ROUNDTABLE January 2022

CYBER SECURITY

Amid colossal pandemic-generated disruption over the past two years, the global economy has witnessed burgeoning cyber crime – a complex and fervent landscape that has become increasingly sophisticated as cyber criminals continue, and even escalate, their activity in times of crisis. As a result, business and government need to prioritise their focus on cyber security to address, prevent and respond to multiplying attacks, adhering to a 'not if, but when' mode of thinking when it comes to security breaches and ensuing impacts. ■

THE PANELLISTS

Lynn Peachey
Director of Business Development, Arete
T: +1 (908) 635 1677
E: lpeachey@areteir.com
www.areteir.com

Lynn Peachey is the director of business development, cyber insurance channel at Arete, focusing on customer service and maintaining partnerships with cyber insurance firms. With more than six years of experience in the cyber claims industry, she works with a team of experts to build a wide range of solutions for clients. Prior to joining Arete, she exclusively handled first- and third-party cyber claims, technology errors and omissions claims, and media injury liability claims for two of the largest cyber insurance carriers in the US.

Raf Sanchez
Head of Cyber Services, Beazley
T: +44 (0)20 7667 0541
E: raf.sanchez@beazley.com
www.beazley.com

Rafael (Raf) leads Beazley's global cyber services team, BBR Services, with responsibility for coordinating and delivering Beazley's suite of incident response and cyber risk services with a focus on giving clients the power, autonomy, knowledge and desire to proactively manage down their cyber exposure by investing in and building out their cyber resilience. He joined Beazley from Bank of America Merrill Lynch where he was an assistant general counsel and director of its UK business.

James Owen
Partner, Control Risks
T: +1 (0)20 7070 2100
E: james.owen@controlrisks.com
www.controlrisks.com

James Owen is global head of cyber security at Control Risks, overseeing the threat intelligence, cyber risk consulting and cyber response teams in EMEA, Asia and the Americas. In this role, he supports organisations navigating cyber and digital risk challenges through threat-led advice, strategic perspective, globally coordinated support, and practical and business risk expertise.

David Navetta
Partner, Cooley LLP
T: +1 (720) 566 4153
E: dnavetta@cooley.com
www.cooley.com

David Navetta is a vice chair of Cooley's cyber data privacy group. Mr Navetta has focused on technology, privacy and information security law since 2002. His work ranges from privacy compliance and product development, and transactional work, to breach notification, regulatory response and litigation. He is a certified information privacy professional through the International Association of Privacy Professionals and previously served as a co-chair of the American Bar Association's information security committee.

Siân John
Senior Director, Microsoft
T: +44 (0)118 909 4786
E: sian.john@microsoft.com
www.microsoft.com

Siân John MBE is senior director of security business development and strategic growth at Microsoft. She leads a team focusing on developing opportunities for Microsoft to deliver new security and compliance, and to identity offerings to market. She is a fellow of the Chartered Institute of Information Security and was awarded an MBE in the Queen's 2018 New Year's Honours List for services to cyber security.

Todd Hinnen
Partner, Perkins Coie LLP
T: +1 (206) 359 3384
E: thinnen@perkinscoie.com
www.perkinscoie.com

Todd Hinnen is a partner with the firm's privacy and security practice. He counsels clients and represents them in litigation regarding privacy, data security, compliance with law enforcement and national security issues. He works closely with the Department of Justice and the Intelligence Community.

Eduard Blanxart Raventos
Senior Underwriter – Financial Lines, Tokio Marine HCC
T: +34 93 530 7349
E: eblanxart@tmhcc.com
www.tmhcc.com

Eduard Blanxart Raventos is senior underwriter – financial lines for Iberia and Latin America. His focus on financial lines also includes cyber insurance and financial institutions. Prior to joining Tokio Marine HCC, he worked for Chubb, Banco Sabadell and Zurich Insurance Company in Barcelona and London.

Great Gu
Chief Information Security Officer, Zai Lab
T: +86 189 1652 7303
E: great.gu@zailaboratory.com
www.zailaboratory.com

Great Gu is a cyber security, risk management and IT governance expert. He is an International Association of Privacy Professionals Asia Advisory board member. He won the ISC 2017 Asia-Pacific Information Security Leadership Achievements award, as well as the only one from China mainland. He is frequently invited to speak on cyber security topics for online seminars and large-scale conferences across Asia-Pacific, and to host elite cyber security panels.

FW: Could you provide an overview of the cyber risks currently facing businesses, organisations and governments across the globe? What are some of the common types of cyber threats, and how have they evolved in recent years?

Peachey: Organisations, large and small, are inundated with information – from government advisories to insurance policy changes – on how to best address increasing cyber risk. They are forced at the highest levels to confront their cyber security posture. And for good reason. According to the Federal Bureau of Investigation, Americans filed nearly 800,000 cyber crime complaints in 2020 – a 300,000-plus increase from 2019 – with reported losses of more than $4.2bn. Most of the cases we see are ransomware-related or business email compromises. While ransomware was once a trivial cyber risk, with cyber criminals extorting small fees from victims with minimal downtime, it has evolved into a highly technical criminal operation. Threat actors are constantly learning to evade best practices with new tactics, for instance exfiltrating data and demanding ransoms in exchange for not publishing stolen data. They charge astronomical sums for decryption keys or promises of non-publication all while crippling victims for weeks at a time, costing them millions in business-interruption losses.

Navetta: Companies in all industries, even non-traditional targets such as manufacturers, oil pipelines and food suppliers, are common targets for threat actors on a daily basis. Ransomware is a serious threat because of its impact. It is one thing to have certain personal information taken from an organisation, or funds taken from a company through account takeovers and wire transfer fraud, and quite another when a hack brings down an entire organisation. The impact faced by companies now impacts their very ability to operate, to provide goods and services to customers that make up their core business. These events often result in direct income loss, loss of customers, degradation of reputation, and for public companies, stock value drops. Unfortunately, because the stakes are so high and victims are willing to pay up to tens of millions of dollars in ransom, the 'market' for these attacks is vibrant and the cost of them is increasing. The market incentives driving ransomware make every company extremely vulnerable – the threat actor groups have built up their monetary resources, created better tools and recruited more attackers.

