REPRINT

FINANCIER WORLDWIDE MAGAZINE

ROUNDTABLE

Cyber risk & security

REPRINTED FROM
MAY 2018 ISSUE

FINANCIER WORLDWIDE corporatefinanceintelligence

ROUNDTABLE:

CYBER RISK & SECURITY

Given how much they rely on technology, cyber risk and security is an increasing concern for all businesses. Protecting valuable data is now a critical issue for management, not just IT. However, many businesses neglect to update their cyber policies and processes, leaving them open to attack and potential financial, operational and reputational damage. Going forward, as risks constantly evolve, companies need to be aware of the vulnerabilities of new technology, software and applications – and remain vigilant. ■

THE PANELLISTS

Great Gu
APAC CyberSecurity Manager, AstraZeneca China
T: +86 18 916 527 303
E: great.gu@astrazeneca.com
www.astrazeneca.com

Great Gu is a cyber security, risk management and IT governance expert. He won the (ISC)2 2017 Asia-Pacific Information Security Leadership Achievements (ISLA) award, as well as the only one from China mainland. He is frequently invited to speak on cyber security topics for online seminars and large-scale conferences across Asia-Pacific (APAC), and host elite cyber security panels.

Paul Lanois
Vice President, General Counsel, Credit Suisse AG
T: +852 9539 0300
E: paul.lanois@credit-suisse.com
www.credit-suisse.com

Paul Lanois is a global privacy, data protection and information security law expert and is an attorney admitted to the Bars of the District of Columbia, New York and the Supreme Court of the US. He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at numerous conferences across Europe, the US and Asia.

Dr Jochen Lehmann
Partner, GÖRG
T: +49 221 33660 244
E: jlehmann@goerg.de
www.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 his expertise in this particular field of law since he began working for GÖRG 15 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.

Jeff Bullwinkel
Associate General Counsel, Microsoft Europe
T: +31 (6) 2786 1320
E: jbullw@microsoft.com
www.microsoft.com

Jeff Bullwinkel is based in Amsterdam and oversees Microsoft's corporate, external and legal affairs team across Europe. This includes supporting commercial transactions and providing regulatory counsel to business groups, as well as contributing to public policy discussions on issues relating to privacy, cyber security, artificial intelligence, competition, intellectual property rights and international trade.

Gerald Reddig
Global Product Marketing, Security, Nokia Software
T: +49 (17) 0632 3498
E: gerald.reddig@nokia.com
www.nokia.com

Gerald Reddig leads the global portfolio marketing efforts for Nokia Software's security solutions. He is a member of the broadband forum, directs Nokia's membership in the IoT Cybersecurity Alliance and steers Nokia's security centre in Finland. He is on the speaker's circuit at international conferences and is a recognised author on the topics he is passionate about: cyber security technology, data privacy and finding the right solutions to prevent vulnerabilities, hacker trojans or man-in-the-middle attacks.

Robert J. Hanna
Partner, Tucker Ellis LLP
T: +1 (216) 696 3463
E: robert.hanna@tuckerellis.com
www.tuckerellis.com

Rob Hanna is a trial lawyer with broad experience in all aspects of business litigation. He chairs the Privacy & Data Security practice group at Tucker Ellis LLP. He concentrates a significant portion of his practice on unfair competition claims, fiduciary duty claims, non-competition agreements, trade secret and other business related torts. He is also experienced in matters involving data security breaches, notification laws and class actions.

FW: How would you characterise the extent of the cyber risks currently facing businesses, organisations and governments across the globe? In your experience, which sectors and industries appear to be particularly vulnerable to cyber attacks, or at least persistent targets for malicious actors?

Hanna: In an era where almost all businesses heavily rely on technology, the cyber risks facing businesses are greater than ever before. The protection of valuable business data against theft and misuse has become a critical management issue. With an increasing amount of a business's assets migrating online, business data is in itself an attractive target for cyber misuse. The education, finance and healthcare industries remain constant targets for cyber criminals. According to the Identity Theft Resource Center's 2017 Annual Report, these industries accounted for 40.2 percent of breaches last year. Now, however, we see that hackers have shifted focus towards service industries – such as hotels – and those industries relying on third-party or outsourced internet providers. This is largely the result of ill-managed or non-existent control measures, outdated policies and weak third-party agreements.

Lanois: Cyber security is becoming an increasingly important issue for businesses, organisations and governments, as evidenced by the fact that data breaches are now regularly making the headlines. There has been extensive media coverage of the devastating effects of attacks such as 'WannaCry', 'NotPetya' or 'Locky'. In addition, regulators have warned that data breaches will lead to increased scrutiny and higher fines. If we take a look at the targets of attacks by malicious actors, it appears that the landscape is very diverse. Companies such as Target, Home Depot, Sony Pictures Entertainment, Sony PlayStation Network, Hilton Hotels, Anthem, Equifax, Uber, Yahoo, Tesco, Ashley Madison and Chipotle have all been victims of cyber attacks, thus showing that no industry or sector is spared.

