding and disclosing business-material cyber risks to investors. This is a board-level issue. A clear link, through policy and process, between board, management, IT and cyber security functional teams, is needed to ensure effective management of this critical risk. In cyber security, we use the acronym ‘APT’ to refer to advanced persistent threat malware. I suggest another meaning for that acronym, ‘accountability for precision and transparency’ in the enterprise management of cyber risk. That means understanding the risk, in financial terms, and managing it through closed loop processes to achieve business goals. This should be an ongoing pursuit for all organisations that depend on IT systems. ■

www.marsh.com

MARSH

Marsh is a global leader in insurance broking and innovative risk management strategies with 30,000 employees advising individual and commercial clients of all sizes in over 130 countries. Marsh’s Cyber Centre of Excellence harnesses its cyber risk, brokerage and advisory expertise under one roof to deliver proprietary, purpose-built and market-leading cyber risk management products and solutions to its clients worldwide.

THOMAS FUHRMAN
Managing Director, Cybersecurity Consulting and Advisory Services
+1 (202) 263 7827
thomas.fuhrman@marsh.com

JIM HOLTZCLAW
Senior Vice President
+1 (202) 297 9351
james.holtzclaw@marsh.com

THOMAS REAGAN
Cyber Practice Leader
+1 (212) 345 9452
thomas.reagan@marsh.com

Argentina

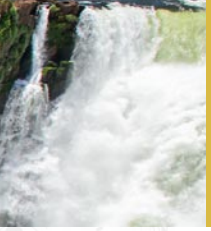
DIEGO FERNÁNDEZ
Marval, O'Farrell & Mairal
Associate
+54 (11) 4310 0100 ext. 1303
dfer@marval.com

Diego Fernández joined Marval, O'Farrell & Mairal in 2003 and is currently a member of the IP, IT and privacy law group. During 2014 he worked as visiting foreign counsel with Foley & Lardner LLP in its Chicago office and was a member of the firm's IT and privacy law group and the Latin American Practice Group. He graduated from the Universidad Católica Argentina with a law degree in 2003. In 2013, he earned an LL.M degree in IT and privacy law from the John Marshall Law School in Chicago, completed with honours, where he participated as the international student ambassador and acting vice president of the Privacy and IT Law Society.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

FERNÁNDEZ: The Argentine cyber security landscape looks much like the rest of the world. Cyber criminals are likely to attack organisations and individuals in Argentina with increasing intensity and frequency. Because Argentina lacks legislation establishing comprehensive cyber security standards, the level of protection used by organisations is inconsistent. Over the past year, Argentina has seen a large number of cyber attacks. Some of these are entirely new or had not been prevalent in the past. For instance, attacks have been carried out which compromise computers in order to use their processing power to mine bitcoins, which are then collected by hackers. Others have targeted physical business assets, leading to losses.

Q. What demands are data privacy laws in Argentina placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?



FERNÁNDEZ: Argentina's Data Protection Law (DPL) established different levels of data protection and assurances of compliance. These standards create three security levels for data controllers and processors: basic, medium and critical. The basic security level covers all databases under the DPL and requires that a data security document be created, implemented and updated. The medium security level covers databases that render public services and entities legally required to observe duties of confidentiality. It mandates that, along with the basic security level document, other, more stringent security methods must also be adopted. The critical security level applies to databases which store sensitive personal data and requires the entity to adopt basic and medium security protocols, as well as further protections, like encryption. Moreover, there is a general duty to prevent harm to third parties, which may include protecting third-party data, and some industries have legislated standards for data security.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

FERNÁNDEZ: Data breach protection can always be done more quickly. Any time that an organisation experiences a cyber security breach, it needs to address the problem as quickly as possible to avoid harm to itself and those that it serves. Given the increasing speed and scope of cyber attacks, many organisations are not handling breaches quickly enough. Many of the most prominent data breaches took weeks, months or even longer to detect and fix, so organisations looking to avoid similarly large breaches should always strive to increase their response speeds. This requires updated cyber security frameworks which are predicated on detection and responses being implemented.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

FERNÁNDEZ: Following the legal minimum for cyber security standards is the first step when establishing appropriate policies and procedures, but since the legal minimum may be insufficient for adequate protection, it should not be the last. Argentina, like some other countries, has a governmental entity which promotes the

collaboration of private and public entities to produce cyber security frameworks. While these frameworks take time to develop, being party to their creation can help businesses tailor their own cyber security protocols while participating and benefitting from model frameworks when they are released. Each organisation should also have a comprehensive security protocol. This should include standard security devices like firewalls and detection software so that breaches can be responded to as quickly as possible. Additionally, all employees should be familiar with the security protocols in place and be tasked with knowing how to implement them.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

FERNÁNDEZ: Cyber insurance is a market with an enormous amount of growth potential. Insurers are increasingly offering cyber insurance to help businesses offset the cost of cyber security incidents. Insurance companies in the past lacked actuarial and other data ordinarily used in calculating insurance rates and so charged inflated premiums and imposed conditions on cyber insurance to ensure that they were not losing money on the policies. However, as insurers collect more knowledge of the costs of cyber attacks, they can charge more accurate premiums and reduce their rates and restrictions so that more businesses can affordably purchase cyber insurance, allowing the market to grow and more businesses to be insured.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

FERNÁNDEZ: Buying cyber insurance in Argentina requires many of the same considerations as buying it anywhere in the world. Insurers which offer standalone policies often provide better coverage than those that offer cyber insurance as part of an existing policy. Some standalone policies may also be customisable for an organisation's specific needs. Some policies cover only the insured, while others extend coverage to third parties also affected by attacks. The types of attacks covered may differ from policy to policy. Policies may cover only targeted attacks on the organisation to the exclusion of non-targeted attacks. Others may cover only network attacks and not social engineering. Coverage should also include attacks which occur over long periods of time, as is often the case. Retroactive coverage may also be desirable. Finally, simple financial comparisons for premiums and deductibles are necessary so that the business can afford its cyber insurance.

"Simple financial comparisons for premiums and deductibles are necessary so that the business can afford its cyber insurance."

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

FERNÁNDEZ: Cyber crime erodes a company's bottom line when attacks result in money being stolen from the organisation and when money is spent to fix data breaches. Cyber attacks also erode many businesses' consumer trust, as data breaches may be perceived as organisational incompetence or lack of care for customer data. Preventing both of these is paramount to ensuring a business' growth by serving its customers as well as possible. This means that organisational leadership is likely to devote more time and resources to cyber security as it becomes increasingly apparent that preventing data breaches and other cyber attacks is essential for company health.

www.marval.com

MARVAL O'FARRELL MAIRAL

Marval, O'Farrell & Mairal is the largest law firm in Argentina. A market leader at both local and Latin American levels, the firm has been providing sophisticated, high-quality advice to international and local clients for more than 95 years. The firm comprises over 300 lawyers and has wide experience of international business issues and the complexities of cross-border transactions.

