CYBER SECURITY & RISK MANAGEMENT

ANNUAL REVIEW **2017**

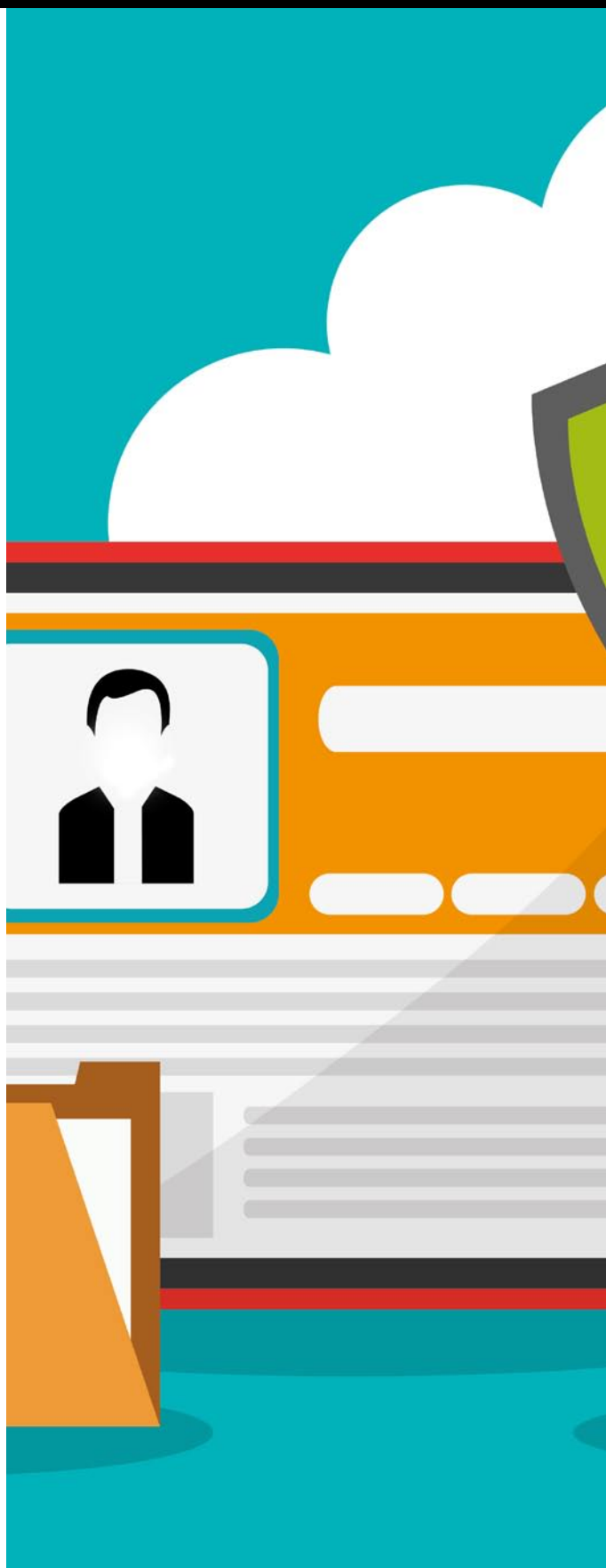
FINANCIER WORLDWIDE corporatefinanceintelligence

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 • June 2017
Cyber Security & Risk Management



CYBER SECURITY & RISK MANAGEMENT

JUNE 2017 • ANNUAL REVIEW

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

Contents

UNITED STATES 08
Shahryar Shaghaghi
BDO USA

CANADA 12
Ruth Promislow
BENNETT JONES

UNITED KINGDOM 16
Simon Calderbank
TOKIO MARINE HCC – UK

FRANCE 20
Xavier Marguinaud
TOKIO MARINE HCC – FRANCE

NETHERLANDS 24
Sandra Konings
BDO ADVISORY B.V.

NORWAY 28
Chris Culina
BDO NORWAY

PORTUGAL 32
Leonor Chastre
CUATRECASAS

GERMANY 36
Dr Jochen Lehmann
GÖRG

CYBER SECURITY & RISK MANAGEMENT

JUNE 2017 • ANNUAL REVIEW

Contents

ITALY 40
Alfredo Gallistru
PWC

TURKEY 44
Burç Yildirim
DELOITTE TURKEY

ISRAEL 48
Ophir Zilbiger
BDO CONSULTING GROUP

JAPAN 52
Takashi Nakazaki
ANDERSON MORI & TOMOTSUNE

AUSTRALIA 56
Leon Fouche
BDO AUSTRALIA LTD

NIGERIA 60
Joseph Tegbe
KPMG NIGERIA

SOUTH AFRICA 64
Graham Croock
BDO SOUTH AFRICA


F11
F12

INTRODUCTION

Cyber security is one of the biggest corporate issues of our time. As the 'WannaCry' ransomware attack in May ably demonstrated, organisations of any size, anywhere, are vulnerable to attack.

Though many companies have improved their cyber security defences in recent years, there is much more work to be done. Cyber criminals are becoming increasingly agile, sophisticated and specialised. It is up to companies to match the ambitions of cyber criminals and develop robust and resilient cyber risk management protocols and strategies.

When a breach has occurred, as it almost inevitably will, companies must ensure that they have the right response measures in place. Though they are by no means deterrents, incident response plans and cyber insurance policies are two important measures that companies should have in place. Cyber insurance can help organisations to mitigate the cost implications of a breach, and an incident response plan will enable it to get back on its feet as quickly as possible. A coordinated response plan will also facilitate better communication with regulators and customers.

Much like affected companies, legislators and regulatory bodies in jurisdictions across the world are responding to current cyber attack vectors. In the US, the New York Department of Financial Services (NYDFS) issued regulations governing cyber security in March 2017, imposing the broadest and most prescriptive cyber security requirements on financial institutions. In Europe, the General Data Protection Regulation will impose data breach notification and reporting requirements. Companies will have to move quickly to ensure they are compliant. Elsewhere, the introduction of the Australian Notifiable Data Breach scheme will require companies to proactively assess their cyber security provisions.

UNITED STATES

SHAHRYAR SHAGHAGHI
BDO USA

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN THE US?

SHAGHAGHI: As the 'WannaCry' cyber attacks proved, companies of any size, and in any industry, are potentially vulnerable. With more than 75,000 ransomware attacks in 153 countries, the world saw the wide scope and unpredictable consequences of a ransomware attack. The healthcare sector remains uniquely at risk to cyber incidents due to a variety of factors, including significant digital transformation in recent years, lack of focus and funding and resources to implement an effective cyber security risk management programme. Because many hospitals maintain and rely on end-of-life technologies, and may prioritise immediate access to data over data security, cyber criminals have found their systems easier to breach. The healthcare sector is also one of the most targeted sectors by cyber criminals and nation states because it is the only sector which combines highly valuable and sought-after bulk data sets of personal health information, personally identifiable information, payment information, medical research and intellectual property.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

SHAGHAGHI: Cyber security has certainly become a concern for most companies; however, except for those companies that are highly regulated, not enough focus and investment is given to cyber risk management and resilience, especially in terms of proactive mitigation strategies. Board members are starting to understand, as well as become more engaged and concerned about this area. The key is to make sure they obtain the right level of information so they can provide appropriate oversight and support for critical areas as it relates to their organisation's cyber security risk management.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN THE US? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

SHAGHAGHI: Cyber security and data privacy compliance, and requirements specific to certain industries, specifically healthcare and financial services, have evolved at both the state and federal levels, as well as globally. For example, the New York Department of Financial Services (NYDFS) issued the first-in-nation state regulation on cyber security in March 2017, imposing the broadest and most prescriptive cyber security requirements on financial institutions, including insurance companies, which operate in New York State – regardless of where the organisation is headquartered. The General Data Protection Regulation (GDPR) is an example of a regulation with a global reach as this EU regulation requires any company in the US that processes EU citizens' transactions to achieve compliance.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

SHAGHAGHI: There is no one step or simple solution to avoid cyber breaches. However, various key functions, at different levels of maturity, need to be implemented by organisations using a risk-based approach. Threat intelligence and early detection, ongoing monitoring, data protection, access control, and fully vetted incident response plans are examples of some of the most critical components.

UNITED STATES • SHAHRYAR SHAGHAGHI • BDO USA

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

SHAGHAGHI: The key in responding to a breach is to control and minimise the impact of that breach. The execution of an incident response plan, which includes engagement of various functions within the organisation, including outside counsel, IT, risk management, corporate communications, HR, compliance, general counsel and, at times, business heads, is critical. Actions such as breach notifications based on local and global requirements, engagement of an external forensics investigation team and immediate and effective 'restore and recovery' of critical infrastructure and data are some examples of actions taken during or post-breach.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

SHAGHAGHI: Cyber insurance can provide much-needed tactical and financial support for companies confronted with a cyber incident. Generally speaking, a cyber policy's first-party coverage applies to costs incurred by the insured when responding to a covered cyber event, while third-party coverage responds to claims and demands against the insured arising from a covered incident. A well-tailored cyber insurance policy can go a long way toward mitigating the financial and reputational fallout of a cyber security incident. As more and more responsibility for cyber incidents is being placed on the shoulders of corporate directors, companies also should make sure that they have adequate levels of directors and officers (D&O) insurance to respond to claims levied against directors and senior management. Those claims are expected to increase in light of new regulatory requirements, requiring senior management to certify compliance with cyber security regulations. Care should be taken to make sure that the D&O insurance policy dovetails well with the company's cyber insurance policy. Lastly, it is crucial to understand the cyber insurance coverage of third-party vendors. In the event of the breach of a third-party vendor, will your data be covered by their policy? There are many considerations to take into account.

"Cyber insurance can provide much-needed tactical and financial support for companies confronted with a cyber incident."

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN THE US OVER THE COMING YEARS?

SHAGHAGHI: Cyber crime will continue to be part of our lives for the foreseeable future due to the transformation of the digital age, both at a personal level, as well as with respect to corporate operations. As the digital age evolves, so does the way we use products and services. We need to view cyber security risk management differently than traditional approaches and start incorporating it into our requirements and initial design of our products and services, rather than tacking it on once you are already down a path – this will help with usability, cost and sustainability of solutions.

www.bdo.com

Shahryar Shaghaghi

BDO Consulting, Technology Advisory Services National Leader and Head of International BDO Cybersecurity
BDO
+1 (212) 885 8453
sshaghaghi@bdo.com

Shahryar Shaghaghi leads the firm's technology advisory services practice and is head of BDO International Cybersecurity, having more than 25 years of experience providing information technology, operations and risk management consulting services to global organisations. He led one of the largest and most complex global cyber security implementations in the world at Citigroup, and is a recognised thought leader on cyber security.

CANADA

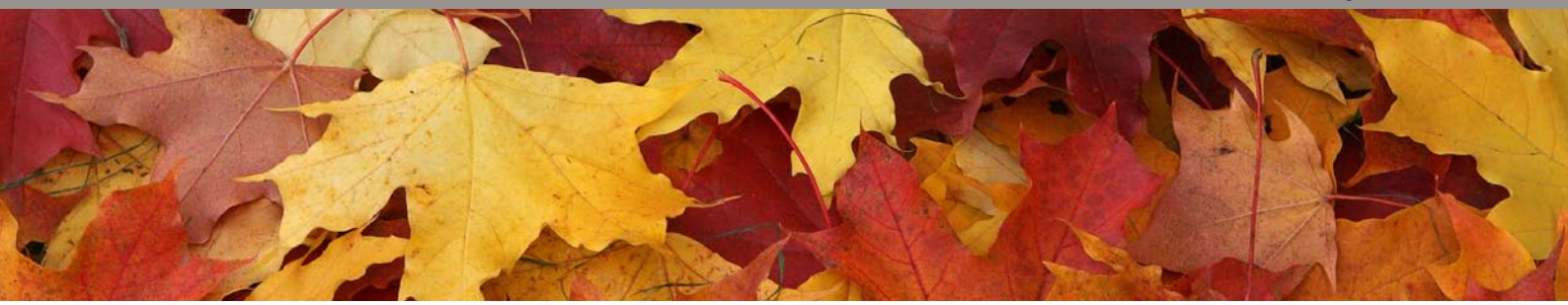
RUTH PROMISLOW
BENNETT JONES

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN CANADA?