Bullwinkel: If not anticipated and mitigated, cyber security risks can be significant. Many sectors are vulnerable, and no sector is invulnerable. But the sectors most frequently attacked are often those that store sensitive personal information, particularly financial information, relating to large numbers of people. Any organisation that has large numbers of records about individuals should know it is a target and should operate under the principle of 'assumed breach'. Additionally, there has been an increase in nation-state attacks that appear aimed at the critical infrastructure of other nations, with the apparent aim of disrupting, or at least having the ability to disrupt, the operation of nuclear power plants, electrical grids or water supplies. 'NotPetya' and 'WannaCry' are prominent examples of that.

Lehmann: It is widely known that today any business has to face up to the possibility of cyber attacks. The 'WannaCry' and 'Petya' incidents made it abundantly clear that there is no kind or area of business that is so unattractive to criminals that these businesses could feel safe or at least a little safer from cyber attack. Those kinds of business where security has played an insignificant role in the past or where business procedures pose difficulties when usual safety measures have to be integrated are the most vulnerable. One example is the healthcare sector where, particularly in hospitals, numbers of different kinds and versions of software are running, lots of different kinds of hardware are being operated and emergencies are the rule. Logistics providers are also vulnerable. The current trend requires an ever higher level of cross-linking so that providers which offer varying degrees of cyber security provisions are all connected to one hub. Anyone who manages to attack the hub successfully will then have access to all the businesses linked to it.

Reddig: Most companies already assume that they will be breached. What sets companies apart is how quickly they can respond to those breaches. If and when a breach happens, the best companies want to be able to say that they responded and were back online in a matter of hours, as opposed to weeks. The reality today is that the number of security incidents is so high that only 30 percent of incidents get investigated. Of those 30 percent, 70 percent are false positives. As a result, 54 percent of incidents that should get investigated do not. Today, communication service providers and organisations managing mission-critical networks, including transportation, utilities and healthcare, have the most vulnerable networks and are the most persistently targeted.

Gu: The cyber risks are growing consistently for businesses, organisations and governments. Currently, cyber attacks are becoming more centralised, professional and sophisticated. Ransomware is increasingly targeting the manufacturing industry, financial institutions and pharmaceutical companies. Largely, there are no weak industries, only organisations with weak security provisions.

FW: How should these risks be identified, analysed and evaluated so that appropriate security measures can be implemented?

Lanois: The starting point would be identifying the organisation's assets, in order to understand what may be of interest to hackers and adopt appropriate security measures. Organisations also need to keep a close eye on social or technological changes and trends, not only to help them identify new opportunities and communications channels to interact with their customer base, but also to identify how technologies can and are being used by others. For example, the rise of social media has created new ways for companies to engage with their customers, however it can also facilitate social engineering and identity theft. One of the key ways to reduce risks is by raising awareness of security issues, at all levels within companies.

Bullwinkel: A significant portion of risk management can be accomplished through the enhanced security that may come through the adoption of enterprise-

grade cloud services. For major cloud providers, cyber security needs to be a core competency and these service providers have the ability to make far greater investments in this area than any single enterprise. Plus, when you are leveraging cloud services you are generally running the very latest software that is up-to-date, with a wide range of security measures already implemented.

Lehmann: The first step would be to evaluate the hardware and software being operated at the moment, as well as where the data flows are and the areas of potential systems access. Then, it would be important to assess whether there are 'open doors' that could be closed and whether and how it might be possible to get the hardware and software to a certain level. After that, staff must be trained on using the new hardware and software properly.

Reddig: Security management requires end-to-end visibility across the device, network and cloud layers. Without the ability to collect, correlate and analyse data from multiple operational silos, it is probable that security threats will be missed. For instance, an Internet of Things (IoT) device may be performing its intended function and still be exfiltrating data. If the device is only monitoring the IoT gateway for anomalies, this breach will likely be undetected, unless the connectivity network itself is also monitored for indicators of data leakage. Multi-dimensional security analytics that correlate data from multiple domains and sources help identify anomalies that might be suspicious, malicious or inadvertent, and provide context intelligence regarding the nature of the threat, the threat vectors used, and the associated business risk and the recommended mitigation steps.

Gu: First, companies need to integrate risk management models into corporate governance. Companies need to build a risk register that reflects their specific risks. A clearly defined risk appetite helps them to adopt different approaches and to carry out proactive actions, for example deterrence and prevention control. Companies need to follow the risk management methodology to build comprehensive risk identification, risk evaluation, risk response and risk monitoring procedures.

Hanna: Identifying, analysing and evaluating cyber risk is tedious. Worse, these actions do not generate revenue. Staying on top of the 'state of the art' measures requires diligence, rigorous attention and effective management at the most senior levels of a business, and it needs to be done much more than just once a year. But more than half of businesses neglect updating cyber security policies. Providing constant attention to risk assessment and knowing where your risks are requires effort. Often, a business will learn the hard way of its most important asset to protect. Although the immediate direct cost of a breach may be small, the long-term losses can include fines, lawsuits, poor public image and loss of consumer trust.