Sanchez: Organisations face a sophisticated, well-funded and innovative cyber criminal landscape where there is very little chance of being punished, let alone physically apprehended. Although there are many threats aimed at acquiring sensitive government or commercial information and others that are destructive in nature, most cyber threats are those that have financial gain as their ultimate purpose. Within financially motivated cyber crime we see automated attacks aimed at acquiring user credentials, for example email phishing campaigns, automated and manual attacks that leverage vulnerabilities in common platforms to obtain access to networks and, possibly most importantly, we see ransomware attacks that involve extorting organisations for the return of their valuable data in exchange for large sums of cryptocurrencies.

Raventos: The European Union Agency for Cybersecurity (ENISA) has recently published its 'Threat Landscape 2021' report. As expected, the study shows that over 2020-21, ransomware was the primary threat on the cyber landscape, with cyber criminals increasingly motivated by monetising their activities. The tactics and techniques employed by cyber criminals have been increasing in complexity – for example, the 'triple extortion' technique, where ransom demands are not only directed at a victim but also at their client or supplier, are becoming increasingly widespread. According to ENISA, the highest ransomware demands grew from $15m in 2019 to $30m in 2020 and to $50m in March 2021. Considering that the latest ransom demand was $70m, made to Kaseya in July 2021, we will probably see $100m in ransomware demands in 2022. Obviously, this is becoming a big concern for companies. Aside from ransomware, the study shows that other types of cyber threats, such as crypto-jacking infections, COVID-19 email campaigns, healthcare data breaches or distributed denial of service campaigns, are also on the rise.

John: This past year the world has been witness to a burgeoning cyber crime economy and the rapid rise of cyber crime services. We have watched this global market grow in both complexity and fervency as the cyber attack landscape becomes increasingly sophisticated as cyber criminals continue – and even escalate – their activity in times of crisis. Cyber crime as a service, especially ransomware, remains a serious and growing plague. But while nation-state actors mostly target victims with useful information, cyber criminals target victims with money. Ransomware continues to be one of the largest cyber crime threats and, in the past year, it has continued to evolve to become more disruptive. Indeed, 58 percent of all the cyber attacks we have observed during this period have come from Russia, according to our 'Digital Defense Report'. Moreover, attacks from Russian nation-state actors are increasingly effective, jumping from a 21 percent successful compromise rate in 2020 to a 32 percent rate in 2021. Russian nation-state actors are increasingly targeting government agencies for intelligence gathering, which jumped from 3 percent of their targets a year ago to 53 percent – largely agencies involved in foreign policy, national security or defence. The top three countries targeted by Russian nation-state actors were the US, Ukraine and the UK. After Russia, the largest volume of attacks we observed came from North Korea, Iran and China. South Korea, Turkey – a new entrant – and Vietnam were also active, but represent much less volume.

Hinnen: Both threat actors and the types of threats that comprise the threat landscape have diversified in recent years. Sophisticated and well-resourced nation-state actors and organised crime syndicates that pose a threat to even the best protected companies have multiplied and software provider supply chain compromises and

hybrid ransomware and unauthorised access attacks have increased the scope and scale of incidents. Businesses, organisations and governments must invest more resources across the board, including specialised cyber security personnel, additional network security tools and applications, more rigorous vendor security programmes, additional training and awareness raising for all personnel, testing and penetration testing, as well as effective incident response planning and exercising. This will help maximise their ability to stay ahead of the curve and minimise their legal risk. Simply put, they need to move cyber security up in their list of organisational priorities.

Gu: At present, global enterprises, organisations and governments are facing increasing network risks from internal data leakage and external hacker organisations. Internal data leakage refers to data security incidents caused by employees or third parties. External hacker organisations generally carry out encrypted extortion for the purpose of money, and such cases can be found everywhere. The common types of network threats include social engineering, penetration injection and advanced persistent threat attacks. In recent years, it can be observed that individual threats have changed to groups, and attacks with weak information security awareness are more effective.

Owen: Ever higher rates of connectivity and the sprawl of technology are supercharging the cyber threats companies and governments face today. Attackers are increasingly targeting digital supply chains and critical technology third parties, given that the compromise of a single software update process can reach thousands of companies around the world. Ransomware continues to challenge, especially hybrid attacks combining encryption and data leak extortion. Disruptive attacks on operational technologies and cyber physical systems powering critical national infrastructure are also posing existential national security challenges to governments. Attackers leverage traditional access vectors such as phishing in most of these attacks, but a new focus on third parties has seen the return of web-facing vulnerability exploitation. Putting security controls in place to mitigate these risks is crucial, but right now businesses are struggling to keep pace with the rapid proliferation of cyber threats.

FW: In your experience, how are companies coping with the regulatory environment around cyber and data? To what extent are they meeting their compliance requirements?

> MULTINATIONAL ENTERPRISES HAVE BEGUN TO CONTINUOUSLY MONITOR AND UNDERSTAND THE CYBER SECURITY LAWS AND REGULATIONS OF COUNTRIES IN WHICH THEY DO BUSINESS.
>
> GREAT GU
> Zai Lab

Navetta: One of the first things that regulators ask about after a significant beach is to provide information concerning the victim's information security programme, and whether it meets applicable legal standards and regulatory requirements. Most diligent companies are focused on appropriately securing their environments, but despite some preaching from the legal community they are less focused on building a legally defensible security programme. The challenge in this context is that companies must defend their security programme after having suffered a breach. Legally speaking, security breaches should not be 'strict liability' events – companies can have reasonable security programmes and still suffer a breach, and in those cases they should not be liable. As such, more focus needs to be put into the rationale for developing a security programme. Legally defensible security is the story as to how a security programme was developed, including the risks that were assessed, how they were mitigated, the standards that were used and the industry benchmarks that were met, among other factors. If the legal team is not working closely with the security team, this aspect of data security, compliance and regulatory is often overlooked, which makes regulatory scrutiny much more challenging.