PROMISLOW: Employee error continues to play a central role in the cyber threats facing companies today. A company's cyber security posture is only as strong as its weakest link, which threat actors will exploit. Unwitting employees clicking on malicious links or providing personal information through phishing or pretexting gives threat actors a way in. Employee error is typically linked to ransomware, which is emerging as one of the largest cyber threats facing companies today. The recent wave of ransomware attack making its way across Europe and other parts of the world – 'WannaCry' – has yet to hit Canada. But we could be only one 'click' away, by an unwitting employee, from this powerful attack. Employee error is also often linked to hacking and the use of malware by criminal actors seeking financial gain as stolen or weak passwords play a role in these cyber attacks. Educating employees on cyber threats is a critical component to a company's cyber security strategy.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

PROMISLOW: Despite the prominent media coverage regarding cyber attacks, many companies continue to operate with a false sense of security because no cyber threat against them has come to their attention. Companies may unknowingly be under attack, possibly due to their weak detection systems or the sophisticated nature of a silent attack. Furthermore, the absence of an attack to date does not necessarily indicate a lack of exposure to such risks, particularly given the increasing sophistication and proliferation of attacks. Given the constantly evolving and expanding landscape of cyber threats, and the potentially devastating impact of cyber attacks, companies should make cyber security a top business priority and plan accordingly. Board members should have a working knowledge of cyber security issues. They are expected to make decisions based on a sound appreciation of their company's cyber security posture. They are also expected to know what questions to ask management and the IT security team, and



to ensure their company has a data security plan in place to remedy any potential deficiencies, monitor the company's system for potential attacks and respond to a cyber incident.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN CANADA? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

PROMISLOW: Amendments in 2015 to the Personal Information Protection and Electronic Documents Act, which are not yet in force, will require organisations to notify individuals and other organisations of breaches that create a "real risk of significant harm" and report such breaches to the privacy commissioner. Under these amendments, companies that fail to report a breach to the privacy commissioner or fail to notify individuals as required, could face fines of up to $100,000 per breach. Currently in Canada, companies only have a reporting obligation in the province of Alberta. The pending reporting obligations will likely affect how companies manage cyber attacks, not only for fear of a $100,000 fine, which is not all that intimidating for larger companies, but also because a plaintiff seeking damages against the company in a civil claim would likely rely on a regulatory penalty as evidence in support of the claim.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

PROMISLOW: There is no 'one size fits all' when it comes to cyber security. Companies must implement a tailored plan to address the specific exposure they face. This requires companies to engage in risk and vulnerability assessments. More specifically, companies should identify the assets to be protected, such as customer information, employee information and confidential proprietary information; the risks to which they are subject, for example, unwitting employees clicking on a malicious link, disgruntled employees installing malware onto the system and outside hackers leveraging weaknesses in the systems; vulnerabilities, such as an unnecessary level of employee

"Cyber attacks are inevitable but liability does not have to be."

access to confidential information, absence of dual authentication process for remote employee log-in, lack of trained staff to monitor sites or third-party access to the system; and the landscape of risk arising from a breach in the various jurisdictions to which they may be subject. Cyber attacks are inevitable but liability does not have to be. Taking reasonable steps to prevent attacks will mitigate companies' exposure to cyber breaches.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

PROMISLOW: To contain the damage and mitigate the exposure from a cyber attack, companies should retain legal counsel, assess the nature and scope of the incident through an expert, determine regulatory reporting and notification requirements in applicable jurisdictions, contact law enforcement, ensure that internal correspondence regarding the incident is marked 'privileged' and that discussion regarding the matter is limited to those who need to know, engage the board of directors regarding details of the incident and the proposed action plan and determine if the incident has exposed risks or vulnerabilities that were not previously addressed, and implement a revised cyber protection plan accordingly.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

PROMISLOW: Cyber insurance can be an effective way of protecting companies and their directors and officers against some aspects of incident exposure. However, insurance is only as effective as the scope of coverage obtained. Just as with a cyber security plan, there is no one size fits all when it comes to cyber insurance. Companies must determine the required scope of coverage, which involves an assessment of the critical assets to be protected, the risks to which the company is subject and the company's vulnerabilities. A risk and vulnerability assessment may highlight, for example, that a company has particular exposure based on the security of its third-party service provider. While companies can delegate certain tasks to third parties, such as processing customer payments, they cannot delegate responsibility for the security of customer information. Therefore, ensuring that this provider has adequate cyber insurance coverage may be central

to protecting against risk of exposure. Defining the scope of required coverage through a risk and vulnerability assessment is critical to mitigate a company's exposure. Engaging in this risk and vulnerability assessment is also invaluable for directors and officers as it serves to fulfil their obligations of understanding the company's cyber security posture and arms them with the tools to direct how resources should be allocated in the company's prevention plan.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN CANADA OVER THE COMING YEARS?

PROMISLOW: Predictions for Canada include an increase in high profile attacks, the emergence of new threats and cyber breach techniques, a surge of class action claims against companies resulting from a cyber incident, the expansion of regulatory enforcement, an increased reliance on cyber risk information sharing among organisations and a heightened focus in corporate transactions on relevant cyber provisions.

Bennett Jones

www.bennettjones.com

Ruth Promislow

Partner
Bennett Jones
+1 (416) 777 4688
promislowr@bennettjones.com

Ruth Promislow practises commercial litigation with a strong focus on commercial crime, including cyber security, investment fraud, employee fraud and anti-money laundering. Ms Promislow focuses on cannabis-related litigation and has extensive experience with cyber security matters including cyber preparedness, incident response and related litigation. She also has extensive experience with recovery issues relating to commercial crime, including tracing, freezing and recovering proceeds of crime, as well as overseeing and conducting internal investigations for clients, working with internal and external auditors.

UNITED KINGDOM

SIMON CALDERBANK
TOKIO MARINE HCC – UK

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN THE UK?

CALDERBANK: The major cyber threat remains understanding the exposures and consequences a company could face when an incident occurs. Outside of $1bn turnover companies, there is still little work being done to understand the implications, financial or otherwise, of a cyber incident. As a result, there is often a lack of planning or strategy to rectify an issue when it occurs. This can allow small incidents to be inflated quickly, resulting in significant cost. This also manifests itself in insufficient employee training and knowledge about how their actions can impact the company – whether that be opening links in emails from unknown sources, inserting a random USB stick into systems, or other. This explains the growth in ransomware – where the volume of cyber incidents currently sits – and increased costs. Being well trained on how to communicate with the press when an issue occurs is also important as this can cause a huge difference in both the short and long term impact of an incident. Finally, it goes without saying that all IT systems and software must be up-to-date at all times, to avoid falling prey to ransomware attacks, such as the recent WannaCry.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

CALDERBANK: The situation is definitely improving, but it is still a long way from sufficient. Below the $1bn revenue bracket there still seems to be the general misconception that 'it will not happen to me' or 'only big companies are targeted'. So, smaller and mid-size companies remain quite exposed. That said, cyber security and protection are only part of the cyber conundrum. As we have seen, it does not matter how much is spent on security. When attackers want to get in, they will, and human error can always play a part in that. So, we must not forget that culture and the general approach within a company are as important as technological security. So it must be led and dealt with seriously by the board.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN THE UK? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

CALDERBANK: Regulatory change has been very slow over the last 10 years or so. However, it is on the horizon now. 25 May 2018 will see the General Data Protection Regulation (GDPR) come into action and for the first time there will be standardisation across Europe. The changes are far-reaching but one of the key areas is notification. Namely, the gap between how the US and Europe deal with notification will be narrowed by the new regulation. We believe this will change the way companies think about cyber security and data privacy, and will lead to more companies looking to transfer risk to insurers.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

CALDERBANK: In reality, it is not possible to stop a cyber breach. From my perspective, as an underwriter of cyber risk, I look to work with companies that have an understanding of their exposure and have implemented reasonable protection measures to slow and deter hackers. Every company faces different risks, so what is reasonable for a small manufacturing company would not be reasonable for a bank. Educating and rewarding staff so that they feel they are responsible and part of the overall security of the firm can help. For internal sources, the focus should be on data accessibility, well-designed processes, education and tight policies. Examples of appropriate measures include disabling USB port access for those who do not need it, allowing access to only the systems and data necessary for each function and removing all access to systems and data immediately when staff leave the company.

"Cyber policies should provide access to the best experts when they are needed and provide further assistance, such as upfront training and support to help understand the exposures faced."

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

CALDERBANK: The first thing is to call in the experts. If the firm has a cyber insurance policy, access to these experts should be granted when notifying the insurer of the issue. The first experts needed are forensics who investigate what has happened and who will stop any further data from escaping. Legal support will also be needed to advise what has to be done around notification and what can be done to minimise any legal repercussions following the event. With the introduction of GDPR on the horizon, there are a number of legal requirements that all companies will now have to comply with, for example, notifying regulators within 72 hours.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

CALDERBANK: One of the big issues is the unknown. Regardless of what an insured spends on security, they are still vulnerable; indeed, no company is 100 percent secure. Once the adequate security for the insureds' exposure is in place, cyber insurance can remove some of the unknown and provide access to those who do know – the response providers and forensic firms. These policies should not be seen as mere indemnity when something goes wrong, as other insurance policies are. Cyber policies should provide access to the best experts when they are needed and provide further assistance, such as upfront training and support to help understand the exposures faced.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN THE UK OVER THE COMING YEARS?

CALDERBANK: The amount of cyber crime will grow, defences will be tested more often and the complexity of attacks will increase. From an insurance perspective, we have only just started. Interest has been growing in the UK and across Europe generally for the last five years or so. Those who have purchased in the past and understand their exposures are starting to purchase more cover. Policies with €100m and €200m indemnity levels are now becoming common practice for larger clients and this looks set to increase and continue. GDPR will also have an impact. Notification costs alone will cause financial problems which some companies will not be able to overcome, pushing the demand for cover even more. This will also increase cyber insurance pricing – perhaps not immediately, but in the long term when claims start to bite.

TOKIO MARINE HCC

www.tmhcc.com

Simon Calderbank

Senior Underwriter - Cyber
Tokio Marine HCC
+44 (0)20 7680 2910
scalderbank@tmhcc.com

Simon Calderbank is a CII-qualified professional with over 13 years' experience in London and regional insurance markets. He started his career at Hiscox, where he wrote professional indemnity, financial lines and commercial risks. Subsequently, he focused on technology and cyber risks at CNA and QBE, where he was senior technology and cyber underwriter. A frequent speaker at industry and client sponsored events, Mr Calderbank's knowledge and underwriting expertise range from very small to London Market multinational risks. He holds a degree in Business Studies from University of Portsmouth.