DIEGO FERNÁNDEZ
Associate
+54 (11) 4310 0100 ext. 1303
dfer@marval.com

United Kingdom

JAMIE BOULOUX
RSG Europe
President of Cyber
+44 (0)1302 303 607
jbouloux@emerginrisk.com

Jamie Bouloux is CEO of EmergIn Risk, an MGA focused on insurance solutions around cyber and technology risk. Prior to forming EmergIn, he spent the bulk of his career at American International Group (AIG) where he held multiple positions including Head of Cyber, Technology and Media for AIG EMEA where he developed the cyber strategy for over 40 territories which were his responsibility.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

BOULOUX: 2017 was an unprecedented year for cyber events. We witnessed two of the largest systemic attacks to have faced the digital age in 'WannaCry' and 'Petya/NotPetya'. These events showed the speed with which a global attack can manifest and their potential economic cost. WannaCry, the single biggest ransomware event ever, spanned 150 countries and led to an estimated economic loss of $8bn. Petya/NotPetya further demonstrated the issues companies face in managing globalisation and sprawling networks, as many of those affected were the subsidiaries or local operations of larger global conglomerates. Further, 'Meltdown' and 'Spectre' showed how hardware, namely a single microprocessor, Intel's chip processors, for example, in this instance, has the ability to affect every major computer manufacturer, operating system vendor and cloud service provider. This highlights how difficult it is to maintain the integrity of systems and data when we are so reliant on third parties to provide the architecture we trust. These events have helped to radically change how companies are addressing the business impact

assessments associated with technology and their subsequent risk tolerance.

Q. What demands are data privacy laws in the UK placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

BOULOUX: The Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR), places tough requirements on businesses to protect personal data and the privacy of all EU citizens. The 'security principle' requires businesses to ensure that they process personal data securely and by means of 'appropriate technical and organisational measures'. Risk assessments should be undertaken to evaluate the level of security and to review organisational policies, with technical controls and measures being implemented to include the use of encryption and pseudonymisation where appropriate. Furthermore, in the event of a data breach, businesses need to ensure that they have a plan in place to deal with the stringent notification requirements. Companies are being challenged to put systems and processes in place to achieve compliance; once achieved, the cost and work required to maintain compliance will be an ongoing burden for UK businesses.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

BOULOUX: Awareness around these issues is not evenly spread across the world. Growth, for the most part, has been legislation-led, with privacy laws in the US emerging first, followed in recent times by updates to privacy laws in Australia and, of course, the GDPR bringing data-related issues into sharper focus in Europe and beyond. However, despite the ever-increasing prevalence of mainstream media stories on security breaches, there is still a large divide between awareness and mitigation in many organisations. What is perceived by some as a new risk, combined with financial pressures on businesses, has resulted in a delay in implementing appropriate security strategies and mitigation procedures. The expansion of global laws and regulations will help drive companies to

map and resolve these exposures accordingly. But like anything, compliance will take time.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

BOULOUX: There is no silver bullet for managing cyber-related risks. Consequently, companies are adopting many different strategies for turning the variables of managing systems, networks and data into a measurable, to be able to execute business risk vulnerability studies and ultimate impact assessments. These assessments may not always be formalised, but an SME data controller who outsources data management and redundancy to a third-party vendor, or employs a virtual CISO, will have rationalised that the vendor is in the best position to support their compliance demands, based on budget and expertise. Similarly, a sophisticated company will adopt strategies for mitigating the exposure of rolling out firmware or software updates by sandboxing before executing a company-wide fix. These are both shrewd practices that are rationalised, based on the size of the company and their level of sophistication. Ultimately, whether large or small, companies will identify what works best for them and should adopt appropriate processes that focus on security, usability, awareness and contingency planning for a time of crisis.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

BOULOUX: In this interconnected world that is ever more reliant on technology, cyber insurance must evolve and develop in tandem with the changing risk to businesses. While continuing to build on traditional extortion and media coverage, cyber insurance has shifted its main focus from covering the costs associated with data breaches, toward broader solutions for the impact of system disruptions. Business interruption triggers have extended to cover loss where the system downtime is caused by any unplanned outage, whereas in the past, this would likely have been restricted to a security breach incident. Furthermore, where clients see cyber as 'peril', coverage is often extended beyond the insured's systems to cover lost business income arising from an outage to not only the company's IT vendors but, in some circumstances, their entire supply chain. Further, cyber as a peril has pushed the agenda for clients to look for gaps where their traditional policies might not provide affirmative coverage.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

BOULOUX: Starting with triggers, companies should avoid language which seeks to narrow the scope of coverage from what a purchaser believes a cyber incident is, or how it might affect their business. This is the first step in removing some of the most contentious issues the courts have had to consider so far in respect of cyber insurance. Coverage should be tailored to a company's business needs, by way of risk review, as simply purchasing what everyone else is buying can lead to problems should the policy need to be called upon. This includes exclusions,

"Cyber as a peril has pushed the agenda for clients to look for gaps where their traditional policies might not provide affirmative coverage."

which may not be problematic if a holistic approach to the entire insurance programme is taken and coverage already exists in other areas, such as crime. Hardwiring incident response into the policy is critical, and partnering with reputable and respected providers in this regard cannot be emphasised enough. Combining the above should pay dividends in the form of the best use of premium spend being achievable.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

BOULOUX: Disruptive technology, the increasing value of intangible property, the proliferation of data assets, enhancing workforce optimisation, expanding global legislation, the overlaying of vendors across corporate infrastructures and the threat that a company could be completely derailed by these investments, have meant that 'cyber' is a top five risk for many companies across the world. Enterprise risk will continue to evolve, as will the price tag for being connected. Organisations have never been more beholden to the operational and financial pitfalls of networked devices. And, as such, we expect to see a direct correlation between the continued 'normalisation' of cyber and the surety with which the boardroom will address the issue.

www.emerginrisk.com

EmergIn Risk

Ryan Specialty Group is an international specialty insurance organisation that provides innovative solutions for brokers, agents and insurance carriers. The RSG family includes a wholesale brokerage operation, RT Specialty (RT), and a collection of managing general underwriting companies within RSG Underwriting Managers (RSGUM). Headquartered in Chicago, Illinois, Ryan Specialty Group has approximately 1700 employees with operations in North America, the UK and Europe.

JAMIE BOULOUX
President of Cyber
+44 (0)1302 303 607
jbouloux@emerginrisk.com

Spain

NELIA ARGAZ
Marsh Risk Consulting
Cybersecurity & Business Resilience Practice Leader – Spain
+34 (934) 94 8100
nelia.argaz@marsh.com

Nelia Argaz leads the cybersecurity & business resilience practice in Marsh Risk Consulting Iberia (MRC). With more than 10 years of experience in managing security operations services, business continuity and risk consulting, Ms Argaz serves as the driving force behind MRC's information security services designed for global organisations. She holds a degree in computer engineering, a postgraduate degree in business management and several security certifications.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

ARGAZ: Today's cyber risk environment often has complex and cascading consequences for organisations, and the threats companies face are growing and becoming more sophisticated as the pace of new technology development accelerates. Moreover, organisational and personal cyber risks are separated by a very narrow and blurring line, so the potential impacts affect all types of technology users. On the one hand, the tools and services available in the deep web used for committing cyber crime appear to be growing steadily and becoming more commercialised. Online trade in 'ransomware-as-a-service' or bulletproof hosting is readily available. Darknet markets are significant threats which provide a wide variety of illicit commodities. On the other hand, even though different information security enforcement regimes – the Networks and Information Systems Directive (NIS), the European Union's General Data Protection Regulation (GDPR) and Enterprise Network Security (ENS) – among others, have come into effect over the past few years, the intangible and unknown nature of cyber risk continues to challenge cyber security innovation activities.