Sanchez: Privacy and cyber security laws, regulations and standards abound, and this is part of the problem for organisations that face a series of sometimes conflicting, or at the very least abstract, requirements that are often not aligned with the true challenges that organisations face. While compliance with these requirements is critical, organisations also must balance these against operational concerns that may require crucial spend elsewhere. Compliance with laws and regulations not only improves cyber risk profiles but can also be used by organisations for competitive advantage. Supply chain risk has become a real concern over the past 18 months, so an organisation that can assure its customers of its robust cyber risk profile is likely to win out over competitors that cannot offer the same assurances.

Raventos: In total, there have been more than 281,000 data-breach notifications since the European Union's (EU's) General Data Protection Regulation (GDPR) was introduced in 2018. According to DLA Piper's 2021 GDPR and data breach survey, fines imposed for a wide range of infringements of Europe's data protection laws have totalled €272m, with Italy at the top of that list. Furthermore, strict interpretations of the GDPR by regulators are setting the scene for heated legal battles in the years ahead. The US also has hundreds of privacy and data security requisites laid out across its states, such as the requirement for safeguarding data, data disposal, privacy policies, and the appropriate use of social security numbers, among others. Brazil enforced the General Personal Data Protection Law in September 2020, the first comprehensive data protection regulation in line with GDPR. We should start to see more fines issued from Brazil in 2022. It is not an easy task for companies to meet all these legal and compliance requirements and it is especially complex for large multinational companies which must consider the different and specific regulations applicable in the many jurisdictions in which they may operate.

> CONSCIENTIOUSNESS AND AWARENESS ARE KEY, FROM THE BOARD AS WELL AS EMPLOYEES IN GENERAL, AS THE HUMAN FACTOR PLAYS A BIG PART IN CYBER SECURITY.
>
> EDUARD BLANXART RAVENTOS
> Tokio Marine HCC

John: As organisations go through digital transformation, they are generating and consuming much more data than in the past to help them gain an edge over their competitors. This data is necessary to continue to stay relevant by empowering employees, engaging customers and optimising operations. Managing this data and the variety of devices on which it is created can be complicated, especially when it comes to ensuring compliance. According to a recent report about the cost of compliance, there were more than 215 regulation updates a day from over 1000 regulatory bodies all over the world, a slight decrease from the previous year. The cost of non-compliance is more than twice that of compliance costs. Some of the challenges we are seeing due to the dynamic nature of the compliance landscape include the following. First, keeping up with the constantly changing regulations. With all the regulatory and standards bodies creating new or revising existing requirements and guidelines, keeping up to date is time and resource intensive. Second, point-in-time assessments create a digital blind spot. Many organisations rely on point-in-time assessments, like annual audits. Unfortunately, they can go out of date quickly and expose the organisation to potential risks until the next assessment is done. Organisations are looking for ways to improve integration and create near real-time assessments to control risks caused by digital assets. Third, inefficient collaboration and siloed knowledge lead to duplication of effort. Organisations are often challenged due to siloed knowledge concerning IT risk management. IT and security administrators know the technology solutions but find regulations difficult to understand. Contrast that with compliance, privacy and legal teams who tend to be familiar with the regulations but are not experts in the technology available to help them comply. In addition, many organisations start their compliance journey using general-purpose tools like Excel and try to track compliance manually, but quickly outgrow this approach because of the complexities of managing compliance activities. Finally, complexity across IT environments hinders adoption. Understanding how to integrate the many solutions available and configure each one to minimise compliance risks can be difficult. This is especially true in organisations with solutions sourced from multiple vendors that often have overlapping functionality. Decision makers want simple, step-by-step guidance on how to make the tools work for the industry standards and regulations they are subject to.

Hinnen: As high-profile cyber incidents have increased, regulatory requirements have proliferated and companies are spending more time and resources understanding them and meeting their requirements. This regulatory proliferation has both good and bad aspects. It is encouraging companies to pay attention to cyber security and to invest more resources in it. To the extent such regulatory requirements are poorly coordinated or duplicative, however, they can be as much of a distraction as they are a benefit, as companies map their cyber security programmes against yet another regulatory framework, instead of focusing on overall programme strength and health. And onerous regulatory requirements can create a barrier to entry for new companies looking to enter the market, even those willing to make an investment in cyber security that is appropriate to their business model and stage of growth.

Gu: Multinational enterprises have begun to continuously monitor and understand the cyber security laws and regulations of countries in which they do business. For example, China has a cyber security law, data security law and personal information protection law. Active preparation and effective communication can enable most enterprises to meet the compliance requirements of local law and regulation. Companies are gradually progressing their cyber posture toward meeting compliance requirements.

Owen: Compliance teams are grappling with stricter and more fragmented global regulations. A complex mosaic of data privacy and cyber security legislation is requiring compliance teams to map their data flows to assess their exposure, given the likelihood and impact of a data localisation failure is now much higher. This, in turn, is making it more important that effective compliance and security controls are built into future state digital transformation and technology planning. Compliance teams should also expect to see more systems-driven regulation in the next few years, especially in the US and Europe. The politicisation of technology is complicating matters. Many countries are now actively seeking to sanction the use of technologies that are owned, controlled or subject to the laws of foreign jurisdictions. It is a combustible mix, underscoring the different and often politically motivated ways in which data and technology are now viewed globally.