FRANCE

XAVIER MARGUINAUD
TOKIO MARINE HCC – FRANCE

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN FRANCE

MARGUINAUD: Companies can be their own worst enemies when it comes to vulnerability. One of the major threats companies face is when they underestimate their cyber exposure and do not delve deeply enough into the solutions they should implement. It is common to think 'it will not happen to us, we are not interesting enough for hackers' and to invest massively in technological solutions without taking into account the key role that employees play in strengthening – or weakening – cyber resilience. Data theft and extortion, through the use of ransomware, is clearly increasing worldwide, as we have seen with the recent WannaCry attack that infected more than 250,000 computers in more than 90 countries and disrupted core systems of major entities such as the National Health Service in the UK and Telefónica in Spain. In France, in addition to organised crime dedicated to cyber extortion, industrial espionage also remains at the top of the cyber threat list. Since 2015, following the TV5Monde network interruption, one could also say that nation state actions are seemingly on the rise.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

MARGUINAUD: France is one of the most cyber educated countries in Europe. Among the CAC 40, it seems that about 80 percent of listed companies are transferring the risk to insurers. Overall awareness is improving considerably, from small and medium enterprises to upper and mid-market companies. This is due to media coverage, claims experience and campaigns carried out by IT and cyber experts, as well as the insurance industry. Of course, there is still room for improvement, particularly regarding risk governance. One of the main challenges has always been, and still is, bringing all company stakeholders together to discuss cyber risks and efficient solutions. It is fair to say that most French companies could be more proactive in their thinking as far as cyber risk is concerned.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN FRANCE? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

MARGUINAUD: The latest data privacy regulations in France have led the largest companies in the country, mainly CAC 40 and SBF 120, to start considering cyber threats. Previous legislations have highlighted the risk and the potential consequences. With the imminent obligatory application of the General Data Protection Regulation (GDPR), there is no more time for companies to overthink what they want or need to do as they will have to comply. This 'pressure' will push companies to take cyber risk even more seriously and to prepare for potential incidents. 25 May 2018 is a key date, which is expected to trigger many changes in Europe.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

MARGUINAUD: A cyber incident is no longer a matter of 'if' but 'when'. A company can take all possible measures to prevent attacks, but if someone wants to hurt or enter their systems, it will be almost impossible to stop them. Some things can be done to make a cyber criminal's jobs more difficult, however. The first step is that it is vital to know what the company should be protecting. Therefore, data identification and classification is the first step of a good cyber risk management strategy. Thereafter, appropriate processes should be set up and the most efficient technology-based solutions deployed. These solutions should be bespoke, however, as one solution does not fit all. The human factor is crucial to a company's strategy – people should be trained and educated, as they are the first line of defence for any company. The main component of any efficient strategy is readiness. Being cyber resilient means that a company is able to recover quickly from a cyber incident, that is why defining a business continuity plan and emergency response plan, establishing a dedicated team, as well as training and testing them, is crucial.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

MARGUINAUD: The first step is to contact the appropriate experts to contain the incident. The first 72 hours are vital when facing a cyber event, so the cyber incident protocol should be activated as quickly as possible. Thereafter, time should be taken to understand the situation – what has happened and the consequences of the event – and to make sure the company is complying at all times with any relevant mandatory requirements in whichever countries it operates. After that, in some cases, it is time to communicate with the customers, so a clear line of communication must be defined and held. After the event, it is inadvisable to try to hide facts. Instead, feedback and lessons learnt should be shared, as it is the best way to regain trust from the community and turn the prejudicial cyber incident into something positive.

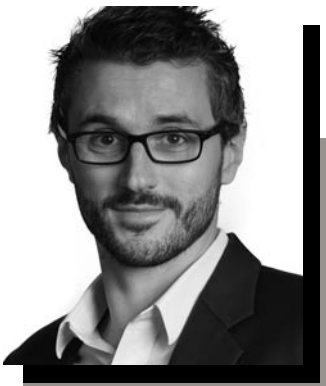
Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

MARGUINAUD: In addition to the common risk transfer component of any cyber policy, companies should be looking for assistance. Directors and officers (D&Os) need to access cyber experts who will handle the most stressful situation of their life in real time, without waiting for any deductible to be exhausted. These experts could manage any potential situations directly or support the company's IT department by sharing their expertise and providing guidance on practical matters. Some insurers also have a proactive approach and offer preventive education and training services or help the company monitor potential breaches around their staff data by screening the dark web.

"The first 72 hours are vital when facing a cyber event, so the cyber incident protocol should be activated as quickly as possible."

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN FRANCE OVER THE COMING YEARS?

MARGUINAUD: What we have seen until now is only the beginning. The volume of cyber crime will grow, attacks will gain in complexity and the consequences of these attacks will be more harmful. Cyber risks no longer represent a static threat; they are constantly evolving, which makes them very difficult to anticipate. The growing penetration of, and dependency on, the internet, along with new trends such as the IoT, is changing the ways in which we do business and, at the same time, widening the area of opportunity for hackers to attack.



TOKIO MARINE HCC

www.tmhcc.com

Xavier Marguinaud

Underwriting Manager – Cyber
Tokio Marine HCC
+34 93 530 7439
xmarguinaud@tmhcc.com

Xavier Marguinaud oversees and coordinates Tokio Marine HCC's cyber strategy for EMEA, APAC and LATAM. Previously, he worked at Marsh as NZ cyber risk specialty head and as financial lines senior risk advisor as well as cyber product champion in France. He launched his career in the Risk and Insurance department of Publicis Groupe.

NETHERLANDS

SANDRA KONINGS
BDO ADVISORY B.V.

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN NETHERLANDS?

KONINGS: We should only be worried about the cyber threats to which companies are vulnerable and which have a negative impact on companies, such as the loss of production and service time or loss of sensitive data. The recent WannaCry attack in Europe showed that many companies are vulnerable to ransomware attacks using zero-day vulnerabilities in hardware or software, even when the patches have been available for weeks. This is a pattern we have seen for years. Even when sophisticated or state sponsored hackers attack companies to gain intellectual property, the first point of entering the system is usually a well-known and unpatched vulnerability.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

KONINGS: Board members are asking more questions about the cyber security status of their company. I would recommend not treating this as a one-off question, but to include cyber attack risks within the overall risk landscape of the company. My first recommendation is not to spend a fixed amount of the ICT budget on cyber security because benchmarks show this is the new standard, but look at your company's risk landscape and define which measures are needed to end up with an acceptable risk. Make sure you review this on regular basis, once or twice a year for instance, since cyber attack risks change rapidly. What is acceptable today might turn into a high risk in six to 12 months. My second recommendation is to include cyber risk management in all business processes, especially in sourcing, human resourcing, on-boarding, off-boarding and through-boarding, and customer relationship management. Stop focusing on this problem as a pure ICT problem. It is a risk to be dealt with by several stakeholders within the company and the solution should be implemented both within ICT as outside ICT.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN NETHERLANDS? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

KONINGS: Regarding data privacy, for years we have had to comply with the Dutch Protection of Personal Data Act. As of 1 January 2016, this law has been extended to include the Data Breach Notification Obligation, meaning companies have to report a possible breach of personal data to the Dutch Data Protection Authority (DPA) within 72 hours after discovery. If this breach has an impact on the persons involved, these persons should be notified also. This Dutch law is the first step in the implementation of the upcoming European General Data Protection Regulation (GDPR) to which all companies processing personal data need to comply as of May 2018. Because of possible reputational damage, media attention and potential fines, in 2016 and 2017 many companies began to analyse what is required of them, whether they already take sufficient measures or what can be improved. Also in May 2018, we expect in Europe the implementation of the NIS Directive, the European directive relating to the security of network and information systems. This directive has been in force since 2016 and must be changed into local law by May 2018 by all EU member states. The NIS Directive states that sectors identified by member states as 'operators of essential services' will have to take appropriate security measures and notify serious incidents to the relevant national authority. Also, key digital service providers, including search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the new directive. So far I have seen no company in our region begin the process of implementing this regulation. I expect this is because it is not clear yet which companies will be 'operators of essential services' and this will differ between member states.

"I expect to see an increase in the number of cyber attacks on office automation using zero-day vulnerabilities."

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

KONINGS: It is impossible to avoid cyber breaches. In my view a company should take eight steps to become resilient to cyber attacks: keep up-to-date with security patches to remove zero-day vulnerabilities as soon as possible; install proper detection mechanism and processes to detect a breach as soon as possible to limit the impact; know your crown jewels, your core data and make sure this data is well protected; implement proper internal controls in your processes, like for-eyes-principle; teach your employees how attackers work and how an attack can be recognised; not only protect your own company but focus also on your supply chain – if your security is up-to-date but your supplier cannot deliver due to a cyber attack, you still have a disruptive process; fight the cyber enemy together and share cyber security knowledge and best-practices with peer companies; and discuss cyber security risks in the boardroom like you would any other company risk.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

KONINGS: Firms should be able to detect the event soon after it happened and should attempt to contain the issue by locking off the infected part of the system to prevent a further spread. Firms should have a press message available at all times, so it can be used whenever something happens and journalists begin to ask questions. In case of loss of privacy data, firms should follow their data breach notification procedures and report it to the DPA within 72 hours after discovery. In case of loss of personal data which might have an impact on the involved persons, firms should inform the persons as soon as possible.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

KONINGS: Insurance might be a good idea for risks with a high impact and low likelihood of occurrence, or for risks which are impossible or too expensive to mitigate. For other risks, I would recommend investing in the eight steps to become resilient to cyber attacks.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN NETHERLANDS OVER THE COMING YEARS?

KONINGS: I expect to see an increase in the number of cyber attacks on office automation using zero-day vulnerabilities. I also expect that these attacks will become more sophisticated and be mainly for financial benefit. In addition, I expect an increase in attacks on industrial automation. The sole reason for this is that countries write viruses to attack industrial environments. These viruses may then accidentally affect those companies which are vulnerable to these viruses. Also, I expect an increase in state-sponsored espionage focusing on research-based companies and their suppliers. Finally, we may well see an increase in cyber attacks between countries, since all European countries are increasing their cyber defence teams. Strengthened data privacy regulations have alarmed the press and we are likely to see an increase in the number of data breaches being reported, leading to companies potentially suffering reputational damage.

www.bdo.nl

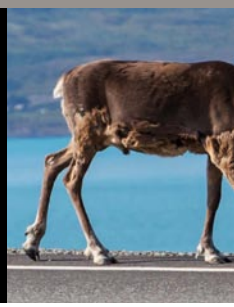
Sandra Konings

Partner Advisory – Cybersecurity Practice Leader
BDO Advisory B.V.
+31 (0)6 5150 8151
sandra.konings@bdo.nl

Sandra Konings has over 22 years of international experience in cyber security, data protection, security governance and ICT management, including 14 years as the chief security officer of large multinational companies. As well as having a practice that supports large and medium enterprises with data protection programmes, she also advises executive management on security risk management. Ms Konings co-founded and runs the cyber security information exchange with enterprises in the high-tech innovation industry in the Netherlands. This public-private partnership co-operates with the Ministries of Internal Affairs and Economic Affairs.

NORWAY

CHRIS CULINA
BDO NORWAY

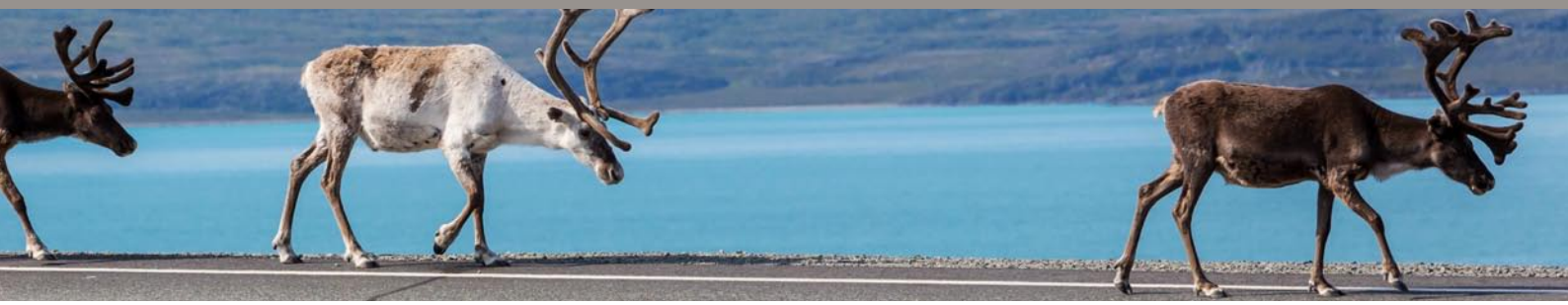


Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN NORWAY?