SPAIN • NELIA ARGAZ • MARSH RISK CONSULTING

Q. What demands are data privacy laws in Spain placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

ARGAZ: A key principle of the GDPR and the Spanish Data Privacy Law (LOPD), which took effect on 25 May 2018, is that you can process personal data securely by means of appropriate technical and organisational measures that ensure a level of security appropriate to the risk. Likewise, in the event of a personal data breach, the controller must, without undue delay, and, where feasible, not later than 72 hours after having become aware of it, notify the relevant supervisory authority of the personal data breach, unless it is unlikely to result in a risk to the rights and freedoms of natural persons. Maintaining regulatory compliance requires the incorporation of a set of new security measures and activities, either technical or organisational, which respond to personal data processing risks. Organisations must engage in a continuous cyber risk assessment process, as opposed to the biennial or one-off assessments that may have been conducted in the past.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

ARGAZ: Although organisations are becoming more aware of cyber security risks, the investments made to mitigate them are definitely not enough in most cases. Today's prevention, detection and response require appropriate technology for a satisfactory level of cyber security and a high level of professional expertise, which can be a major challenge for organisations, in order to manage, operate, monitor and innovate the necessary cyber security activities. In addition, cooperation within an organisation and across sectors is a must, but it can be elusive. Fostering discussion and cooperation across departments and between the private and public sector to defend and protect information from cyber attacks is necessary. Hackers have their own trusted networks, social and otherwise. Defenders need to do the same.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

ARGAZ: Companies should take a structured approach to cyber security governance, based on a comprehensive cyber risk analysis. Once cyber risk is understood by the board and senior leadership, and the structure for decision making has been clarified, it is time to apply agreed measures to reduce cyber risk. That means defining and aligning roles and responsibilities for managing cyber risk, designing a cyber security programme, implementing cyber security plans and defining standardised and accurate cyber risk metrics to measure the likelihood and impact of cyber risk scenarios. With these elements in place, it is then time to review, refresh or create appropriate enterprise information security policy documentation and underlying procedures. These may focus on enterprise-wide information security, employee cyber security responsibilities, awareness and IT acceptable use, identity and access

management, incident response and escalation, data classification, cyber risk management, third-party or vendor management and mobile device security.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

ARGAZ: Following the May 2018 enforcement of the GDPR, companies are increasingly concerned about their exposure to data privacy violations. As a result, underwriters are facing an increased demand for cyber insurance as a way to mitigate the potential financial consequences of GDPR violations or breaches. Within Spain, this demand has generated a corresponding increase in new insurance markets interested in exploring opportunities to offer this line of coverage. The entrance of new carriers and the expanded offerings of current carriers are increasing available capacity and driving higher indemnity limits. At the same time, with steps being taken to simplify the underwriting process, pricing continues to be competitive. As GDPR and other data privacy regimes come into play and related insurance offerings grow, there is a natural expectation that claims frequency will increase. This, in turn, may drive the purchasing of cyber insurance, as buyers become more familiar with coverage benefits, scope and the responsiveness of the insurance contract itself.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

ARGAZ: While pricing is always a relevant factor when purchasing insurance, companies should bear in mind that obtaining the appropriate scope and breadth of coverage should be the first priority. The organisation's assessments of cyber risk, and its ability to mitigate it, are key to determining which coverages are necessary for its unique risk profile. Companies should also assess if and how their cyber exposures may be covered under their current risk transfer portfolio, paying close attention to wording and policy language. Potential gaps, overlaps or coverage needs can then be easily identified, and an appropriate coverage solution designed and placed in the market. Cyber risk assessments and quantification, coupled with insurance coverage needs evaluations, are driving good decision making around cyber insurance and cyber security investment. Risk transfer should be considered in tandem with technology and mitigation efforts. Insurance and cyber security are complementary. Collaboration between IT or IS leaders and risk management can help support

"Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming commonplace."

and clarify the respective value of cyber security and cyber insurance within a holistic cyber risk management strategy.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

ARGAZ: According to the World Economic Forum, cyber attacks and data fraud are two of the top five global risks by perceived likelihood. Moreover, the financial costs of cyber attacks are rising. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming commonplace. Specific ransomware attacks, such as 'Wannacry', 'Petya' and 'NotPetya' have affected a broad range of companies and monopolised media coverage due to their massive unforeseen spreading capacity. Other attacks, such as 'Mirai', have highlighted the potential for the abuse of the Internet of Things. And spam 'botnets' and social engineering initiatives are now being used as an alternative malware delivery method. Given these currents threats and developing scenarios, we expect cyber risk management to continue to climb the boardroom agenda.

www.marsh.com

MARSH

Marsh is a global leader in insurance broking and innovative risk management strategies with 30,000 employees advising individual and commercial clients of all sizes in over 130 countries. Marsh's Cyber Centre of Excellence harnesses its cyber risk, brokerage and advisory expertise under one roof to deliver proprietary, purpose-built and market-leading cyber risk management products and solutions to its clients worldwide.

NELIA ARGAZ
Cybersecurity & Business Resilience Practice Leader – Spain
+34 93 494 800
nelia.argaz@marsh.com

SARA MUNOZ
Cyber Risk Insurance Leader - Spain
+34 91 514 26 94
sara.munozrubio@marsh.com

JOSÉ MARÍA CARULLA
Client Services Advisor Leader - Spain
+34 93 494 80 41
josemaria.carullamarques@marsh.com

Netherlands

MAURICE KOK
Tokio Marine HCC
Junior Underwriter
Financial Lines
+34 93 530 7365
mkok@tmhcc.com

Maurice Kok joined Tokio Marine HCC's transaction risk insurance team in 2015 as an underwriting assistant and then moved on to the Benelux team as an underwriter specialising in D&O and cyber insurance. He holds a Bachelor's in Business Administration from Universidad del CEMA and has previously worked for ExxonMobil and Assekuransa, among others. He speaks Dutch, English, German and Spanish.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

KOK: By now, most of us have heard about the data breach at Equifax, the business interruption incident at Maersk or about Facebook under scrutiny for its treatment of privacy. The cyber threat landscape can be quite overwhelming and it is not only limited to online activities. Hackers often perform physical reconnaissance on site to detect an easy way in. After all, why bother trying to hack an expensive security system if you can just walk into the server room? Social engineering is another popular technique which is employed by attackers to appear trustworthy to employees. Device hacking has become common too, as more devices form part of the Internet of Things. Ransomware attacks are also gaining momentum.