Peachey: On the digital forensics and incident response (IR) vendor side, we are seeing more organisations looking to start pre-breach planning, get to know vendors, invest in endpoint detection and response (EDR), migrate to the cloud and implement multifactor authentication (MFA). They understand how these are huge gaps that, if filled, can drastically reduce their attack surface. Organisations have also become increasingly aware of third-party supplier risk. As a result, they are not only asking for but requiring detailed information on suppliers' internal processes and procedures.

FW: What advice would you offer to boards and senior management in terms of protecting their company networks and the data housed within them? What key questions should they ask when reviewing and reinforcing frameworks, policies and processes?

Sanchez: Senior management should understand that to holistically protect their organisations, they must understand that electronic data and communication forms a crucial part of their organisations' reputation, goodwill, customer trust, revenues and operations. Buildings, stock and equipment are tangible and the risk of their theft or destruction may be easier to imagine than the risk of theft or destruction of intangible assets such as databases, websites or even goodwill and reputation. Electronic data and communications form a crucial basis for most organisations' operating models, so any framework, policy or process should ensure that those intangible resources are measured, assessed and protected.

Raventos: Conscientiousness and awareness are key, from the board as well as employees in general, as the human factor plays a big part in cyber security. Each company is unique, but to achieve an adequate level of maturity, companies should be consistent in their methodologies, and in the case of large multinationals, these methodologies should be applied groupwide. Companies can use solid frameworks such as National Institute of Standards and Technology (NIST) or International Standard Offering (ISO) but testing all these frameworks, controls and procedures within their company is equally important. Testing procedures, lessons learned and remediation actions all count toward achieving a good level of cyber security maturity.

John: Organisations should be regularly evaluating their risk threshold. When we talk about risk, this should include an evaluation of an organisation's ability to effectively respond to changes in the cyber landscape.

Hinnen: Boards need the expertise to conduct effective oversight of their companies' cyber security programmes, whether through the inclusion of board members with expertise or the retention of cyber security experts to assist them in understanding the issues and meeting their oversight obligations. Both boards and senior management need to dedicate their sustained attention to the issue, revisiting it regularly, requiring reporting

> "ONCE A COMPANY HAS A PLAN, THE COMPANY SHOULD EXERCISE IT REGULARLY, IDENTIFYING GAPS AND WEAKNESSES, REFINING PROCESSES, AND REVISITING WHETHER THE PLAN IS ATTUNED TO CURRENT THREATS."
>
> TODD HINNEN
> Perkins Coie LLP

and tracking programme development. They should be asking key questions. What are our greatest risks? What steps have we taken to effectively protect against them? When was the last time we penetration tested our networks? What additional tools and resources do we need to improve our cyber security posture? Are we adequately insured to weather a major incident if, despite our best efforts, we become a victim?

> OPERATIONAL RESILIENCE REQUIRES A STRATEGIC AND HOLISTIC VIEW OF WHAT COULD GO WRONG, AND HOW AN ORGANISATION WILL RESPOND.
>
> SIÂN JOHN
> Microsoft

Gu: Boards and senior management need to continuously evaluate and assess the enterprise's information security management capability. As the basis of information security strategy, in the face of external compliance requirements and internal data protection requirements, it is recommended that boards and senior management pay attention to investment in information security management capability, invest appropriate resources in weak areas, and improve and strengthen the framework, policies and processes.

Peachey: We still see many large organisations that do not know where their sensitive data resides or what comprises a given data set. If a threat actor exfiltrates a database whose contents are unknown, it is difficult to ascertain a client's bottom line, which in turn can complicate the negotiation process, add internal burden to an already stressful IR process and delay notification obligations. Organisations should know what data they are holding, for how long and where. They should check that it is securely copied in three different places across three different media types. For example, is it stored in the cloud? Offline? Is it air-gapped and routinely tested? I would also recommend not only practicing IR plans, but also business continuity plans (BCP). Cyber security is everyone's responsibility. So, hold every employee accountable to the company's cyber security objectives and be sure everyone is trained to avoid risks like phishing emails and malicious links.

Owen: Boards and senior management teams should view cyber as a security, compliance and resilience issue. Organisationally, it is crucial to have clear ownership for cyber risks at the top of an organisation. A robust security structure and culture is critical, which is where the widely accepted three lines of defence model can help to institutionalise organisational roles and responsibilities. Boards should ensure that this is the case. Frameworks and controls are important, but they do need to be brought to life through testing and exercising. They should also be based on a threat-led approach to assessing cyber risk – where security planning and ultimately spend is proportionate to the unique threats that the company faces. A pragmatic view of cyber as a risk management issue will help, given it is never possible to protect everything. Boards and senior management teams should instead prioritise their most critical assets for protection and be ready to respond if the worst should happen.

Navetta: The first step in analysing risk is understanding its potential impact. According to reputable sources, the average material downtime arising out of a ransomware attack is about 23 days. As such, companies must begin by asking themselves: what would the impact to my organisation be if the company could not provide its goods and services, and satisfy its core mission for 23 days? From there they will gain an understanding of the seriousness of a ransomware attack, which will hopefully allow them to obtain the focus and resources needed to address the threat. Organisations focusing on reducing their risk should employ a holistic approach, including implementing some of the following measures. First, hardening of remote access points. To this day, many of the ransomware attacks we see come in using legitimate credentials at remote access points. Cut those off and risk is greatly reduced. MFA can also help, but it is not failproof. Second, more phishing training and prevention. Since threat actors are after credentials and often need to gather intelligence internally to obtain those credentials, many ransomware attacks start with phishing campaigns and email account access. Third, detect lateral movement. Since many threat actors use legitimate credentials, often with administration rights, to stage and launch their attacks, companies that can detect unusual 'lateral movement' by actors that look legitimate may be able to stop a ransomware attack before it starts. Fourth, system impact assessments. Companies should gain an understanding of the operational and financial impact of losing various systems, networks and data centres.