CULINA: You can never know or choose which threat actor you will be exposed to – the threat actor will make that choice for you. The number of incidents involving threats like ransomware and CEO fraud over the past year tells us that many companies are vulnerable to general threats. Sadly, if you are vulnerable to those threats, you are vulnerable to everything. We have recently seen targeted attacks from nation state actors and widespread ransomware campaigns. I would not say one is worse than the other. Both can seriously harm a company's ability to carry on with its business.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

CULINA: Clearly, companies are not placing enough importance on cyber security. That being said, there is a big difference between the professionals and the amateurs, and this is often linked to which sector your business operates in. We are even seeing huge differences within the same line or sector of business. Our experience is that a serious incident must occur within a company before management is able to identify the risk and take it seriously. In the last couple of years, there has been an increasing focus on cyber attacks in the media. This raises awareness among companies. However, awareness is worth very little if you do not understand threats and vulnerabilities.



Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN NORWAY? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

CULINA: Cyber security and data privacy is high on the agenda in Norway these days. Both national and regional regulations have been updated. EU regulations such as the GDPR and the NIS directive will both soon be incorporated into Norwegian law. The GDPR means that both private and public companies have work to do when it comes to data protection compliance. For a lot of companies, this means first time investments into information security management systems and modern solutions for detecting, preventing and handling cyber threats. The NIS directive defines a certain level of IT security on a national level.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

CULINA: Every company, public or private, should have a risk based approach to IT security, and should handle cyber risk in a planned and balanced way. Unfortunately, there is no silver bullet when it comes to cyber threats. Every organisation needs a combination of a good security baseline, such as a firewall, antivirus protection, secure configuration and timely software updates, and security measures that enable monitoring and threat hunting. The baseline picks off the low-hanging fruit, so that you can focus on more serious threats. Monitoring lets you put up a safety net for detecting the threats that passed under your baseline's radar, and gives you the visibility you need when a breach occurs. It is the foundation for what we call intelligence-driven computer network defence, which entails actively gathering and using intelligence for hunting down threats in your networks. Regular vulnerability scanning and penetration testing of your own systems lets you find and fix vulnerabilities before the threat actors do. In addition, you need to have a good information security management system that ensures management's involvement and continued improvement of your security work. It is important to understand that the risk ownership and ultimate responsibility lies with the board and senior management, regardless of the security organisation.

"Companies with high value information assets will continue to be subject to targeted attacks and digital espionage."

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

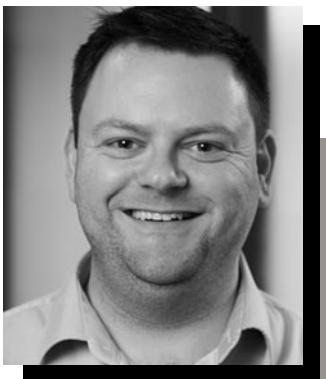
CULINA: Ideally, the company will have an emergency plan that is implemented prior to the incident. This plan will dictate how they should react to a cyber attack. Most companies would probably need to involve security professionals to help them understand the attack, limit the damage and return to normal operation. If you do not have an emergency plan and lack sensible risk analyses, you are likely to take the blame. Playing with open cards and taking action shows your partners and customers that you have learned something.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

CULINA: This is much debated. In the professional CERT community, we are not certain if it is possible to insure yourself from the damage of a cyber attack because it is almost impossible to put a price on the damage that is inflicted on the organisation that has been attacked. The real damage might not be apparent for a long time. Arguably, however, the kind of risk we are talking about here cannot be transferred to a third party. If you leak sensitive customer data or R&D that was meant to ensure your competitive edge for the next 10 years, having someone pick up the cleanup crew's bill is not going to make a very big difference.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN NORWAY OVER THE COMING YEARS?

CULINA: Different kinds of ransomware and fraud will continue to be highly relevant threats and will cost businesses a lot of time and money. In addition, we believe that companies with high value information assets will continue to be subject to targeted attacks and digital espionage. The rapid growth in cloud services and Internet of Things (IoT) devices will attract the attention of threat actors. Nation states will continue to develop their offensive cyber capabilities, and use them to exert pressure in international conflicts. As a society, we have a lot to learn about cyber security, and we have to learn fast.



www.bdo.no

Chris Culina

Senior Manager
BDO - Norway
+47 968 77 000
chris.culina@bdo.no

Chris Culina leads BDO CERT. He has experience from operational security at the Norwegian National Security Authority (NSM) and the Norwegian Health Network (NHN), devops at the University of Oslo, as well as several other sectors. His security related work has included leading incident response, intelligence and technical and tactical analysis related to targeted attacks and digital espionage.

PORTUGAL

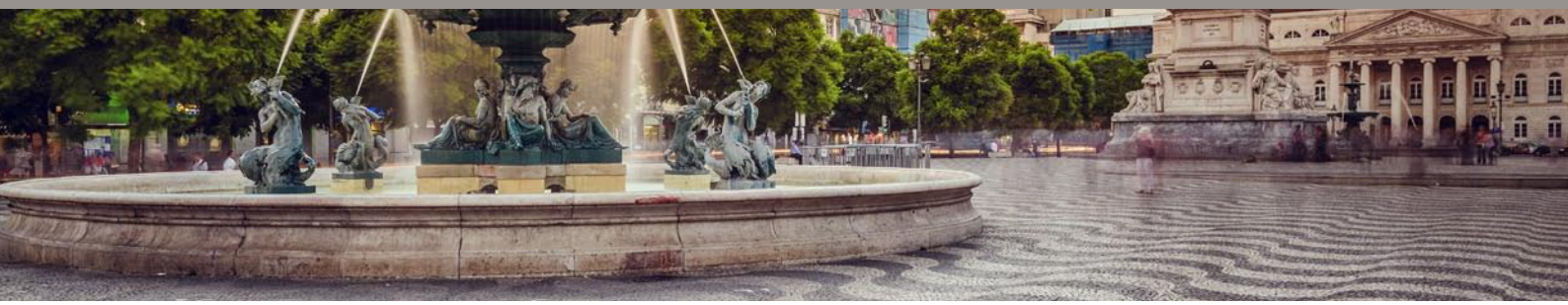
LEONOR CHASTRE
CUATRECASAS

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN PORTUGAL?

CHASTRE: Cyber attacks are an escalating and increasingly sophisticated threat. These attacks are evolving, spinning off new variants and extending their scope. First, companies should be aware that most cyber attacks, whether malicious or not, do not come from external agents but from insiders. Then, the new technologies behind digital transformation for businesses that are changing the way we work inevitably pose new threats. That is the case with enterprise mobility: as the use of enterprise connected personal and mobile devices becomes ubiquitous, new security risks that represent back door opportunities for cyber criminals arise. The use of cloud computing services also brings increased risks for companies, such as the proper selection of the type of data transferred to the cloud and the clear definition between the owner of the information and the cloud provider of the security measures that each one is responsible for putting in place. Then again, if 2016 had already been considered the year of ransomware, the recent 'WannaCry' attack is a stark reminder of the wide reaching impacts of cyber threats, which will certainly make cyber security a top priority for executives. The 'WannaCry' attack was certainly felt in several institutions in our region.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

CHASTRE: Given the escalating cyber threats that companies face and their wide reaching impacts, cyber security is increasingly being taken more seriously by directors. From an internal perspective, companies are investing and strengthening their IT departments in order to enhance their best practices and procedures. But companies, regardless of their size, are also seeking external support from cyber security specialists, in order to get a thorough assessment of their systems' vulnerabilities. So-called 'white hat hackers' play a vital role, detecting weaknesses and improving security measures before malicious hackers can find and exploit them.



However, it is crucial that cyber security is not perceived exclusively as an IT issue. In fact, to tackle this problem, a multidisciplinary approach is required, involving business strategies, operations and technology. And there is still much to be done. Board members must consider cyber risk issues, and, in tandem with experts in the field, assess cyber risk, manage it and devise a breach contingency plan.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED PORTUGAL? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

CHASTRE: The legal framework regarding cyber security and data privacy has changed substantially with the adoption of the new General Data Protection Regulation (GDPR), which will be implemented on 25 May 2018. The GDPR creates a single set of rules for all organisations processing personal data in the European Union, imposing much tougher rules on any affected organisation. Key innovations introduced by the GDPR include the implementation of Data Privacy Impact Assessments (DPIA), mandatory notifications to data protection authorities in the event of a data breach and the appointment of data protection officers. Another important element is that the new data protection rules provide for strengthened and enforceable rights for citizens. This allows a better control of individuals over their personal data, leading to more trust in online services on a cross-border scale, which will boost the digital single market. On the other hand, infringements will be subject to administrative fines up to €20m, or up to 4 percent of the company's total worldwide annual turnover of the preceding financial year, whichever is higher. The potential applicable penalties do incentivise companies to achieve compliance. However, these are just some of the changes. The reform itself is much broader and will require companies to exert significant effort and noteworthy investment. GDPR will also mean companies will face larger privacy compliance burdens.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

CHASTRE: Companies will have to develop IT compliance policies, procedures and oversight processes concerning cyber risks, for which purpose boards and IT departments will have to work closely. The first step companies should take is to assess their potential cyber risks, identify their most valuable assets and data in order to insulate them against the effect that a breach would have on the company, such as notifications of data security breaches, fines imposed by regulatory bodies, loss of intellectual property, in-house investigations, insurance premium increases, operational disruption or destruction, loss of customers or damage to brand and reputation. Another step is to work on a plan to both prevent cyber attacks and to deal with the aftermath of a security breach. One more essential aspect is to promote security awareness training among employees, provided that the impact of misuse by employees can result in massive damage for the company. Of course, this is only valid for incidents caused by negligent acts. It is much more difficult to prevent breaches caused by rogue employees, whose purpose may be stealing competitive information or to pursue some vendetta against the organisation.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

CHASTRE: Any organisation subject to the GDPR will be required to notify its local data protection authority within 72 hours, where feasible, and its data subjects, including clients, should it suffer a personal data breach. Besides these legal obligations resulting from the GDPR, in the event of a data breach, companies must also implement their contingency plan, if one exists.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER

CHASTRE: Given the severity and far-reaching consequences resulting from a cyber attack and the responsibility of directors for managing and mitigating risk exposure, cyber security insurance policies are an effective tool to help manage those risks. Insurance companies in Portugal have already developed specific products and policies designed to address different cyber risks, which means that each policy will be tailored

"Another step is to work on a plan to both prevent cyber attacks and to deal with the aftermath of a security breach."

RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

to a company's risk profile. Once again, making the right choice when contracting an insurance policy in this field requires a deep understanding of the risks a company faces in order to align the exposures and gaps to proper risk transfer solutions.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN PORTUGAL OVER THE COMING YEARS?

CHASTRE: According to the annual report published by the public prosecutor's office, one of the crimes most investigated in 2016, in the district of Lisbon, was cyber crime. There were 3493 cyber crime criminal investigations, 167 of which resulted in prosecution, criminal proceedings dropped in 3225 cases. Going forward, we are likely to see continued growth in the number of cyber attacks, which means that cyber defence capabilities will almost certainly increase as well. Therefore, we can only expect that cyber crime and data security will remain hot topics on business decision makers' agenda in the coming years.

CUATRECASAS

www.cuatrecasas.com

Leonor Chastre

Partner
Cuatrecasas
+351 21 355 38 00
leonor.chastre@cuatrecasas.com

Leonor Chastre graduated from the University of Lisbon Law School and has a postgraduate degree in IP Law from the University of Lisbon Law School. She also completed an Advanced Data Protection Course at the Instituto de Ciências Jurídico-Políticas of the University of Lisbon Law School. In addition, she is a lecturer for the postgraduate course in privacy and data protection at the Catholic University of Lisbon. The Portuguese Bar Association recognises Ms Chastre as an IP law specialist. She is the head of IP, media and IT practice at Cuatrecasas in Portugal.

GERMANY

DR JOCHEN LEHMANN
GÖRG

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN GERMANY?