Q. What demands are data privacy laws in the Netherlands placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

KOK: Companies that collect data from EU citizens should comply with the new General Data Protection Regulation (GDPR), which came into force on 25 May 2018. Many companies have devoted a great deal of attention to complying with the GDPR as data breaches must now be reported within 72 hours. Fines can amount up to €20m or 4 percent of the company's worldwide annual revenue, whichever is higher. Furthermore, the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) must also be considered. The GDPR has intentionally vague descriptions of what constitutes personal data and how it should be protected. Companies will need to apply the same security standard to social security numbers as they do to an individual's IP address.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

KOK: A study conducted by the Ponemon Institute shows it takes a company, on average, more than six months to identify an intrusion and 55 days to contain it. Each passing day can increase the company's net financial loss as the attacker has more time to steal valuable data or to interrupt day-to-day business. The business sector has the highest percentage of the total amount of breaches reported, with 54.7 percent of incidents reported six months after the initial breach had taken place. Though compliance with regulations like GDPR, PCI DSS and HIPAA does not come cheap, the alternative can be much more expensive. The cost of non-compliance is 2.71 times higher than the cost of compliance.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

KOK: A three-pronged approach, focused on people, processes and technology, is recommended. The saying 'a chain is only as strong as its weakest link' applies twofold when it comes to cyber security. A company should know what information it holds, who is able to access it and where and how it is stored. These are basic questions to be answered when drafting an information security policy. Investing deeply

in technology, yet neglecting to sufficiently train employees, or outsourcing a large part of a company's IT environment, yet overlooking the need to vet or control the outsourced service provider, can be costly mistakes. Each area needs due attention.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

KOK: We see great variety in the coverage offered by insurers as the cyber insurance market is still developing and new features are being added continuously. One way in which insurance firms can help companies manage their exposure to cyber risks is to offer preventative consulting services. Up to a certain level, the costs of such services are covered in policies. A company is free to contract additional preventative services at its own cost, of course. Services available range from informed briefings and workshops, to the drafting of a data breach response plan and tailor-made reports on how to prevent business interruption within the company.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

KOK: While the cyber insurance market is expanding rapidly, there is still little data available to predict if a cyber policy will perform as expected when business is interrupted or should a data breach take place. This can be due to the poor drafting of policy wording, which often leaves the insured and the insurer's claims handler with areas of uncertainty in the cover to resolve. Therefore, a simple 'coverage at a glance' schedule that clearly shows the insured what is covered and when, has, in our experience, proved to be the best solution. Crystal clear language in the wording means that, after a cyber event, insurers can quickly assist the insured should they recur to their policy, without having to discuss the scope of coverage at length.

"If the board does not put cyber risk management on its agenda, the first sign of business interruption or a data breach certainly will."

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

KOK: If the board does not put cyber risk management on its agenda, the first sign of business interruption or a data breach certainly will. Unfortunately, without proper preventative measures in place, the costs to repair any damage can easily exceed those of investing in a better cyber security system. Being hacked is not even the worst-case scenario; not knowing what to do or how to deal with it is. Therefore, finding an insurance partner that includes coverage for emergency response costs is essential. This coverage will provide immediate assistance from experienced IT, legal and PR professionals. ■

www.tmhcc.com

TOKIO MARINE HCC

Tokio Marine HCC is a leading specialty insurance group with offices in the United States, the United Kingdom, Spain and Ireland, transacting business in approximately 180 countries and underwriting more than 100 classes of specialty insurance.

MAURICE KOK
Junior Underwriter - Financial Lines
+34 93 530 7365
mkok@tmhcc.com

Germany

GÜLSAH DAGDELEN
Tokio Marine HCC
Senior Underwriter
Financial Lines
+34 93 530 7358
gdagdelen@tmhcc.com

Gülsah Dagdelen is a FCII-qualified senior underwriter with over 10 years of experience in the insurance industry. At Tokio Marine HCC she focuses on financial lines insurance, especially cyber risks, for the German and CEE markets. Prior to joining the company in 2013, Ms Dagdelen worked for Manager-Assecuranz-Compagnie and Proxegur. She holds a Bachelor's degree in insurance science from TH Köln as well as a Master's degree in Law (LL.M) from FOM München. She speaks German, English, Spanish and Turkish.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

DAGDELEN: Cyber risk is one of the main concerns for companies around the globe. Due to the interdependent and correlated nature of cyber risks, not only from risk to risk but even from company to company, insurance solutions need to go beyond the traditional. Automation, digitalisation, the Internet of Things (IoT), artificial intelligence (AI) and Big Data are daily boardroom discussion topics. They not only present opportunities but also significant risks to companies of all sizes. This strongly points to IT security as a risk management priority. Companies should ensure that they are prepared for any cyber incident. Hackers targeting sensitive data, data breaches and business interruption are also major risks. The increasing use of cloud services and the implementation of AI provide hackers with new points of entry and increase the risk horizon. In fact, the risk horizon is ever-expanding, meaning that all companies, large and small, ought to continually assess their vulnerabilities and take preventive measures. In general, however, how a board prioritises cyber security differs considerably, depending on industry sector and company size.

Middle market corporations also seem to underestimate their vulnerabilities considerably.

Q. What demands are data privacy laws in Germany placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

DAGDELEN: As data accumulates, data privacy is becoming more crucial. The EU General Data Protection Regulation (GDPR), effective May 2018, requires organisations to have an incident response plan in place. These regulations require much preparation. New processes must be outlined and new rules defined. Any company risk and compliance department, worldwide, that interacts with the EU will be impacted. Conversely, according to a recent study from the Ponemon Institute, most mid-market companies do not have an incident response plan applied consistently across their entire organisation. Also, most countries surveyed feel they are not truly compliant with the GDPR.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

DAGDELEN: Cyber risk is a relatively new menace and, as such, historical data on the perils of breaches can be quite limited. As the risk landscape rapidly and constantly evolves, there are still uncertainties surrounding security technologies for risk reduction or potential for loss accumulations, which makes the risk difficult to measure for most companies. Yahoo, for example, not only lost billions of sensitive data records, but also took almost two years to identify all necessary details of the incident. On average, it takes an organisation 191 days to detect a data breach, according to the Ponemon Institute. A hacker may find a way into a company's systems and be present for months until taking action or being discovered. This, in general, limits an organisation's ability to mitigate the damage.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

DAGDELEN: Whereas IT systems might be protected reasonably well, they must be constantly updated and backed by a high level of technology. Vulnerabilities often result from human error. Human error is the number one cause of any financial loss from a cyber incident and yet it is so often underestimated. Armed with just an employee's full name and username, an imposter can call the company helpdesk requesting a new password. This is often an easier and more effective way to access company systems from the outside than any, more complex, technological method. As such, this makes a social engineering attack one of the fastest growing security threats for organisations. As cyber exposure increases, the implementation of effective employee security awareness programmes, in addition to implementing modern technologies, has become equally important to a company's survival.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

DAGDELEN: Companies need to identify and quantify their cyber exposure. They should liaise with their brokers and underwriters to quantify the risk and outline coverage decisions. However, as the symmetry of information between the insurer and the insured, relative to the real cyber exposure, is never fully achieved, processes need to be well prepared and carefully examined to get as close as possible to the most appropriate coverage. The cyber market is still young and a lack of historical data poses a challenge to insurance companies developing exposure models and setting premiums. Even wordings available in the market can differ on some critical points. Insurers' risk appetites also vary and this contributes to increased volatility in the cyber insurance market. Nevertheless, insurance markets make an important and positive contribution to cyber management by promoting risk awareness, encouraging measurement, supporting incident management and providing incentives for risk reduction.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

DAGDELEN: Companies should be encouraged to take out cyber security insurance because it typically provides first-party and third-party coverage. Cyber exposure may be covered under a specific endorsement on an existing policy, such as personal injury, property or crime insurance. However, unless it leads to a named peril or is captured in an exclusion in the policy it could be that any cyber related losses will not fall under the insurance clauses, and therefore, should not be relied upon. Available cyber security insurance policies in the market vary and it would be wise to consider several points, such as relevancy, depending on the range of exposure or business requirements, due to industry segment or otherwise. Sub-limits too should be an important consideration as these can essentially limit coverage. Whether contingent business interruption is provided, for example where a cyber incident at a third party can cause a business interruption for the policyholder, should be taken into account. Finally, whether the policy offers incentives to organisations to invest in security solutions should also be considered, as should ways to improve their network security.