FW: Given that the chances of falling victim to a successful cyber attack are high, how should companies prepare in advance

to respond quickly and effectively to potential scenarios? What are the essential elements of the planning process?

Raventos: Identification, protection, detection, response and recovery are key elements in any planning process. We are seeing that active and intelligent monitoring is fast becoming the new tendency in detection. Security information and event management tools and security operations centre capabilities are very helpful for this, and the implementation of security orchestration, automation and response, with automatic and intelligent response, is becoming more relevant to this end. On the other hand, one should not lose sight of the importance of developing a comprehensive BCP, that involves all key departments, including legal, compliance, production plants and so on, and includes a deep business impact analysis with clearly defined recovery time objectives and recovery point objectives. Again, testing procedures with red and blue teams will help test your level of protection and resilience. Without this, all these recovery plans become immeasurable and irrelevant.

Hinnen: Every company should have a company-wide, multi-stakeholder incident response plan. Although they still have a critical role to play, incident response is no longer the exclusive province of the technical staff. Most incidents call for a response coordinated among legal, risk management, public relations, customer relations and human resources, and often third-party forensic, crisis communications and incident response services specialists. The incident response plan should spell out roles and responsibilities, address common issues, centralise incident response resources, explain whether and how incident response efforts will be supervised by counsel – and therefore privileged – provide for retention of third-party vendors and include default holding statements the company can use and modify in the event of an incident. Once a company has a plan, the company should exercise it regularly, identifying gaps and weaknesses, refining processes, and revisiting whether the plan is attuned to current threats. Effective incident response is a learned behaviour refined through consistent practice.

Gu: From my experience, we should pay more attention to early prevention and detection. In the early stage of the information security incident cycle, enterprises should establish a set of business continuity defence plans for the information security incident in advance, to support the stable and sustainable operation of the business at a specific time.

Owen: Testing crisis management plans against realistic scenarios relevant to the organisation is crucial. Depending on the company, this could be a supply chain compromise, an insider threat or a data leak extortion. Given how the regulatory environment is changing, it is also critical to understand what data sits where, so that compliance and legal teams can notify customers, regulators and third parties within appropriate time frames. Broader developments in security orchestration, automation and response solutions are starting to alleviate the burden on human responses to operational threats, including attacks such as ransomware. Advances in emerging technologies such as machine learning are helping to rapidly identify and contain many common attacks, but sound crisis readiness is still critical for senior leadership. In other words, such technology advances need to fit into an organisation-wide risk management approach – which is ultimately the best way to prepare for an effective response.

Navetta: Overall, events like Colonial Pipeline and additional Securities and Exchange Commission (SEC) guidance and enforcement have awakened boardrooms to data security issues. Many of the new initiatives we are seeing are being driven by the top. More boards are developing data security and privacy committees and expertise to be able to digest and understand these issues. They are pushing for more resources to address these risks. While motivations are always difficult to determine, I believe boards and senior management are more interested in cyber issues now because of ransomware. Board members do not need to understand the technology issues associated with such attacks, but they do understand the operational and financial impacts. Those impacts fall directly into their world, and they are charged with oversight of management to help mitigate the risk, and impacts, of cyber attacks. When analysing the risks associated with ransomware and similar attacks, acutely understand the various opportunities an organisation has to either prevent or disrupt an attack. Those opportunities do exist and taking advantage

> “THE APPETITE FOR CYBER INSURANCE HAS INCREASED SIGNIFICANTLY; UNFORTUNATELY, DUE TO THE RANSOMWARE EPIDEMIC, THE MARKET FOR CYBER INSURANCE HAS TIGHTENED UP AS WELL.”
>
> DAVID NAVETTA
> Cooley LLP

of them can mean the difference between a complete non-event and a catastrophic, business-ending loss.

Peachey: It is important to know your insurance carrier and how to report a claim. The same goes for knowing what vendors can assist you in the event of an incident, knowing if your insurance carrier has a panel of preapproved vendors to ensure you connect with the appropriate ones and knowing what internal personnel will run point on a matter. Also, make sure your internal team is practicing the IR plan throughout the year. This plan must be both a written policy and a practiced procedure. And again, know where your data is, how it is stored, and that you have protected copies that threat actors cannot reach.

> BROADER DEVELOPMENTS IN SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE SOLUTIONS ARE STARTING TO ALLEVIATE THE BURDEN ON HUMAN RESPONSES TO OPERATIONAL THREATS.
>
> JAMES OWEN
> Control Risks

John: As security threats become more daunting and many organisations remain in a remote work environment, global organisations must reach a state where their core operations and services will not be disrupted by unexpected global changes. This is where operational resilience comes in. Consider the risk and response for a utility company, for example an organisation that relies on internet of things (IoT) data, or a manufacturer of medical supplies. While their approach may differ, the impact would be equally as devastating should their operational continuity be halted. Operational resilience is critical to your ability to sustain your business operations in the event of any major event. In today's digital world, this must also include a cyber event. Operational resilience requires a strategic and holistic view of what could go wrong, and how an organisation will respond. The bottom line is that organisations must have the ability to operationally execute the processes through a combination of human efforts, technology products and services. The ability to do something as simple as restoring from recent backups will be tested in every ransomware attack, and many organisations will fail this test. Not because they are not backing up their systems, but because they have not tested the quality of their backup procedures or practiced for a cyber event.

Sanchez: First, organisations need to understand that cyber risk involves much more than 'cyber attack'. There are many ways in which organisations can be damaged by the misuse of data and digital systems, from simple user errors to exposure to vendor problems, aggregated supply-chain risk and cloud platform outages. Organisations must understand the universe of challenges they face and identify the correct stakeholders that need to be involved in dealing with these. Once an organisation has this basic understanding it can begin to plan how to react. Ideally, it will identify gaps in its own capabilities and resources and seek to supplement these by buying cyber insurance, retaining external vendors and so on.