LEHMANN: The major threats organisations are currently facing are attacks from outside of the company that capture whole IT landscapes. Recently, the 'WannnaCry' virus infected hundreds of thousands of servers and even affected train traffic in Germany. On a smaller scale, companies are often confronted with ransomware and the problem of whether they should pay up or try to fight the virus. And, finally, the 'fake president' trick seems to still be working.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

LEHMANN: Companies are definitely becoming more alert to data security issues. One need only look at the efforts that are being put into improving data security, such as the measures that are taken to make staff aware of the significance of data security or the money being spent on security measures. In order to achieve more data security, companies often consult not only the internal IT department, but also an outside adviser. Moreover, new responsibilities are being created that are making sure that IT security is a major task that receives enough attention and gets enough resources. However, it seems that if there is no chief information officer or a similar board member, the board tend to delegate this responsibility.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN GERMANY? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

LEHMANN: New regulations on data security and protection have placed more emphasis on compliance by creating new obligations and threatening ever heftier fines. However, the major change is still approaching. The General Data Protection Regulation comes into force in May 2018 and everyone has to comply from day one. Companies are currently trying to prepare for implementation day, however they have been very much left to their own devices. German regulators have, so far, failed to offer any guideline, even on the most basic of topics. Therefore, companies are currently reminiscent of a captain steering his ship through heavy fog, knowing that he might fail to reach his destination.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

LEHMANN: With regard to external attacks, companies should check internal and external protective measures. These measures should be brought up to the appropriate level. Staff awareness should also be raised, particularly for unusual events and the avoidance of the usual failures, such as the use of weak passwords, neglecting security measures and others. Companies should also look for advisers that are necessary in such a case, such as technical or forensic experts or public relations professionals. If the company wants to do its utmost to prepare for a breach, it will simulate practice attacks. As to internal threats, such as rogue employees, companies should introduce policies that restrict access to data and monitor that access. It should be possible to detect and register any access, for example, a major download, in order to investigate that. Often, employees that are about to leave the firm will try to take customer data or any other valuable data with them; as such, these employees should be placed under closer surveillance. And finally, all staff should be made aware of the fact that any attack or theft – from inside or outside – is a threat, not only to the company, but to their job.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

LEHMANN: The best response is diligent preparation beforehand and without such preparation, a company will never be able to demonstrate that it was compliant. The company must have an emergency plan, a short and efficient reporting chain in emergency cases and practice. The company should ensure access to the right expert, such as forensic experts, public relations experts and lawyers with specific expertise in such cases. The latter should know whether regulators have published guidelines and the whole emergency process should be assessed against the background of these guidelines. Although it is inevitable that mistakes happen in case of successful attacks because the attack cannot be predicted and the time pressure is enormous, the preparations will then enable the company to demonstrate that it acted as well as can be expected.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

LEHMANN: Insurance is crucial for three main reasons. First, it forces companies to bring their protective measures up to the necessary level. Most insurers require information and sometimes even testing. Second, if the company was successfully attacked, a severe production breakdown could have occurred that is often covered by the insurance by additional expenses for technical help and help with public relations. Finally, a director who does not arrange a good insurance policy is bound to neglect his duties and may be held responsible for the damages that would otherwise have been covered by the insurance.

"Cyber insurance will become as customary as D&O insurance."

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN GERMANY OVER THE COMING YEARS?

LEHMANN: It is likely that attacks will become ever more frequent and sophisticated. Security will often be just one step behind criminals so that every company will, at one time or another, be attacked. Therefore, companies will become better prepared and the demands on boards will steadily rise. So will the demands placed on companies by legislation because every few years a new bill with new security requirements will be enacted. Finally, cyber insurance will become as customary as D&O insurance.

www.goerg.de

Dr Jochen Lehmann

Partner
GÖRG
+49 221 33660 244
jlehmann@goerg.de

Dr Jochen Lehmann has been a partner at GÖRG since 2007 and specialises in IT matters with a particular focus on data protection and data security. He has built up his expertise in that particular field of law since he started working for GÖRG about 17 years ago. Dr Lehmann is a regular speaker on the subject of data secrecy and data protection in various contexts, such as data secrecy and directors' liability or data secrecy and insurance. He is also a member of GÖRG's IT group, which is led by four partners including himself, as well as the firm's internal IT advisory board.

ITALY

ALFREDO GALLISTRU
PWC

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN ITALY?

GALLISTRU: Cyber security threats are constantly evolving and are becoming more sophisticated with each new attack forcing organisations to increase their levels of protection. However, what makes this evolving environment more challenging is that businesses are up against a host of different attackers, for example, nation states, organised crime groups, hacktivists and insiders, who are highly skilled and armed with very sophisticated tools. Many of the major cyber threats companies face include: insider theft of intellectual property due to data exfiltration; loss of money due to ransomware attacks; loss of reputation and market share due to denial of service attacks (DoS); and the theft of personal data, due to advanced persistent threats (APT). Besides the recent WannaCry attack, which compromised countries around the world, one of the latest significant cyber espionage attacks occurred in Italy – 'Eye Pyramid' – saw information from the email accounts of high profile politicians, bankers and entrepreneurs stolen. Attackers were able to access important domains, for example, the central Italian bank and one of the major Italian political parties. Moreover, all stolen data was sent in a list of emails and then stored on servers in the US.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

GALLISTRU: Of course, cyber security is critical, and any new cyber attack hitting the news only raises its profile further. However, the importance of cyber security varies, depending on the company and the related industry it belongs to. Historically, industries like financial services and energy recognise the importance of cyber security, and are often a step ahead in protecting their own data and systems. Over the past few years, cyber security capabilities have been strengthened, formal processes have been implemented to identify and prioritise ICT security risks, mitigation strategies have been developed, and significant investments have been made to both execute these strategies and be well prepared to face cyber threats. For the other remaining industries, cyber security perception is

changing and the level of consideration is increasing. While some small firms are still naïve about cyber attacks, unable to realise how vulnerable they are and believing that a cyber attack will not happen to them, the majority of bigger companies are moving toward a model where cyber security is embedded into organisational culture.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN ITALY? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

GALLISTRU: The introduction of the General Data Protection Regulation (GDPR) is forcing companies to improve their security measures to protect personal data. Since January 2017, most companies in Italy have started to request a gap analysis to identify all legal and technical activities to address, in order to achieve compliance with the new regulation. The GDPR encourages companies to implement and manage protective security measures corresponding to the level of risk of their data. Therefore, this risk-based approach to data protection promoted by the new European law is leading many organisations to perform their first IT risk analysis on systems and applications, introducing the concept of prioritisation and adaptation of security measures, based on risk level.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

GALLISTRU: Cyber breaches can have a significant and potentially devastating effect on a company's reputation or financial position. For unprepared companies, a cyber breach can spiral out of control. In order to adequately address these likely large and complex breaches, it is necessary to develop a structured response framework and a cyber crisis management programme, which would enable the organisation to build clarity and discipline out of a chaotic environment and, ultimately, survive the cyber breach with minimal damage.

ITALY • ALFREDO GALLISTRU • PWC

"There is limited publicly available data on the scale and financial impact of cyber attacks, which makes it difficult to evaluate or price 'value at risk' with any precision."

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

GALLISTRU: First of all, having a structured cyber security incident response process is required to quickly respond to a cyber attack. Preparation activities, for example, risk assessment, awareness and training sessions, together with systems and network continuous monitoring, are all activities which enable IT specialists to create a steady environment to detect cyber incidents and minimise their impact. Once the breach occurs, containment actions, system recovery and collection of evidence lead companies to react to cyber incidents quickly enough to prevent them becoming a crisis. Follow-up reports and sharing lessons learned with subsequent document updates fosters continuous improvement, increasing security level and standards.

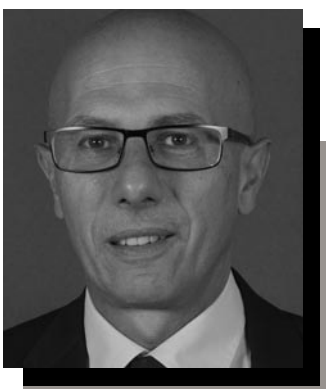
Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

GALLISTRU: Cyber insurance is a potentially huge market for insurers, and an opportunity for parties to cover or partially transfer the risk of suffering a security breach. However, the biggest challenge is that cyber is not like other risks: there is limited publicly available data on the scale and financial impact of cyber attacks, which makes it difficult to evaluate or price 'value at risk' with any precision.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN ITALY OVER THE COMING YEARS?

GALLISTRU: In line with recent trends, cyber attacks will become more sophisticated, difficult to trace and customised to the targeted company. This is because professional cyber crime organisations, political 'hacktivists' and state-sponsored groups have become more technologically advanced. Internet of Things (IoT) devices will massively increase and penetrate business operations. IoT devices run the risk of being used both as a platform to attack other external targets and also to compromise internal business operations and interrupting critical infrastructure. With vehicles becoming more automated and connected to the internet, to other cars and even roadway infrastructure, the number of potential intrusion points will grow exponentially, creating the opportunity for unforeseen types of cyber threats. Both IoT and 'next generation' cars affect people in their daily life, exposing them to safety risks which will seriously increase if criminals decide to exploit the high number of cyber security vulnerabilities currently

available on these technologies. Moreover, an emerging technique that could protect cyber environments will be the use of predictive models, which will enable cyber security teams to reduce delays identifying cyber threats and to define potential groups of assets that might be targeted by cyber criminals. Though 2016 was the year of ransomware, we predict that it will remain a very significant threat. In light of this, to face current and forthcoming cyber security threats, companies must ensure that cyber security strategy is aligned to enterprise strategy and fully supported by management. They must identify critical data in order to prioritise investments by assessing IT risk and defining cyber threat predictive models. They must know threats actors, their motivations, their resources, methods and techniques in order to reduce time between detection and reaction to an incident. They should assess both third-party and partner cyber security status, verifying that security policy and procedures have been adequately adopted. Finally, they should share and collaborate with peers in order to improve defences and cyber attack response capabilities.



www.pwc.com

Alfredo Gallistru

Partner
PwC
+39 02 7785 483
alfredo.gallistru@it.pwc.com

Alfredo Gallistru is a partner at PwC Italy. Within the risk assurance services practice he leads the IT risk assurance solution set. Mr Gallistru is a certified information systems auditor (CISA), certified internal auditor (CIA), certified information security manager (CISM), certified in the governance of enterprise IT (CGEIT) and certified in risk and information systems control (CRISC). He is vice president of the local ISACA Chapter in Milan. Mr Gallistru has more than 20 years of experience in information system auditing, privacy and information security consulting, compliance review and in the assessment and implementation of IT governance and IT controls.

TURKEY

BURÇ YILDIRIM
DELOITTE TURKEY

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN TURKEY?