“ Human error is the number one cause of any financial loss from a cyber incident and yet it is so often underestimated. ”

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

DAGDELEN: Cyber security should be a topic on every boardroom agenda if it is not already. The 2017 World Economic Forum identified cyber risk as one of the greatest concerns in doing business. Cyber attacks cause significant business interruption and will therefore continue to dominate media headlines mentioning data leaks, diverted funds, hacked elections or governments and so on. The growing scope of digitalisation in today’s economies also increases the future risk. New regulations and trends lead to new vulnerabilities relevant to cyber risk. Due to its dynamic nature, therefore, cyber security constantly presents fresh challenges for board members. Cyber security breaches, and their relevant disclosure and reporting procedures, influence and impact future earnings and business operations. Consequently, directors and officers of the company must be able to respond effectively to cyber-related litigation.

www.tmhcc.com

TOKIO MARINE HCC

Tokio Marine HCC is a leading specialty insurance group with offices in the United States, the United Kingdom, Spain and Ireland, transacting business in approximately 180 countries and underwriting more than 100 classes of specialty insurance.

GÜLSAH DAGDELEN
Senior Underwriter - Financial Lines
+34 93 530 7358
gdagdelen@tmhcc.com

Malaysia

DEEPAK PILLAI
Christopher & Lee Ong
Head of Technology, Media, Telecommunications & Data Protection
+603 2273 1919
deepak.pillai@christopherleeong.com

Deepak Pillai has practiced exclusively in the areas of telecommunications & technology law and personal data protection for two decades and is acknowledged as a leading telecommunications & technology lawyer in Malaysia. He advises clients on matters relating to IT contracts, electronic commerce, online financial services, outsourcing, telecommunications, IT security, personal data protection and digital media. He also advises a wide array of international, private and public sector clientele in addressing the commercial, regulatory and policy issues relating to information and communications technology law.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

PILLAI: The cyber risk environment is rapidly expanding, not only in terms of increasing risk exposure faced by companies and individuals from cyber risks, but also in terms of awareness of the cyber risks among corporate clientele and government authorities. There is also a growing realisation among the latter that there is a clear need for targeted regulation and the imposition of appropriate penalties. While cyber risks appear to be increasing for businesses, levels of accountability lag behind more mature jurisdictions, as evidenced by the very small number of lawsuits being brought against companies in relation to the damage and harm caused by cyber breaches. Over the past year, Malaysia has witnessed several major data breaches spanning the communications, broadcast, banking and medical sectors. The data breach involving the communications sector saw the personal details of 42 million mobile users being sold online. To date, no party has been penalised, though a court action has been mounted by an individual against the party that allegedly failed to take sufficient measures to prevent the breach.

Q. What demands are data privacy laws in Malaysia placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

PILLAI: In Malaysia, the Personal Data Protection Standard 2015 requires companies to have minimum security standards in place when processing personal data. Failure to comply could expose companies to fines of up to RM250,000 or imprisonment for up to two years. Other than this, the Personal Data Protection Act 2010 imposes fines of up to RM300,000 or imprisonment for up to two years for breach of the security principle which requires companies to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. There are no general breach notification requirements in place at present, but with the coming into force of the General Data Protection Regulation (GDPR), we expect that Malaysia will be adopting a breach notification regime in time. However, certain sectors are already subject to specific breach notifications to their respective regulators, such as listed companies and financial institutions.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

PILLAI: In terms of privacy risks, the message is slowly but surely starting to get through to business owners that privacy is one of the essential elements for business success, especially with the spate of news relating to recent Malaysian privacy breaches. Unfortunately, in terms of enforcement, it is still 'early days'. What will spur businesses on is the imposition of stiff penalties for reported data breaches, but it remains to be seen whether this will take place. In terms of detecting security breaches, as organisations do not typically disclose this information and would seek to handle these types of breaches without undue publicity, there have not been many security breaches reported of late. However, if there is any correlation between privacy breaches and security breaches, then it must be conjectured that the rate of security breaches is equally high.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

PILLAI: Broadly speaking, companies would need to identify all IT infrastructure assets and data that need to be secured, and assess the risks posed as a result of cyber-related risks. Companies would also need to ensure that the necessary risk management processes and procedures are conducted on an ongoing basis, which would include obtaining the necessary IT security certifications required, verifying adequate security controls have been deployed, ensuring that laws are complied with, managing the security postures of the vendors to the organisation, and conducting annual audits. Bearing in mind that IT incidents are unfortunately inevitable, it would also be incumbent on companies to plan for a cyber breach to mitigate the potential consequences. This would include ensuring disaster recovery, business continuity and incident response plans are deployed, assembling the relevant teams, testing plans at least annually, and ensuring that the necessary cyber insurance is in place.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

PILLAI: The market for cyber insurance in Malaysia is relatively new, with the first provider in Malaysia launching its cyber insurance policy in 2013. Although the market has grown, there remain only a handful of players in the Malaysian market. In response to requests from policyholders for a more comprehensive risk management approach to cyber insurance that includes risk assessments, insurance providers have partnered with IT service providers to offer clients cyber security tailored to their risk profiles. The IT service provider will assess the risk level of the organisation's IT systems, and based on the assessment, the insurer will provide insurance cover, access to tools and best practices. Insurance providers have also introduced value added services to enhance their cyber insurance solutions – providing policyholders with access to a dedicated risk portal which provides around the clock incident responses to help clients respond to cyber attacks more efficiently, and which provides helpful resource materials for policyholders, such as an incident road map, templates for a data security incident response plan and an e-risk resources directory.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

PILLAI: Companies should be wary of certain provisions. First, panel provision policies that require you to use the insurer's pre-approved forensic consultants and defence counsel. Second, consent provision policies which state that important costs, such as forensic and notification, along with defence costs, are only covered with the insurer's 'prior consent'. Third, war and terrorism exclusions, which eliminate coverage for cyber attacks from foreign countries with political, religious or social motivation or for personal gain. Fourth, any 'retroactive date' which may eliminate coverage for losses arising from events that precede the policy date.

"The market for cyber insurance in Malaysia is relatively new, with the first provider in Malaysia launching its cyber insurance policy in 2013."