FW: In what ways has the appetite for cyber insurance increased in recent years? How would you describe trends in the coverage, limitations and premiums on offer?

Navetta: The appetite for cyber insurance has increased significantly; unfortunately, due to the ransomware epidemic, the market for cyber insurance has tightened up as well. For perhaps 10 to 15 years, the cyber insurance market was very profitable and competitive, which led to lower premiums and expanded coverage. That has now completely flipped – premiums have increased, coverage has narrowed, and importantly cyber insurers are requiring their insureds to have more 'skin in the game'. For example, where previously cyber insurers would cover extortion payments from dollar one, now many carriers are requiring their insureds to pay a retention – often in the millions of dollars – before the carrier's extortion coverage is available. In addition, because of potential legal prohibition around paying a ransom – and specifically because ransomware groups, bitcoin wallets and individual hackers are being placed on the Office of Foreign Assets Control (OFAC) sanction list in the US – some carriers are balking at paying or reimbursing extortion demands.

Gu: Cyber insurance used to be considered a risk transfer method. As an effective enterprise cyber security risk management tool, cyber security insurance covers a wide range of losses, including not only the first-party expenses and economic losses caused by the insured due to cyber security events, such as data leakage and hacker attacks, but also the civil liability that the insured needs to bear to third parties arising from personal information obligations under law. So, the increase in cyber insurance purchases will continue. In China, I believe that cyber insurance brings more benefits for cyber security practitioners.

Peachey: Overall, uptake for insurance policies is on the rise. According to the US government's 'Accountability Office May 2021 Cyber Insurance Study', there was a 47 percent uptake in cyber insurance purchases in 2020 versus 26 percent from 2016 to 2019. The survey also revealed an increase in premiums of 30 to 50 percent. No doubt, the ransomware epidemic has contributed to this rise and limitations on policy offerings for ransom payments and associated IR costs. But while the frequency of attacks, coupled with million-dollar business-interruption losses and lingering third-party lawsuits in the past two years, did impact carrier profitability, the cyber market is still expected to see billion-dollar growth. Thus, carriers are not exiting the cyber game entirely. Rather, they are working to improve underwriting with data-driven decision making. Starting from the broad coverage offerings in the early 2000s, we are seeing expected pullbacks in terms of offering coverage altogether and restricting ransomware coverage – for example, co-insurance and sublimits for ransom payments and associated costs. And many underwriters are also requiring organisations to implement MFA and EDR solutions before they will consider extending a policy.

John: Managing risk is a critical business objective for all companies. Yet, even with the adoption of best-of-breed cyber security technologies and best practices, companies can face residual risk due to inconsistent management of apps and other productivity platforms exploited by a quickly evolving threat landscape. To bridge this gap, insurance providers have begun offering policies to help mitigate the impact of data breaches and ransomware attacks. This new area of insurance is growing rapidly, however uncertainty is common as insurers struggle to acquire and use the dynamic, real-time data needed to mitigate cyber risk, while growing threats like ransomware drive urgency. With this complexity, insurers are seeking increased visibility into each company's security environment and hygiene to better underwrite new policies. To address this, there are innovative data-driven cyber insurance products that allow customers to safely share security posture information through security platforms. In this way, all data and details about a covered company's technology environment will be owned and controlled entirely by that customer, but customers can opt-in to securely share them with providers to receive benefits like enhanced coverage and more competitive premiums. This model rewards customers with real savings when adopting cyber security best practices and gives insurers the information they need to proactively protect their customers against breaches.

Owen: A surge in cyber attacks over the last two years has increased the frequency and severity of cyber insurance claims, leading to higher premiums and stricter limits on coverage. Some insurers now require prospective insureds to implement stronger security controls before they are offered a policy; others are reducing the compensation for business interruption and data recovery losses or are suspending the writing of policies that refund the cost of ransom payments. Quantifying cyber risk is a notoriously complex exercise, given it involves modelling a constantly changing man-made peril where the identity and goals of the perpetrator are often obscure and where a contagion-style attack could lead to losses larger than the insurance industry itself. Demand for protection remains high, particularly among small and medium-sized companies keen to navigate tighter disclosure requirements and avoid fines. The question is whether this protection will come through cyber insurance in the future or via a different mechanism.

Sanchez: As organisations were forced to comply with lockdown restrictions at the beginning of the pandemic, they found themselves more exposed to a greater threat of disruption because they had inadvertently opened the door to cyber criminals who moved fast to exploit staff, processes and networks that were suddenly exposed beyond the corporate firewall through mandatory home working. This is a risk that is not going to go away; many organisations have said that hybrid and remote work are here to stay, and so the appetite and requirement for cyber insurance that protects against malicious attacks has naturally increased. It is important to not only cover organisations against these risks, but to help them prepare better so that they are not caught on the back foot as cyber criminals seek to exploit new working practices.

> "WE EXPECT AN INCREASE IN D&O CLAIMS LINKED TO CYBER ATTACKS IN THE COMING YEARS, AND UNDOUBTEDLY THERE WILL ALSO BE AN INCREASE IN THIRD-PARTY LITIGATION ARISING OUT OF CYBER EVENTS."
>
> RAF SANCHEZ
> Beazley

Hinnen: The appetite for cyber insurance has grown immeasurably, but the market is still immature. Most policies are still manuscript policies, as opposed to standard policies, meaning that each carrier drafts its own policy and, in many cases, several different versions of its policy. There is little consistency or predictability for consumers, and many of the policies contain pitfalls that can compromise a company's protection. It takes an expert to navigate this thicket, select an effective policy, and understand how it interacts with the company's other policies. For cyber, more than most of their policies, when it is time for renewal companies should work with their broker to get different bids from different insurers, assess them, and select a policy that meets their needs.