YILDIRIM: We are seeing a significant increase in cyber attacks across the world, and the level of sophistication of these attacks is progressing in tandem with Moore's Law. The threats that these attacks pose to target organisations are not random. Effective defence against these issues requires a deep understanding of the actors, their sophistication and their motives. Different actors function differently and use a variety of techniques to exploit weaknesses in cyber defences. Organised crime is becoming a frequent threat actor against modern companies. Nation-state actors are more interested in companies operating in critical infrastructure. These actors cause data loss, fraud and revenue loss, reputational damage, IP theft and pose a threat to life and safety, through operational disruption. In our region, organised attacks targeting financial gain are on the rise. Some of these attacks are increasing in complexity, using different techniques to gain access to financial systems and use money mules. We have also seen a rise in ransomware attacks and whaling, which are causing both financial loss and operational disruption.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

YILDIRIM: Board members are increasingly realising that cyber risk must be treated as a top-tier business risk; however, they are far removed from the day-to-day challenges of monitoring, detecting and responding to evolving cyber risks. Leaders who develop a deeper view into where their organisation stands when it comes to cyber risk can gain a critical understanding for better managing the business. Effective cyber risk management starts with awareness at the board and c-suite level. Sharpening a company's ability to understand risk, manage performance, and move the organisation closer to cyber maturity often begins with answering important questions, and should result in becoming a more secure, vigilant and resilient business. All three traits are critically important today, though cyber threat management

traditionally has focused on 'secure' while paying less attention to 'vigilant' – comprehensively monitoring the extensive threat landscape – and 'resilient' – responding to, and recovering from, attacks.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN TURKEY? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

YILDIRIM: Several regulatory offices are expanding enforcement powers to include cyber security and data privacy in Turkey. Regulators may issue fines on type of violation and history. New privacy laws in Turkey mandate that companies protect personally identifiable information, build protections into core architecture and conduct regular assessments. Privacy laws extend the regulatory point of view into many sectors. Companies must go through a paradigm shift to manage and maintain compliance. This means changing the way they do business and handle data. The awareness level of employees must also be raised to maintain compliance.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

YILDIRIM: Focus on what matters – your crown jewels and relationships. Identifying your crown jewels will help you prioritise security investments and the security requirements for third parties that might host your data off premises. Companies should also proactively assess their cyber risks. Cyber threat intelligence involves using technology, processes and people to proactively acquire, analyse and disseminate intelligence – internally and externally – as a way of improving security. The CTI approach emphasises situational awareness and tactical or strategic responses that can help reduce the likelihood of harm or risk for your organisation. Companies should also focus on building a multi-layered defence, particularly as cyber adversaries, actors and criminal organisations continue to employ increasingly sophisticated exploit techniques, and evolve their tactics. Some of these methods bypass traditional cyber defence systems, as well as more sophisticated

defence systems. Steps must also be taken to fortify organisations; even though you know what your organisation's critical assets are, that does not make you secure. While the news is filled with accounts of cyber attacks that target unknown system weaknesses, most attacks exploit well-known system weaknesses. Fix known vulnerabilities, use security by design and identify physical vulnerabilities. Finally, companies must prepare for the inevitable. Organisations should carry out cyber simulations to test their true cyber security preparedness and to determine the usefulness of existing crisis management and security incident management processes. Cyber simulations are interactive techniques that immerse participants in a simulated attack scenario to help organisations evaluate their response and preparedness.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

YILDIRIM: To prepare for the inevitable attack, your organisation should be asking the following questions: who should be contacted during and after an incident? Which groups and individuals should be engaged? Which third parties will you need to notify or engage? Which customers or external users will you need to alert? What will you tell them? How will you tell it to them? And what about regulators and the role of privacy and legal groups in your organisation? How will you engage them? And ultimately, how quickly can you contain a security breach and restore your organisation to normal operation? Having answers to the key questions and many more organisation specific questions can help you bounce back quickly after an attack. But answering the questions is just part of the equation. Testing your answers is critical.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

YILDIRIM: The ever-evolving cyber risk landscape is driving interest in cyber insurance as one complementary element of the cyber risk management approach, which allows organisations to transfer some of the risks associated with cyber incidents to their insurance provider. Cyber insurance can complement an organisation's active security measures by providing insurance coverage in three broad areas: liability for a data breach or loss; remediation costs, for example, for investigating

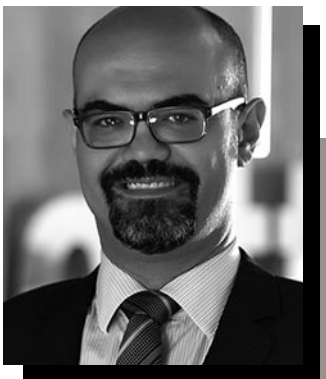
"The penetration of IoT devices will definitely grow and will cause several new types of threat."

the breach, notifying affected parties, and so on; and regulatory fines or penalties and settlement costs.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN TURKEY OVER THE COMING YEARS?

YILDIRIM: The coming years will bring more conventional problems. The criminal community is sharing information, tactics and techniques very effectively and quickly. The penetration of IoT devices will definitely grow and will cause several new types of threat. We are facing a cyber talent shortage which will continue to escalate. We will continue to see the effects of cyber crime on companies.

Deloitte.



www2.deloitte.com

Burç Yildirim

Cyber Risk Services Leader
Deloitte Turkey
+90 212 366 60 34
buyildirim@deloitte.com

Burç Yıldırım is the partner responsible for cyber security services offered under risk advisory in Deloitte Turkey. He has over 15 years of experience in IT security, especially in offensive techniques. His experience includes penetration testing, technical assessments, code review, malware analysis, digital forensics, secure development, ICS security and embedded systems security. Between 1999 and 2005 he developed a web and email filtering solution for SMB's at a local firm. Between 2005 and 2007 he was an architect for local developed UTM solution. Later he continued his career at a local integrator as a manager.

ISRAEL

OPHIR ZILBIGER
BDO CONSULTING GROUP

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN ISRAEL?

ZILBIGER: The WannaCry attack represents a new wave of threats derived from 'weapons grade' cyber attack tools. It is based on the leaked NSA arsenal of cyber weapons and demonstrates the level of threat state-sponsored cyber attack represents. Though it was all over the news, it had a limited impact on organisations in Israeli systems and around the world. It did serve as a wakeup call for raising the awareness of executive and operational management to cyber risk. Current cyber threats applicable to companies can roughly be divided into two groups: cyber crime and state sponsored. Cyber criminals are mostly looking for ways to make money. It's as simple as that. Every company needs to think about how an attacker might be capable of making money by attacking the company as part of their risk assessment process. State-sponsored cyber threat is mostly about intelligence, IP theft and the ability to use cyber as an attack vector. Companies usually would not be able to mitigate state sponsored attacks and it is not necessarily in their business interest to do so. This is where the government needs to step in and regulate, assisting in mitigating risks that might be associated with cyber threats.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

ZILBIGER: Two factors that influence the level of maturity of cyber security in companies – among others – are geography and industry. In certain geographies, one can find a very high level of awareness to cyber risk and, as a result, highly motivated management that invests in cyber security. Other geographies are well behind, although it seems like everyone understands that cyber risk is important enough not to be ignored today. Industries such as financial services or critical infrastructure face higher risk levels and are usually highly regulated, resulting in a higher level of maturity while more traditional industries,

such as real estate or manufacturing, are usually less mature. In general, we believe that a risk driven approach has to be adopted, and therefore the board has to be able to effectively assess cyber risk and manage the high risks identified. For this to happen, companies need cyber aware board members with the ability to understand these risks. In most cases, it is rare to find boards that have these capabilities. The US recently drafted a bill to require boards to have board members that have cyber related knowledge to improve this.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED ISRAEL? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

ZILBIGER: Israel is one of the leaders in cyber security regulation. The bank of Israel released its 'cyber defence management' regulation in 2015 that took information security a step further, requiring banks to have a new role – a chief cyber defence officer (CCDO) – whose role is to manage cyber risks and control information security, physical security, fraud and business continuity. This has significantly changed the way that banks address cyber risks today, having to assess cyber risks and report their cyber risk posture in their financial statements. The new CCDO role is more senior than the traditional CISO and has more authority. Board and senior executive management are required to manage cyber risks and to sign off on strategy and policy. This kind of approach was also adopted by the regulator of insurance companies and the rest of the financial sector. This drives a shift in the market moving from compliance based security to risk based and effectiveness driven cyber security with a broader scope of defence, not only protecting information but protecting the ongoing operation of the organisation, its reputation, money and even human life, in the healthcare sector.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

ZILBIGER: The most important part of cyber security nowadays is cyber resilience. We define cyber resilience as anything that needs to be in place post an attempted breach or an actual breach. Companies have to realise that no matter how much they invest in prevention, a breach might still happen and when it does, they have to be able to identify the breach and respond to it effectively, in order to reduce its impact. Monitoring, incident management and cyber business continuity are mandatory, yet traditionally they are areas that have not been addressed in many or even most organisations' security programmes. The mid-market segment is facing a huge challenge implementing these and has to consider moving to a managed services model utilising managed security service providers.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

ZILBIGER: This is also geography dependent as regulation and social acceptance are different. In Israel, notification of a cyber breach has only been recently introduced. I believe companies have to utilise PR experts to maintain share value. Effective management of a cyber incident relies on highly trained management. It is key for top executives to know what to do in case something happens. We recommend running an annual cyber drill or a tabletop exercise, at the very least, to allow management to be trained and versed in recent cyber threats and their implications.

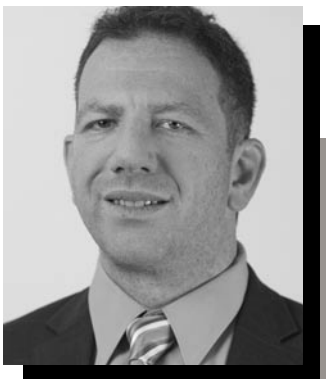
Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

ZILBIGER: Cyber insurance must be considered to transfer some of the cyber risk. It is important to keep in mind that cyber insurance is tricky and has to be looked at by experts to make sure that coverage is adequate. Cyber risk management has to be the basis of cyber insurance, therefore companies must have a mature cyber risk management programme including the ability to effectively assess cyber risk. Today, there are no standardised cyber risk assessment programmes and traditional risk assessment methods are not compatible with cyber risk and do not provide a clear cyber risk map to enable the above.

"Law enforcement agencies and the government must provide companies with insight and intelligence with regards to cyber criminals' ability and intent in each geography."

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN ISRAEL OVER THE COMING YEARS?

ZILBIGER: Law enforcement agencies and the government must provide companies with insight and intelligence with regards to cyber criminals' ability and intent in each geography. It is impossible for companies to know if cyber criminals are willing to commit cyber crime that, for instance, involves physical crime as well. With no knowledge of the current threat landscape in terms of cyber crime, companies are blindfolded and cannot address cyber crime effectively. Intelligence is in fact one of the representations of the evolution from traditional information security to today's cyber defence.



www.bdo.co.il

Ophir Zilbiger

Partner – Head of SECOZ Cybersecurity Center
BDO Consulting Group
+972 (3) 966 8855
ophirz@bdo.co.il

Ophir Zilbiger leads the development and ongoing day to day operations of the BDO SECOZ Cybersecurity Center, supporting clients globally to meet their cyber defence challenges. His cyber security expertise combines insight into risk management, IT and information security and technology. He began his career as a technical team leader involved in worldwide information security projects, managing the Israeli global risk management solutions of PwC in which he led large-scale consulting projects in the areas of risk management and information security with leading local and international companies.

JAPAN

TAKASHI NAKAZAKI
ANDERSON MORI & TOMOTSUNE

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN JAPAN?

NAKAZAKI: Traditionally, Japanese companies have been confident about their ability to thwart cyber attacks, but this confidence is wavering. In recent years, many Japanese companies have been victims of cyber attack perpetrated by external hackers and data theft carried out by current and former employees. 2015 saw a significant cyber attack and the Japan Pension Service suffered a highly publicised data breach after an employee opened a phishing email containing malware that attacked the department's network. In 2016, a record 128.1 billion cyber attacks against networks in Japan were detected, more than double the previous year, according to a recent survey by a public research institute. Furthermore, it was reported that 2000 computers at 600 Japanese companies had suffered from the global 'WannnaCry' ransomware attack in May 2017. In recent years, there have been a number of serious data leaks by current and former employees and outside contractors. Typically, an employee would steal trade secrets from his or her former employer and hand them to a new employer. Those affected companies have internal rules and policies, however, they do not have technological and physical countermeasures to avoid intentional data leakage.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON

NAKAZAKI: There has been a growing awareness among Japanese companies that cyber security needs to be stronger and that organisations need to devote more time and money to building more sophisticated security frameworks. This awareness is being driven by several events, including the Tokyo Olympics in 2020. However, to date, many Japanese companies have not placed enough importance on cyber security. Many IT departments have inadequate budgets to implement sufficient cyber security countermeasures. The Japanese

APPROACH TO IMPROVING POLICIES AND PROCESSES?

government has recognised this issue and publicised the Cybersecurity Management Guidelines. These guidelines stress that the failure to take sufficient cyber security countermeasures might possibly result in heavy damages against private companies.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED JAPAN? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

NAKAZAKI: In Japan, cyber security and data privacy regulations have changed greatly in recent years. Japan has a dedicated cyber security law – the Basic Cybersecurity Act – which was enacted in 2014. In consideration of increasing threats to cyber security, the Basic Cybersecurity Act was partly amended in 2016 to fundamentally reinforce the countermeasures taken by the national administrative organs. More specifically, under the amended Act, the scope of parties to be evaluated by the government, in terms of cyber security measures, has been expanded to cover special corporations and authorised corporations, in addition to the central government and incorporated administrative agencies. Under the Basic Cybersecurity Act, the private sector in a number of areas has been required to take technological and organisational countermeasures including cyber threat drills. The Act specifically prescribes, in addition to the cyber security duties of the state and the local authorities, the cyber security duties of critical infrastructure business operators and cyber related business operators. Critical infrastructure business operators in information and communications technologies (ICT), finance, aviation, railway, electricity, gas, government and government services, including local authorities, medical, water, and logistics sectors are expected to safeguard data with the same level of security as governmental institutions.