Companies should have the retroactive date backdated as far as possible. Fifth, open-ended exclusions which seek to exclude coverage arising from a policyholder's failure to follow minimum required security practices or its own security protocols. Companies should ensure the policy wording includes coverage for loss of data, not just the theft of unauthorised data, and vendors' errors and omissions. The policy should state the insurer will pay for losses arising out of a breach of not just the insured, but also third parties, such as the service providers of the insured.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

PILLAI: With increased digital penetration, digitalisation of service offerings and take up of the services provided via the electronic and internet medium among Malaysians, this will likely result in increased regulatory oversight and the imposition of stiffer penalties for not securing a company's digital infrastructure and data. Due to the escalating financial and reputational damage that can arise from a cyber breach, we do not doubt that cyber risk management will be one of the major considerations for boards going forward, if not already.

www.christopherleeong.com

CHRISTOPHER & LEE ONG

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

Formed in 2013, Christopher & Lee Ong is part of the Rajah & Tann Asia network. Christopher & Lee Ong is led by a senior team of Malaysia-qualified partners who have accumulated considerable experience over the years in the Malaysian legal market. The firm's aim is to provide a truly collaborative approach in the best interests of its clients. At Christopher & Lee Ong, there is a belief that a winning performance for clients depends on a truly cooperative and collaborative approach to the practice of law.

DEEPAK PILLAI
Partner
+603 2267 2675
deepak.pillai@christopherleeong.com

INTAN HARYATI
Partner
+603 2273 1919
intan.haryati@christopherleeong.com

Taiwan

SEAN Y. S. LIU
Lee, Tsai & Partners
Associate Partner
+886 2 23 78 57 80
seanliu@leetsai.com

Sean Y.S Liu is an associate partner at Lee, Tsai and Partners, Attorneys-at-Law. He is an experienced litigator and has acted for clients from the government to major companies, domestic and abroad. He works on a wide variety of legal issues and specialises in construction, antitrust, unfair competition and commercial disputes. With an extensive understanding of technology and business, Mr Liu advises many major companies in corporate legal matters, such as electronic commerce, information security, licensing and others.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

LIU: The most serious cyber security incidents in the past two years were First Bank's ATM theft in 2016 and the cyber attack on Far Eastern Bank's SWIFT system in 2017. Both cases involved the careless management of information systems and insufficient personnel training and supervision. There have been a few instances where companies have endured a cyber attack despite solid management of information systems. Most cyber breaches involve human error. While the business environment is becoming increasingly internet oriented, many companies' internal control systems have been unable to keep pace. This has been the most significant risk in today's environment.

Q. What demands are data privacy laws in Taiwan placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

LIU: Industries which handle heavy volumes of personal data are required to have a security plan, which should include a notification mechanism. That said, different industries have different regulating authorities and thus face different security demands. Banks and other financial institutions have to meet the highest standards in Taiwan, set by the Financial Supervisory Commission (FSC). Failure to comply with the FSC's demands will result in fines and other penalties.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

LIU: First Bank and Far Eastern Bank suffered greater reputational than financial damage because most of the stolen money was recovered quickly after the incidents. It may have been that they were quick to detect the breach or perhaps it was just luck. One thing for sure is that, except for a few financial institutions and major tech companies, most companies in Taiwan do not have a sound cyber security system in place.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

LIU: Companies should devote substantial resources to establish a sound security system and keep it up to date. It is also important that companies hold periodic training sessions to remind employees of how important it is to play by the book.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

LIU: There are hundreds of thousands of companies in Taiwan, including more than 1600 listed companies, but only a few of them have bought cyber insurance – 139 in 2016 and 311 in 2017. The main reason for this is that the penalties included in Taiwan's Personal Information Protection Act are not strong enough. Furthermore, the legal system imposes a high burden of proof on consumers to prove their losses. Therefore, companies generally think the potential risk is too small to justify

the premium. Currently, financial institutions are more willing to buy cyber insurance because they have always been targets of cyber attacks. Another important reason is the fact that the FSC may impose much higher fines on financial institutions, pursuant to the Bank Act and other laws regarding financial institutions. Before the structural problems are solved, enhancing cyber insurance solutions will not greatly help the business of insurance providers.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

LIU: Most cyber insurance policies in Taiwan do not cover fines imposed by the authorities, indirect losses and the costs of upgrading information systems after a vulnerability has been detected. Therefore, in addition to the general provision of insurance, companies should pay attention to these exclusions.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

LIU: With businesses increasingly intertwined with the internet, I believe cyber risk management will climb the boardroom agenda.

"With businesses increasingly intertwined with the internet, I believe cyber risk management will climb the boardroom agenda."

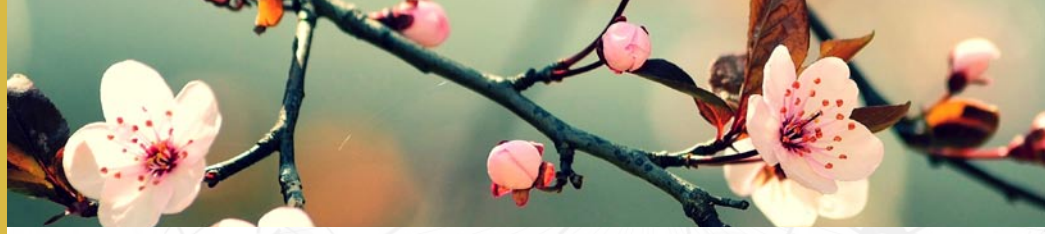
www.leetsai.com

理慈 Lee, Tsai & Partners

A GREATER CHINA LOCAL FIRM

Lee, Tsai & Partners provides inbound and outbound transactions legal advice, as well as advice on the most optimal structure for handling these transactions. The firm handles joint ventures, strategic alliances, distribution, licensing, real estate, employment, and merger and acquisition matters in the region. It also advises parties on how to structure dispute resolution clauses in cross-border transactions and on enforcing arbitral awards. The firm also has substantial experience in representing companies and state entities in disputes before the International Chamber of Commerce, the International Centre for Dispute Resolution, the China Maritime Arbitration Commission, CIETAC, and other institutions.

SEAN Y. S. LIU
Associate Partner
+886 2 23 78 57 80
seanliu@leetsai.com



Japan

MITSUHIKO MARUYAMA
Deloitte Tohmatsu Risk Services
Partner
+81 (3) 6213 1300
mitsuhiko.maruyama@tohmatsu.co.jp

Mitsuhiko Maruyama is a partner at Deloitte Tohmatsu Risk Services Co., Ltd as well as executive director at Deloitte Tohmatsu cyber security advanced laboratory. He has over 20 years of experience working with clients in a risk management and cyber risk capability, primarily IT governance and cyber risk. He is a recognised cyber expert contributing to several committees including the National Centre of Incident readiness and Strategy for Cybersecurity (NIST) and the Ministry of International Trade and Industry (MITI). His latest engagement to NISC is as the senior specialist for cyber security.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

MARUYAMA: We are seeing an increasing number of cyber attacks perpetrated by organised criminals and nation-state actors. The use of IT among attackers is evolving, as we have seen in the use of cryptocurrencies as a means of earning money, for example. Internet of Things (IoT) devices and factory systems are being targeted by attackers. IoT devices are also being used as an attack vector. Furthermore, attacks seem to be becoming larger in scale. New monetisation techniques, like cryptocurrency mining malware are also emerging, and the traditional cyber attack framework may not be able to detect them.