> ORGANISATIONS SHOULD KNOW WHAT DATA THEY ARE HOLDING, FOR HOW LONG AND WHERE. THEY SHOULD CHECK THAT IT IS SECURELY COPIED IN THREE DIFFERENT PLACES ACROSS THREE DIFFERENT MEDIA TYPES.
>
> LYNN PEACHEY
> Arete

Raventos: Directors and officers (D&Os) are now more aware of the importance of cyber security due to the high volume of cyber incidents affecting all sectors and types of company worldwide. In addition, chief information security officers (CISOs) and risk managers now work closely to document their risk appetite in more detail through formal cyber security frameworks. They assess risk avoidance, mitigation, transfer and acceptance. The transfer of cyber risk through cyber security insurance is now obviously on the rise. However, considering the high volume of claims – both in frequency and severity – faced by many of the big insurers, the cyber insurance market is also changing dramatically. In general, premiums are increasing and coverages are narrowing, such as the introduction of a sublimit for ransomware, however it does always depend on the level of maturity of the company. Insurers, brokers and clients should work together to achieve a good level of maturity for a win-win scenario.

FW: Could you outline the main risks that cyber issues pose to D&Os on a personal level? What measures should a company take to ensure that robust D&O liability cover addresses cyber security and data breaches?

Gu: D&O insurance is used to protect the potential personal liability risks faced by the company's directors, supervisors and senior managers when performing their management duties. The problems associated with cyber security and data leakage exacerbate the personal liability risks they may face. This risk is heightened by the potential penalties that may be imposed by local cyber security law and personal information protection law. At present, for such risks, enterprises should consider purchasing additional cyber security liability insurance to supplement their D&O provision.

Owen: Although D&O insurance was not specifically designed to protect D&Os in cyber incident scenarios, perceived personal liability from major breaches is making a clearer case for these products. Understanding how senior stakeholders make decisions during data breaches is already a key consideration during the loss-adjustment process. Boards are being targeted in litigation over cyber breaches, which is increasing scrutiny of important documentation such as crisis management minutes, forensic reporting and regulatory notifications, all of which will have been approved by senior D&Os within the business. Given this, we are starting to see D&O insurance become more appealing for some leaders as they look to limit their liability. This is increasing demand and premiums, with insurers making complex decisions as to which companies to insure. As with cyber insurance, questions related to the security and risk management culture of a company are increasingly critical to effective underwriting in this space.

John: For cyber insurance to play a meaningful role in overall risk management, buyers and sellers need the benefit of data and clear visibility into what is covered and factors either minimising or multiplying risk exposure. It is important for D&Os to understand the risk to their business, including any regulatory requirements that they may face and to ensure they have the appropriate level of protection for the risk of the data they handle.

Peachey: In the recent SolarWinds' securities litigation, shareholders are calling out D&Os for having knowledge of cyber security risks and not adequately responding. They allege the board failed to implement procedures to monitor cyber security risks – for example, by not requiring management to regularly report on risks, which ultimately contributed to the decline in share price. The trend seems to be moving away from blaming the CISO or head of IT, who have often begged for more funding and resources only to be told no, and instead, forcing cyber security

responsibility onto the highest levels of management and hitting companies where it hurts most: their pockets. Moving forward, companies should ensure that insurance policies specifically address these newer risks to D&Os rather than arguing silent cyber cover. They should also create an internal cyber security framework that places IT concerns, including the budget, at the forefront. Some risks may be unavoidable, for example human error-related cyber security events. But having a layered cyber security defence plan that highlights documentation and use of vulnerability patching, best-in-class technologies and workforce training will greatly assist in risk mitigation while also providing evidence of due diligence.

Sanchez: Many organisations think that they are resilient to cyber events, but our experience is that they are not. A large part of any cyber incident is the potential impact that it has on reputation, and it is difficult for organisations to pinpoint just how seismic the impact of a cyber attack will be until it happens. Taking the right steps can stop a small attack from becoming something so serious that you must notify all clients, employees and regulators about it. Once that happens, organisations face huge reputational risks. We expect an increase in D&O claims linked to cyber attacks in the coming years, and undoubtedly there will also be an increase in third-party litigation arising out of cyber events.

Hinnen: In the US, under the 1996 *Caremark* case, directors can be held personally liable for failing appropriately to monitor and supervise the business. To avoid liability, they must demonstrate diligence and good faith in dispatching their duties. In the cyber security context, that means they must be actively engaged in overseeing the company's cyber security programme. The topic should make a regular appearance on board meeting agendas. The board should leverage the resources, whether a member with a background in cyber security or an expert consultant, to understand the information they are receiving from the company, ask probing questions and hold company leadership accountable. They must pay attention to 'red flags' that suggest gaps or weaknesses in the programme, demand appropriate commitment and accountability, and follow up across meetings. In placing a D&O policy, companies should again work with their broker to evaluate a number of different policies and select the policy that best covers their risks.

Raventos: D&Os are facing many new responsibilities, including cyber risks. Until recently, D&O insurance policies did not specifically mention anything about cyber. As cyber risks become an increasing concern for D&Os, insurers are now introducing specific extensions and exclusions to these policies that are more or less restrictive depending on the jurisdictions and the company's level of cyber maturity. In my opinion, however, full disclosure of these risks, a clear cyber strategy, the appointment of cyber committees and the purchase of a standalone cyber security insurance policy are key to protecting D&Os from potential cyber liabilities.

Navetta: Ransomware attacks can impact the core mission of an organisation: to deliver goods and services and provide investors with a return on investment. The legal system in the US – both in terms of regulatory and litigation activity – is increasingly scrutinising whether D&Os meet their duty of care with respect to minimising this risk. D&O insurance is an important tool for protecting these individuals. The question becomes: how much coverage is adequate given the magnitude of the risk and impact? That is a question all boards should be asking, both around cyber insurance and D&O insurance.