"It is essential to control each employee's access to personal data and to monitor unauthorised access to restricted areas and protected data."

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

NAKAZAKI: Companies should develop a system to ensure good governance, decide on matters concerning internal regulations and other systems. Internal regulations governing risk management are general in nature, and they are typically not intended for ensuring cyber security. Provisions for ensuring cyber security, however, may be required as part of the internal policies, depending on the type or the volume of information held by the company or its business type. To avoid cyber breaches from internal sources, many companies are eager to implement education and training programmes and to establish strict internal rules and policies. Such countermeasures, however, do not seem sufficient. In addition, technological and physical countermeasures also should be implemented. To avoid the actions of rogue employees, it is essential to control each employee's access to personal data and to monitor unauthorised access to restricted areas and protected data, unauthorised utilisation of devices and unauthorised carrying devices.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

NAKAZAKI: Affected companies should understand the damage done by cyber incidents and take immediate steps to stop the attack by implementing technological countermeasures and reporting the breach to the authorities. With regard to cyber attacks, it is strongly recommended that companies voluntarily share cyber threat information within their industry, as well as with regulatory bodies. As to personal data, the APPI, either before or after the amendment, does not include obligations to notify the regulators or affected individuals of any breaches of security. However, upon the occurrence of any such breach, notification to the regulator or an accredited personal information protection organisation, if applicable, is generally required or recommended under the guidelines for the APPI. In addition, such guidelines generally recommend or require notification of the affected individuals or a public announcement in case of serious security breach incidents.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE

NAKAZAKI: The Cybersecurity Management Guidelines suggest purchasing insurance products designed for cyber incidents to avoid

related risks, including costs to recover lost data and establish safe environments and compensation to a third party who suffers as a result of the leak. Such insurance services are new in Japan and fees are relatively high but it should be necessary to mitigate significant risks.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN JAPAN OVER THE COMING YEARS?

NAKAZAKI: More Japanese companies will probably suffer from cyber attacks from overseas hackers and data breaches from internal resources. By contrast, many companies will recognise the importance of taking countermeasures for cyber security and data security and propose to increase their budgets in this area. In relation to the Basic Cybersecurity Act, there are cyber security guidelines for parts of infrastructure business areas, such as finance, medical and electricity. The Act requires the relevant regulators to establish detailed rules for each relevant private sector and, in the near future, it will be possible that the duties for these business operators could belong to other infrastructure business areas.

HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

ANDERSON MŌRI & TOMOTSUNE

www.amt-law.com

Takashi Nakazaki

Special Counsel
Anderson Mori & Tomotsune
+81 3 6888 1101
takashi.nakazaki@amt-law.com

Takashi Nakazaki is special counsel at Anderson Mori & Tomotsune with broad experience in the areas of data protection; information security; intellectual property, including copyright and trademarks; licensing, including software licences and patent licences; payment services, including credit cards and pre-paid cards; cyber law issues, such as e-commerce, domain names, cloud computing and other technology related areas, including computer forensics, digital copyright, software development and open source code; telecommunications; labour and general corporate law. He frequently advises various international and domestic online service companies including operators of online games, social games, online gambling, SNS and live streaming.

AUSTRALIA

LEON FOUCHE
BDO AUSTRALIA LTD

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN AUSTRALIA?

FOUCHE: Instances of confidential data disclosure in the healthcare sector and unavailability of internet connected services within the Australian federal government have been widely publicised. Unfortunately, the frequency of such events is increasing and eroding the general public's trust in internet connected services. Cyber attacks against small to medium size businesses (SMEs) are also of concern, but this activity is receiving less publicity. In most cases the aim of such attacks is to steal intellectual property or disrupt business operations. The impacts are often significant for the SME due to lost commercial opportunities or the eradication of the business's market advantage. As a country with a growing technology and digital economy, where 70 percent of all Australian businesses are classed as SME, cyber incidents and loss of intellectual property have the potential to considerably impact the nation's economy.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

FOUCHE: Company boards are taking notice of cyber security risks. A recent survey indicated that nearly half of the country's ASX100 boards are confident their companies are properly secured. What is less obvious is how boards are effectively addressing this risk, in collaboration with their organisation's ICT and cyber security teams. While we have seen boards increasing investments in technology to address cyber risk, a focus on establishing a strong organisation-wide security culture is still needed. Boards also need to understand that cyber resilience is dependent on a culture that embraces strong risk management practices, with the right mix of technical, procedural and people led controls.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS

FOUCHE: For more than two decades Australian organisations have been expected to proactively maintain the security of individuals' data to protect privacy. Although recent privacy regulatory changes will introduce more external insights into how organisations address privacy

CHANGED AUSTRALIA? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

regulations, compliance expectations have not changed considerably. What is changing quite drastically within the Australian business landscape is how organisations will be held to account by those the regulations aim to protect. Consumers and customers stand to gain a clearer picture of how well businesses are doing when it comes to cyber security and data privacy protection. Data protection failures will likely need to be disclosed, resulting in increased public awareness. The reputational impact of these notifications could be considerable. The Notifiable Data Breach scheme, due to begin on 27 February 2018, should see organisations take action to understand privacy regulations fully and proactively assess their compliance.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

FOUCHE: There are a number of basics that everyone should be doing. First, organisations need to understand what the critical information and IT systems are in their environment – the 'crown jewels' – and how well these are protected. It will be important to have appropriate resilience in place for these should it be impacted by a cyber event. Second, ensure the security of applications, operating systems and devices in their environment are kept up-to date. If it is no longer used, uninstall or remove it from their environment. It sounds simple but it is a very effective way to reduce the attack surface. Third, improve cyber security awareness among employees and management. They are quite often the initial target of a cyber attack, and if users can identify and avoid threats, the likelihood of a successful attack will reduce. Fourth, demonstrate vigilance and closely monitor your environment. Logging system events and investigating anomalies in real time is the best way to identify a cyber breach. Knowledge of what is happening across the environment will ensure issues can be addressed before they have a significant impact. Most importantly, be prepared. The impact of many cyber security incidents can be reduced if action is taken early and decisively.

"Ransomware has proven to be a lucrative approach for criminals and it will continue to impact individuals and SMEs harshly."

Organisations need to understand their risk exposure and have a plan in place to respond quickly and efficiently to cyber incidents. This plan needs to be kept up to date and tested regularly.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

FOUCHE: When a cyber breach or data loss event is suspected, or occurs, investigations should be initiated as quickly as possible. Firms will want to establish the facts quickly and ensure they work in the best interests of all potentially impacted parties. Advanced preparation is essential to achieve this. Organisations should take stock of where critical, valuable and sensitive data is stored and systems are located. They should assess the impacts of such data or systems being lost or exposed, from the perspective of the subject, meaning the customer, as well as the organisation. Next, they should ensure data and systems are adequately protected to avoid the worst case scenarios. One last preparation step is to know who to call for help if a breach is suspected. Typically the first person to call is a lawyer as this provides protections under client privilege.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

FOUCHE: Cyber insurance is starting to become a popular risk management approach among Australian businesses. It typically forms part of an organisation's approach to managing the costs associated with recovering from a cyber security incident. However, a policy is only of real value when it is combined with a considered approach to managing all cyber security risks. These policies cannot plug the holes where security controls should have been adopted. Adequate consideration of cyber security risks and the approach to minimising impacts really is the only way business owners and leaders can deal with cyber risk, potential losses and related liabilities. As the regulatory landscape becomes more stringent and enforcements occur, more organisations will consider and take up insurance.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN AUSTRALIA OVER THE COMING YEARS?

FOUCHE: Ransomware has proven to be a lucrative approach for criminals and it will continue to impact individuals and SMEs harshly. The availability of new cloud based services from new providers seeking to disrupt commercial markets may lead to more organisations experiencing collateral damage to ransomware. The changing regulatory landscape will certainly lead to more data breaches becoming public knowledge. The lesson others will quickly learn from these breaches is that incident response capabilities are paramount to survival. All Australians will experience increasing impacts of cyber security incidents as attacks against critical infrastructure increase in sophistication and frequency. The effects of these will be a stark reminder that as Australia builds a digital future, cyber security will be a keystone of success. The Australian government is expected to continue investing in educating organisations and citizens on cyber wellness and online safety to improve our national cyber security awareness, as well as putting strategies in place for addressing the critical shortage of skilled cyber security professionals.

www.bdo.com.au

Leon Fouche

National Leader, Cyber Security
BDO Australia Ltd
+61 7 3237 5688
leon.fouche@bdo.com.au

Leon Fouche is an experienced ICT professional specialising in cyber security, cloud and technology risk advisory services. With more than 20 years' experience delivering a wide range of business and IT projects, ranging from strategy development through to system implementations across Australia, Europe and Africa, Mr Fouche works with company boards and the C-suite where he helps them understand the cyber threats and risks that impact their business and the strategic activities required to manage these risks. He also works with technical teams to help them understand the security vulnerabilities and technical security gaps in their organisations' systems and processes.

NIGERIA

JOSEPH TEGBE
KPMG NIGERIA

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN NIGERIA?

TEGBE: The cyber threats faced today by companies are similar across sectors and geographies. Rapidly evolving business ecosystems, as a result of the convergence of digital technologies, are expanding the cyber attack surface for cyber criminals. However, cyber threats are not conventional, neither are threat actors. These threats include denial or disruption of service, phishing, ransomware, cyber espionage, sabotage and hacktivism. According to a World Economic Forum Global Risk Report, "The internet has opened a new frontier in warfare: everything is networked and anything networked can be hacked". Furthermore, a 2016 Symantec survey noted that 430 million new malwares were discovered in 2015 alone, an increase of 36 percent on 2014. The cyber threat landscape is changing and our approach to managing cyber risk must also evolve. Countries in Africa are not insulated from this global menace. There have been a number of cases of cyber attacks across different sectors in Africa. North Korea was linked to attacks on banks in several countries, including Nigeria. Organisations in Nigeria have continued to face cyber security challenges; there have been instances of fraudulent transactions on different online banking platforms, successful DDoS attacks on some banks, attacks on websites of some government agencies and instances of identity theft.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

TEGBE: CEOs are beginning to acknowledge that the new wave of technological advancement that comes with cyber risks cannot be ignored. According to our recent survey, cyber security is the top risk named by global CEOs. However, there is a need for boards and senior management to do more. The board needs to ask the right questions of the company's cyber security strategy. Every company must assess the success of its cyber security programme. Organisations also need to periodically assess and enhance capabilities in place to respond adequately to a cyber incident.

Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED IN NIGERIA? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

TEGBE: A number of countries in Africa have enacted laws on cyber crime. For instance, in response to the various requests and demands from concerned stakeholders in both the ICT and legal sectors, the Cybercrime (Prevention, Prohibition, Etc) Act was signed into law in Nigeria in May 2015. The Act provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes in Nigeria. However, there is a need to put in place frameworks and capabilities that will ensure adequate incident and emergency response to cyber security incidents.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

TEGBE: There are no foolproof systems. However, every organisation must take pragmatic steps to secure its crown jewels. The approach to securing the cyber ecosystem has to be holistic and must be integrated into the enterprise-wide risk management strategy. Countering an evolving threat landscape requires board level steer, insight and decision making. Every board that will be successful in mitigating cyber risk must be able to ask and answer these critical questions: What are our crown jewels? What and where are the digital assets that give us our competitive advantage? We need to protect what matters. Do we really know our enemy? Every organisation must have a clear understanding of the motivation, intent, strategy and tactics of the enemy in order to anticipate threats and effectively prevent, detect and respond to attacks. Who is in charge of managing cyber risk? Do those charged with cyber security possess the capability to effectively manage this risk? Are we measuring the success, or value, of cyber security efforts correctly? Are we making progress? Are our efforts yielding the right results? Do our partners and service providers have equivalent capabilities and skills to protect our data? There is a need to pay attention to third-party risk management.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

TEGBE: Being agile enough to respond to a cyber event often depends as much on the organisation's governance as its technological capability. In a recent survey conducted by KPMG, 75 percent of global CEOs were not fully prepared for a cyber incident. There is a need for every organisation to adequately prepare in order to respond to cyber incidents. There is a need for every organisation to have a clear strategy and relevant procedures in place for responding to cyber events based on its business continuity plan. The response plan must be clearly defined and regularly exercised. Once these are in place, firms will be able to respond constructively to a cyber breach in a way that their customers, investors, regulators and other key relationships will be assured that due care was exercised in the event of the incident.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

TEGBE: Cyber insurance is a broad range of insurance products designed to protect businesses from operational risks affecting confidentiality, integrity and availability of information assets. Cyber insurance products can include coverage for various risks, including data breach, cyber extortion, identity theft, disclosure of sensitive information, business interruption, network security and breach notification and remediation. Globally, the cyber insurance market is booming. There are several indicators that demonstrate that it will be the one of the biggest markets for insurance organisations in the coming years. However, insurance organisations in Africa must be more sophisticated in assessing cyber risks to turn this emerging opportunity to a sustainable line of business and create products and policies leveraging this business opportunity.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN NIGERIA OVER THE COMING YEARS?

TEGBE: As digitisation continues to open up innovative products and services, cyber attack vectors will continue to expand and evolve. We expect that we will continue to see more sophisticated and widespread attacks, much like the 'WannaCry' ransomware attack which affected around 150 countries; compromising more than 200,000 computers in

"Being agile enough to respond to a cyber event often depends as much on the organisation's governance as its technological capability."

about 72 hours. We also expect the profile and motivation of attackers to evolve from just obtaining monetary gains to more damaging goals, such as industrial espionage, reputational damage, political or social causes and the like. Similarly there will be an increase in the pool of typical targets from predominantly financial institutions, as we see today, to other sectors and even government. However, while we believe that businesses and governments need to view their major digital transformation initiatives through the cyber security lens, cyber risk should not be an impediment to digital innovations but an advantage; if adequately managed. The key is keeping cyber security as a top management agenda and deliberately establishing and maintaining cyber defence mechanisms that cut across people, process and technology.

home.kpmg.com

Joseph Tegbe

Partner & Head, Technology Advisory
KPMG in Nigeria
+234 803 402 0989
jtegbe@kpmg.com

Joseph Tegbe is the partner and head of the technology advisory practice of KPMG in Nigeria with over 27 years of extensive experience in servicing clients across the public and private sectors of the economy. He has served as engagement partner on several cyber security projects across several clients in the public and private sector. He is currently the KPMG Africa lead for cyber security strategic growth initiative (SGI).

SOUTH AFRICA

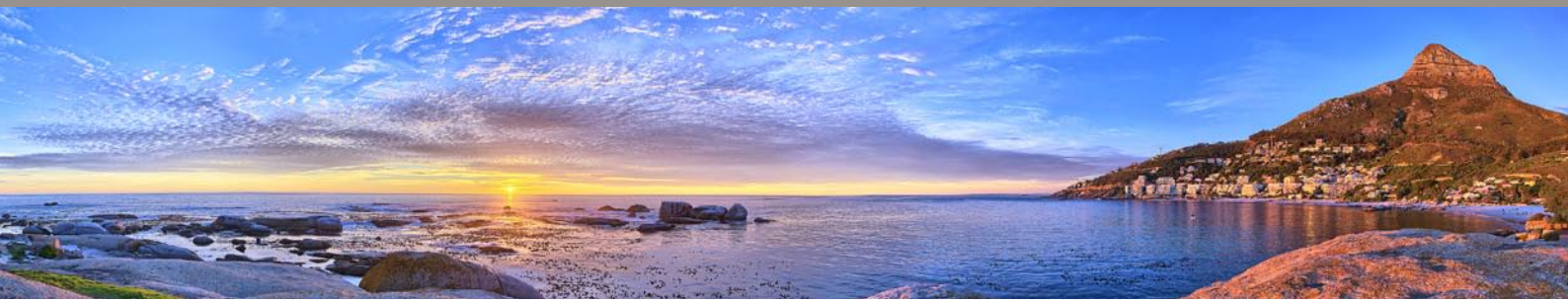
GRAHAM CROOCK
BDO SOUTH AFRICA

Q IN YOUR OPINION, WHAT ARE THE MAJOR CYBER THREATS TO WHICH TODAY'S COMPANIES ARE VULNERABLE? COULD YOU COMMENT ON ANY RECENT, HIGH PROFILE CYBER ATTACKS IN SOUTH AFRICA?

CROOCK: The most significant cyber threats that parties are experiencing are ransomware attacks via social engineering schemes. These are perfectly avoidable attacks that require employees to be vigilant when responding to or actioning emails. There are also a vast number of organisations that are of the belief that their infrastructure and networks are secure, only to discover after a vulnerability and penetration test that they are in actual fact open and vulnerable to outside attackers who are able to access extremely sensitive information and, more often than not, violate the organisation in more malicious ways.

Q GIVEN THE RISKS, DO YOU BELIEVE COMPANIES ARE PLACING ENOUGH IMPORTANCE ON CYBER SECURITY? ARE BOARD MEMBERS TAKING A PROACTIVE, HANDS-ON APPROACH TO IMPROVING POLICIES AND PROCESSES?

CROOCK: Until recently, we found that organisations typically had a 'superhero' mentality and in ignorance believed that a cyber attack 'will not happen to me'. Top executives and board members are slowly awakening to the inevitability and the subsequent reality of the devastation that a cyber attack could cause and are now beginning to ask the right questions. This happens, predominantly, after a significant attack has occurred, and the impacts of the devastation are reported. The response is therefore more reactive, and motivated by a strong sense of fear, doubt and uncertainty. We would like to see this reactive stance shift to a more proactive stance where leaders are showing a more hands-on approach to improving their cyber health. Compounding the problem, however, is that most organisations conceal their misfortune and, as a result, other organisations are unable to learn from a major incident that could easily have affected them. Organisations should rather spin the negative publicity of a misfortune as a positive educational service to the community.



Q TO WHAT EXTENT HAVE CYBER SECURITY AND DATA PRIVACY REGULATIONS CHANGED SOUTH AFRICA? HOW IS THIS AFFECTING THE WAY COMPANIES MANAGE AND MAINTAIN COMPLIANCE?

ROOCK: There is pressure on organisations to become more conscious of data privacy laws that are most likely to take effect next year. There is a great deal of preparation work required to be done in order to secure an organisation's data and to ensure compliance with the POPI Act. Organisations will be severely impacted by the regulations as they will need to rework the manner in which data is collected, processed and stored. This may entirely affect the way in which an organisation conducts its business. Compliance with the act, however, is becoming a key competitive advantage factor, separating those who know how to securely handle data and the processing thereof, and those who do not.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD COMPANIES TAKE TO AVOID POTENTIAL CYBER BREACHES – EITHER FROM EXTERNAL SOURCES SUCH AS HACKERS OR INTERNAL SOURCES SUCH AS ROGUE EMPLOYEES?

CROOCK: There are several activities that can be explored as immediate action steps to avoid an unforeseen cyber attack. These include: ensuring that your organisation's IT is compliant to standards and controls provided by the guidelines of COBIT, ITIL and ISO27001; conducting a gap assessment of the cyber risks facing your organisation, as measured against the NIST Framework; conducting a compulsory cyber awareness training initiative among all employees, regardless of title and status; conducting a vulnerability scan and penetration test to verify the security of your organisation's infrastructure and network security; and engaging ongoing monitoring services that provide immediate alerts at the first trace of a threat.

Q HOW SHOULD FIRMS RESPOND IMMEDIATELY AFTER FALLING VICTIM

CROOCK: It is imperative that an organisation has a cyber crime support partner. That is, a go-to partner that has a first response team to guide victims through the 'do's and dont's' of an attack, as and when it occurs. Your selected partner must have sufficient experience of a

TO CYBER CRIME, TO DEMONSTRATE THAT THEY HAVE DONE THE RIGHT THING IN THE EVENT OF A CYBER BREACH OR DATA LOSS?

host of attacks and be backed by the necessary skills and technology to remedy and restore the situation. Such a partner should also be engaged early, in order to determine the cyber risk maturity of the organisation and to best advise what controls need to be in place to mitigate such risks. In this way, the cyber crime support partner is involved in developing a cyber security strategy for the organisation and aids not only in reactive, but also proactive, support.

Q IN WHAT WAYS CAN RISK TRANSFER AND INSURANCE HELP COMPANIES AND THEIR D&OS TO DEAL WITH CYBER RISK, POTENTIAL LOSSES AND RELATED LIABILITIES?

CROOCK: To help bear the costs associated with data breaches, some companies are turning to cyber insurance as part of their overall risk management strategy. The costs of a cyber attack include investigating the cause of the breach, hiring expert consultants to remedy it, setting up customer support to tackle questions relating to the breach, and others. More difficult to quantify are potential fines and reputational damages that arise from the breach. Cyber insurance cover varies greatly from one policy to another, and it is vital that organisations work with a broker that specialises in placing cyber insurance policies. Some of the basic coverage areas include: privacy liability; forensic investigation; network or business interruption; extortion; data loss and restoration; theft and fraud coverage; notification costs; crisis management; and credit/identity monitoring and regulatory actions. The adviser and underwriter work to evaluate an organisation's specific needs and risk areas by using cyber risk assessments.

Q WHAT ARE YOUR PREDICTIONS FOR CYBER CRIME AND DATA SECURITY IN SOUTH AFRICA OVER THE COMING YEARS?

CROOCK: Cyber crime is a threat that is permeating the business world at a rapid rate, with more and more criminals mastering the trade, which has proven to be a financially thriving trade to be in. As organisations tighten security measures and controls, we are finding that criminals are devising even more ingenious means to outsmart them. The trend is such that cyber crime attacks follow a very close trail behind the newest and most robust defence solutions. Perpetrators constantly need to be more creative to breaking through these defences. With this in mind, we predict that there will be a trend toward developing

"We predict that in the near future, cyber insurance will feature in every organisation's income statement."

cyber readiness solutions, over and above the focus on cyber defence solutions. This means that organisations will dedicate more spend on technology and services that will aid them after an attack, for example, data backups, data recovery and restoration, so as to prevent attacks from bringing them to a grinding halt. Furthermore, we are seeing a trend where top management is enforcing a general cyber education within their organisations. Employees are becoming more cyber-savvy, which is a powerful defence solution as most cyber attacks are targeted at tripping up employees via phishing campaigns. We also predict that organisations are accepting the inevitable fact that it is only a matter of time until they fall prey to an attack, which is driving an increase in cyber insurance investments. We predict that in the near future, cyber insurance will feature in every organisation's income statement.

www.bdo.co.za

Graham Croock

Director IT Audit, Risk & Cyber Laboratory
BDO - South Africa
+27 82 606 7570
gcroock@bdo.co.za

Graham Croock leads the BDO technology advisory services practice and he heads up the BDO cyber laboratory. He has more than 25 years experience providing information technology (ICT), operations and risk management services to listed companies and various other high value businesses. His skill lies in ICT risk, cyber risk, specialised disaster recovery planning, business continuity management and ICT audit and governance services that enables innovation and agility to facilitate regulatory and compliance requirements. In addition, he serves as a trusted adviser to company boards, CIOs, COOs and CFOs.

www.financierworldwide.com