Q. What demands are data privacy laws in Japan placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

MARUYAMA: The Personal Information Protection Act (PIPA) of Japan was enacted in 2003 and was amended in 2017. The amendment was intended to align it with other privacy protection laws around

the world, including those in the EU. The legal system around information management will be further developed by reflecting more sensitive information, such as genetic and healthcare data. A certain level of change to internal processes will be required if companies are to conform to the PIPA. However, considering that it has been aligned with equivalent EU laws, the Japanese PIPA does not impose particularly severe requirements on companies, compared to the global standard. That being said, each country has a different privacy policy, so conforming to all of the relevant privacy laws will be even more complicated for global enterprises. More and more countries, including China, Russia and Vietnam, require companies to store personal data domestically, so we need to pay attention to how the 'data localisation' trend develops moving forward.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

MARUYAMA: Since the PIPA requires companies to inform the affected data subjects as well as the competent regulatory authority of any personal data leaks or other incidents, they can now act more quickly on any personal information incidents, once they have been identified. On the other hand, many companies are still not up to speed on detecting security breaches in general, and it is still common that security incidents are first detected by external parties. It would be prudent for organisations to enhance their monitoring on 'edge devices', endpoints and other systems so that better mechanisms can be established to detect incidents as quickly as possible. It would also be wise for companies to implement AI and other technologies as early as possible.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

MARUYAMA: In Japan, ISO/IEC 27001 Information Security Management System has rapidly spread, and executives have established policies along with it. Thus, the mechanism to create a good plan-do-check-act (PDCA) cycle has been adopted fairly easily. On the other hand, some organisations just pretend to have created a good management system; indeed,

a number of organisations have declared that they have created a good system, although they actually have not. We need a system which will enhance security measures by simulating more practical attacks, such as recovery time objective (RTO).

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

MARUYAMA: Insurers are commoditising cyber insurance by selling it to a wide range of companies, including small and medium enterprises (SMEs). Such insurance mainly covers incident response cost, indemnification of victims, investigation cost, and so on. There are some insurance policies that also cover parts of the cost of establishing a recurrence prevention system. It is predicted that damage due to cyber attacks will increase and so will the need for cyber insurance among SMEs.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

MARUYAMA: Data loss is probably the number one area to apply cyber insurance to, so companies usually purchase cyber insurance policies to apply to the entire company, instead of buying them for each system. Moving forward, challenges will arise around the need for higher amounts of coverage, or how to combine policies from multiple insurers effectively to reduce insurance cost.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

MARUYAMA: Cyber attacks and potential data losses are regarded as threats globally, as well as in Japan. As more systems become connected, the threat of cyber attack will continue to grow.

“ Moving forward, challenges will arise around the need for higher amounts of coverage, or how to combine policies from multiple insurers effectively to reduce insurance cost. ”

www2.deloitte.com

Deloitte.
デロイト トーマツ

As a member firm of Deloitte’s Cyber Risk Services (CRS) team, Deloitte Tohmatsu Risk Services provides high-quality consulting service concerning risk management. The firm works in close coordination with other organisations of Deloitte Tohmatsu Group (Deloitte Japan) and with member firms of Deloitte Touche Tohmatsu Limited (DTTL) throughout the world in order to provide IT risk consulting services for leading global companies and organisations.

MITSUHIKO MARUYAMA
Partner
+81 (3) 6213 1300
mitsuhiko.maruyama@tohmatsu.co.jp

Australia

PAUL KALLENBACH
MinterEllison
Partner
+61 3 8608 2622
paul.kallenbach@minterellison.com

Paul Kallenbach is MinterEllison's head of cyber law and data protection and is a technology law specialist. He advises Australian and international companies on technology contracting and licensing, outsourcing and procurement, privacy and data protection, intellectual property rights and telecommunications and ecommerce law. He co-founded Exari, a leading provider of document automation technology, is a director of MinterEllison's software companies, Safetrac and Boardtrac, and is on the advisory board of MinterEllison's newly acquired technology consulting arm, ITNewcom.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

KALLENBACH: There has been a rise in cyber risk mitigation activity in the six to 12 months leading up to Australia's new mandatory notifiable data breaches regime. The subsequent implementation of the EU's General Data Protection Regulation (GDPR) has contributed to this activity, which continues to increase. The main trend that has emerged in recent months is the rise of sophisticated social engineering or 'human hacking' incidents, with senior financial employees targeted in criminal attempts to intercept payments. Another trend has been a rise in data breaches occurring within a third-party supplier's computer systems – data processors, using GDPR's terminology – but impacting data owned or controlled by the principal entity, known as data controllers under the GDPR. These emerging risks highlight the need to adopt a comprehensive approach to cyber resilience planning. For example, social engineering incidents are often best prevented through a combination of raising awareness, implementing policies and providing training.

Q. What demands are data privacy laws in Australia placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

KALLENBACH: Privacy and cyber security are certainly hot topics in Australia at the moment and we are continuing to see increased levels of engagement in this area. In our experience, organisations generally have a base level of compliance which they are continually working to enhance to meet evolving regulatory obligations, heightened community expectations and ever-increasing cyber risk. The GDPR has been a game-changer in this space. While this new regime only impacts a proportion of Australian businesses, it has created a new gold standard for compliance. We have seen evidence that organisations that are not strictly obliged to comply with the GDPR are still aspiring to compliance. This seems to be part of a wider trend toward organisations using privacy compliance as a differentiator, from a reputational perspective.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

KALLENBACH: Many organisations are educating themselves on the changing regulatory landscape and are actively working toward compliance. However, our 2018 annual cyber survey identified inadequate levels of practical incident response planning. For example, while 70 percent of respondents identified as having a 'fair' or 'good' understanding of cyber exposure, only 54 percent of organisations had a data breach response plan in place. Furthermore, only 40 percent of surveyed organisations are prepared for the new notifiable data breaches scheme in the months leading up to its implementation.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

KALLENBACH: Companies know best what data of theirs has value outside of their organisation. A useful starting point

is to identify data that is 'at risk', whether due to regulatory oversight or commercial considerations, and work toward enhancing existing protections to better manage that risk. The Australian government and related agencies have invested heavily in providing guidance to organisations interested in improving cyber security protections. The Australian Signals Directorate has produced a 'Guide to Strategies for Mitigating Cyber Security Incidents', which has been widely adopted by government agencies and businesses in Australia. The Office of the Australian Information Commissioner has also published a guide to securing personal information.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

KALLENBACH: The Insurance Council of Australia has identified cyber insurance as the fastest growing commercial segment of the Australian market. Insurance providers are identifying and responding to emerging cyber risks. There are a number of providers offering low-cost standalone cyber and privacy policies to small and medium enterprise (SME) companies, which are keen to mitigate the risks but do not wish to spend large amounts on this. Further, many cyber insurers have started to offer social engineering endorsements in response to the rise in 'human hacking' incidents.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

KALLENBACH: Organisations should seek specialist advice from experts with experience in cyber insurance to avoid potential gaps in coverage. A common example in Australia is for funds lost as a result of a successful social engineering incident to fall between an organisation's cyber policy and crime policy, on the basis that the payment was made 'voluntarily'. However, insurers are alert to this issue and have introduced products, such as social engineering endorsements, to address such gaps in coverage. It is also important that organisations recognise that cyber insurance, while a key risk management measure, should not be seen as a panacea for cyber risk exposure.

"The Insurance Council of Australia has identified cyber insurance as the fastest growing commercial segment of the Australian market."