FW: Looking ahead, how do you expect the cyber security landscape to evolve, in terms of its impact on companies? What major trends are on the horizon?

John: In cyber security, we quite often focus on negative trends. Therefore, I want to share some positive trends I am seeing, which includes transparency. We see both governments and companies coming forward and working together to combat cyber crime. They are also prioritising their focus on cyber security to address, prevent and respond to these attacks. New laws, task forces, resources and partnerships are increasing, and this is good news in my view.

Peachey: Major trends include threat actors mid-game hunting. This means they will target smaller fish versus those that would garner national attention to avoid potential government involvement or criminal prosecution. Now, that does not mean we expect ransomware to go away any time soon; rather, the tactics of threat actors will continue to shift around regulation and clients increasing security. The insurance 'hard market' will continue to drive insureds' pre-breach planning and willingness to spend on tools and training to gain better cyber security and more effective breach response in worst-case scenarios. Correspondingly, we expect to see carrier claim volumes continue to decline as underwriting controls tighten. Government guidance will also undoubtedly continue to impact organisations' response to ransomware – for example, advising against paying a ransom – and thus, increase the need for data recovery and restoration services along with client focus on preventative cyber security measures.

Sanchez: Unfortunately, the cyber criminal landscape will continue to develop because the techniques, tactics and procedures currently being implemented are so effective at generating excellent financial rewards. Attackers are 'reinvesting' their gains in new tooling, research and resources so that they are constantly able to stay several steps ahead of organisations' defensive efforts. There is also increasing specialisation so that certain groups concentrate on certain strategies, for example 'initial access brokers' specialise in selling access to networks that they have infiltrated, and this leads to those groups becoming very effective in their chosen area of operations. Despite the efforts of various

stakeholders in the risk management space, from private organisations to insurers, tech vendors and governments, ransomware will continue to be a trend that we do not see dissipating any time soon.

Hinnen: It is hard to imagine that the risks associated with cyber security will not continue to grow in coming years. We are living more of our lives, having more of our interactions and transacting more of our business online. We are incorporating IoT devices into our homes and office places. We are increasingly relying on industrial control systems and supervisory control and data acquisition systems to monitor and manage industrial processes. Globally, law enforcement mechanisms for combatting cyber crime remain weak and immature, with some jurisdictions harbouring cyber criminals, some looking the other way, and others without adequate resources and expertise to respond effectively. Companies will have no choice but to invest increasing resources – human, financial and technological – in securing their networks and their data. Governments, too, will have to invest in greater resources, and redouble their efforts to create international enforcement networks that can effectively reach bad actors in lawless countries and regions, safe havens and weak states. And governments and the private sector will increasingly have to work together to protect the network infrastructure with respect to which they have shared responsibility.

Raventos: The cyber security landscape is evolving very quickly, on both the hackers' side and in the insurance market's response. As such, we have seen an increase in the number of attacks on big multinational providers, which means that systemic risk and accumulation exposures are becoming major concerns for both companies and insurers. On the other hand, what we see in countries such as Germany is that big multinational companies prefer to have big deductibles or a major self-insured retention with the aim of insuring their catastrophic risk. In my opinion, we will see higher deductibles in the future as this ensures that responsibility falls both on companies and insurers. Again, companies, brokers and insurers will all have to work hand in hand.

Navetta: Most diligent companies adhere to the 'not if, but when' mode of thinking when it comes to security breaches and ensuing business impacts. These companies build out incident response plans to ensure readiness and resilience. They employ zero trust models that recognise that corporate networks are made up of and are interconnected with third-party networks and devices they do not control and require users – both inside and outside of the organisation – to be authenticated, authorised and continuously validated with respect to security across all environments. Companies now realise and act like they are under constant siege because they are. The key strategy now is to assume that significant breaches will happen, but to be ready and resilient so that those breaches do not become catastrophic.

Owen: The threat landscape is always expanding, shaped by the rapid adoption of technologies, including artificial intelligence, quantum computing and 5G, plus more straightforward applications of existing ones such as connected devices in the IoT, Industry 4.0. and cloud and edge computing. These technologies are driving huge leaps forward in innovation, such as enhancing the speed, precision and impact of operational defence. However, the same technologies are also being leveraged by attackers. And right now, this is particularly concerning for those companies that sit in the crosshairs between threat, geopolitics and critical supply chains, for example companies working in health, biotechnology, semiconductors, cloud services and critical national infrastructure. Ultimately, though, this is less a sectoral and geographical phenomenon and more a global and transformational moment in the way new and existing systems come together – cyber threats impact all companies and are only likely to become more disruptive and ultimately destructive.

Gu: With changing network technology and the emergence of new risks, the protection scope of cyber security insurance is also expanding. Now the protection scope has been expanded to 19 items, including the loss of business income caused by computer system failure, network blackmail and ransom payment, as well as social engineering crimes. Research carried out by Anda Insurance Agencies shows that the network risk consists of far more than external network attacks, and the proportion of employee-related events in claim cases is also significant. According to research carried out over the past 10 years, in terms of the main triggers of network risk events, hacker intrusion accounts for about 28 percent, human error accounts for about 20 percent, equipment loss and theft accounts for about 14 percent, and employee retaliation accounts for about 13 percent. From an industry perspective, medical, professional services, technology and retail industries face the highest risks. Meanwhile, two-thirds of the more than 6500 data breaches disclosed in 2018 came from the commercial sector. At the same time, government departments accounted for 13.9 percent, medical departments accounted for 13.4 percent and education departments accounted for 6.5 percent. Furthermore, there were 12 data breaches involving more than 100 million people or more, accounting for 74 percent of all attacks last year. In terms of the cost of network risk events, the nature and scale of cyber risk varies greatly from region to region, as does their prevalence. As far as China is concerned, I predict that the cost and number of cyber attacks will rise sharply. ■