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

KALLENBACH: Boards are becoming increasingly educated and informed in relation to cyber security and cyber risk, and will continue to do so in this evolving cyber and regulatory landscape. With the implementation of a notifiable data breaches scheme in Australia, and the GDPR and related developments abroad, boards are likely to become increasingly aware of the risks as data breaches are escalated within organisations.

www.minterellison.com

MinterEllison

MinterEllison is an international law firm, headquartered in Australia and regarded as one of the Asia-Pacific's premier law firms. Its teams collaborate across Australia, New Zealand, Asia and the UK to deliver exceptional outcomes. The firm has a clear goal – to be its clients' best partner. The firm puts clients at the centre of everything it does and partners with them to deliver truly innovative solutions. The firm also thinks beyond the law, offering clients advisers who are multi-disciplinary and industry-facing to help them realise their strategic goals, grasp business opportunities and create value for their stakeholders.

PAUL KALLENBACH
Partner
+61 3 8608 2622
paul.kallenbach@minterellison.com

LEAH MOONEY
Special Counsel
+61 7 3119 6230
leah.mooney@minterellison.com

Bahrain

STEVEN BROWN
Al Ruwayeh & Partners (ASAR)
Partner
+973 17 533 182 /3
sbrown@asarlegal.com

Steven Brown is a partner at ASAR – Al Ruwayeh & Partners, joining the firm since June 2010. He primarily practices in the areas of mergers and acquisitions, banking and finance, corporate law, regulatory law and employment law. He holds a Juris Doctorate, awarded in 2007, from Washington University in St. Louis (United States). He was admitted to practice law in New York in 2010. Since he has managed the Bahrain office, ASAR has acted as counsel on a number of major local and multinational restructuring projects, including leading the restructuring of Ithmaar Bank for regulatory capital purposes.

Q. How would you summarise today's cyber risk environment? What new risks have emerged in the past 12-18 months?

BROWN: In Bahrain, cyber risk is constantly being affected by the rise in the use of technology and the recent introduction of electronic wallets in Bahrain. Bahrain has taken a strong stance on protection of online payment systems, noting that this has been led substantially by the private sector. Use of one-time password (OTP), randomised e-pin input pop-ups and other online tools to protect against cyber criminals' use of Bahrain issued cards has expanded through the last 12 months. In particular, Bahrain has introduced a regulatory sandbox for the introduction and promulgation of electronic payment systems by the Central Bank of Bahrain. How effectively encryption and anti-hacking mechanisms will be in light of cash, rather than mere information, being maintained in electronic form remains to be seen.

Q. What demands are data privacy laws in Bahrain placing on companies to implement security measures and follow notification requirements? How challenging is it to maintain regulatory compliance?

BROWN: As of May 2018, Bahrain has not introduced a formal data privacy legislation or regulatory regime. Accordingly, data privacy falls under the general rubric of wrongful actions implemented by the Bahrain court. The lack of information regarding which security measures are followed, along with a general under-appreciation of the value of private information, has had the effect that most entities, other than banks, avoid spending on data protection software or systems. Moreover, other provisions concerning data protection lack the consequences, and often include substantial vagueness in the definition of violations, making them essentially unenforceable.

Q. Would it be fair to say that, in general, organisations are still not up to speed on detecting security breaches and privacy risks quickly enough?

BROWN: We note that financial institutions have led the way on ensuring data privacy and protection. This derives in part from heightened expectation by the Central Bank of Bahrain. Moreover, restrictions on outsourcing have introduced a level of enhanced protection which is quasi-regulatory. For example, the regulator may refuse an outsourcing agreement for inadequate data security or privacy notwithstanding a lack of clear regulations on the requirements for such services. We believe banks regularly look to outsource data protection, as it is not a core competency. We note that data breaches are not published, nor are they required to be published, under Bahrain law. Therefore, it is difficult to tell if organisations are engaged in the type of notification to customers, or on detecting breaches promptly, which may be found in other jurisdictions.

Q. What steps should companies take to establish appropriate processes and policies to manage cyber related risks and keep systems safe?

BROWN: There is discussion surrounding the introduction of a data privacy law in the immediate future. It would be most appropriate for companies to await implementation of such a law prior to developing protocols and systems. Nevertheless, we believe that a progressive entity headquartered or operating in a jurisdiction where data privacy is taken very seriously could implement similar procedures in Bahrain and remain a market leader in the field even after

any data privacy law is introduced. For an entity without a current nexus to a data protective regulatory regime, strong consideration could be given to implementing best practices derived from European jurisdictions as a starting point to implementation of appropriate processes.

Q. How are insurance providers enhancing their cyber insurance solutions to meet market demands and help companies manage the downside?

BROWN: We have not seen any insurance entities providing cyber insurance solutions. It should be noted that insurance policies covering risk in Bahrain must, generally, be underwritten in Bahrain. Moreover, insurance policies underwritten in Bahrain are subject to regulatory review. Accordingly, the roll-out of cyber insurance solutions would require an active role from the Central Bank of Bahrain. Any insurance company looking to roll-out such a product would likely be a first mover and bear substantially higher administrative costs than later participants, which may be delaying interest in providing such insurance products.

Q. What considerations should companies make when evaluating cyber insurance coverage, including pricing, policy provisions and exclusions?

BROWN: Unfortunately, due to the absence of such polices, at least from mainstream knowledge, it is not possible to discuss evaluation factors. As these products become more available and begin to compete with each other, this will allow the nuanced analysis of optimal types of insurance coverage. Also, the introduction of any data protection regime will form a starting point for cyber insurance underwriters to analyse the risk of claims accurately and thereby allocate appropriate premiums for such insurance.

Q. Going forward, do you expect cyber risk management will continue to climb the boardroom agenda as major cyber threats increase?

BROWN: While we believe that these threats will be readily recognised by boards which, until now, may not have given much thought to these matters, we believe that Bahrain businesses do not view cyber risk as a priority. Instead, we

> *"With the lack of public pressure, we believe that companies will have less interest in spending significant funds to protect customer information for customers who are not raising objections to the use of their data."*

believe that the introduction of data protection legislation will spur these discussions and may result in greater focus by directors. We also note that public sentiment has not rallied against the type of data infringement which draws headlines in other jurisdictions. With the lack of public pressure, we believe that companies will have less interest in spending significant funds to protect customer information for customers who are not raising objections to the use of their data.

www.asarlegal.com

ASAR
AL RUWAYEH & PARTNERS
Attorneys and Legal Consultants

Al Ruwayeh & Partners (ASAR) is the largest full service corporate and commercial law firm in Kuwait and one of the largest in the Middle East, with strong connections throughout the Gulf region. As one of the region's premier law firms to many foreign and domestic multinational companies, the firm advises many of the biggest and most ambitious organisations. ASAR has been operating in the State of Kuwait since 1977 and in the Kingdom of Bahrain since 2006, and has been recognised for professional legal services of the highest order.

STEVEN BROWN
Partner
+973 17 533 182 /3
sbrown@asarlegal.com

HISHAM AL QURAAN
Partner
+965 2292 2700
halquraan@asarlegal.com

PAUL DAY
Partner
+965 2292 2700
pday@asarlegal.com

www.financierworldwide.com