> "STAYING ON TOP OF THE 'STATE OF THE ART' MEASURES REQUIRES DILIGENCE, RIGOROUS ATTENTION AND EFFECTIVE MANAGEMENT AT THE MOST SENIOR LEVELS OF A BUSINESS, AND IT NEEDS TO BE DONE MUCH MORE THAN JUST ONCE A YEAR."
>
> ROBERT J. HANNA
> Tucker Ellis LLP

FW: To what extent do different types of risk require companies to adopt different cyber security strategies? How should an entity go about ensuring that the cyber security controls it chooses are appropriate to the risks it faces?

Bullwinkel: It is a truism that different types of risk require different types of defensive strategies. A more specific idea is that defensive measures should be proportionate in cost to the potential harm that may be suffered through a data breach and the likelihood of that breach actually occurring. These two factors can move in opposite directions. For example, the destruction of your corporate data centre by an asteroid dropping out of the sky would certainly be far more devastating than the leak of a spreadsheet listing the salaries of all your employees. But such a disaster is orders of magnitude less likely to occur than the leak of a spreadsheet, and orders of magnitude more expensive to defend against. So, you should probably not move your data centre to an underground cave. But you should devote a lot of attention to verifying that all of your sensitive spreadsheets are encrypted and that access to them is strictly limited by a strong role-based user authentication system.

Lehmann: Naturally, the kind of safety strategy a company chooses depends on the nature of the business. If we are talking about an internet store, for example, then it is not possible to reduce the connection to the internet or the volume of internet traffic. In such instances it is not possible to implement security measures that

slow down the traffic because customers are used to immediate responses from shopping websites. The only option is to make the website as secure as possible so that would-be hackers are unable to find a loophole. Also, companies must have redundant systems that could take over in case of emergencies so that no traffic or data is lost. By contrast, a business that is not dependent on the permanent flow of data might be advised to reduce traffic down to just the essential and channel it through one particularly secure access point. So any business would have to identify how much openness to traffic it needs and then tailor its strategy, either by reducing the flow of traffic, or by acquiring the means to maintain its business even in the event of a successful attack.

> SECURITY OPERATIONS WORKFLOW AUTOMATION AND ORCHESTRATION ARE AT THE HEART OF THE TRANSITION FROM A STATIC DEFENCE TO AN AGILE AND ADAPTIVE RESPONSE.
>
> GERALD REDDIG
> Nokia Software

Reddig: Security operations workflow automation and orchestration are at the heart of the transition from a static defence to an agile and adaptive response. Automation is the process of executing repeatable actions without human intervention, while orchestration chains these automated tasks into executed playbooks to perform workflows that accelerate both investigation and mitigation.

Hanna: No one-size-fits-all solution exists. Some organisations, such as financial institutions and healthcare providers, have regulatory concerns in addition to business concerns that need to be addressed. According to ISACA International, only 38 percent of global organisations claim they are prepared to handle a sophisticated attack. To ensure that controls are appropriate, businesses should take the following steps. First, conduct a full risk assessment and identify where data comes from, where it is stored and who has access to it. Second, keep track of both internal and external threats, and consider what types of cyber crimes threaten your business and how they are typically carried out. Third, identify where your systems are most vulnerable and determine the impact of threats and how likely they are to occur. This includes vetting outside vendors and partners. Finally, prioritise risks and start resolving them, by implementing an IT protocol, recovery plan, and ongoing and regular training and education about security threats.

Gu: Every company should have a sound incident response plan (IRP). The best approach is to check the risk register to prepare the response plan. From minor to critical incidents, we need to prepare a red-button emergency plan if there is a catastrophic incident or a breach which damages the company's valuable data.

Lanois: Any risk assessment process should begin with the development of an operational framework that fits the size, scope and complexity of the organisation, taking into account the organisation's business needs and goals. There is no one-size-fits-all process. Of course, every organisation needs secure systems, but finding the right cyber security strategy will depend on the organisation's nature and requirements. In addition, certain organisations, such as those handling financial or healthcare information, need to comply with additional regulatory requirements which should be addressed in the organisation's cyber security framework.

FW: In your experience, considering the extent of the cyber risks facing companies, are boards and senior management allocation sufficient resources to addressing the issue?

Lehmann: Generally, boards are allocating sufficient resources, given that the number of widespread attacks and the media coverage of incidents like the 'WannaCry' virus and the implementation of the General Data Protection Regulation (GDPR) have served to generate a high level of awareness. Senior management and boards of directors know that a successful attack will not only harm their business but they might face serious and even ruinous claims by their companies if they failed to achieve an appropriate level of security. Therefore, reasonable businesses currently have no problem allocating sufficient resources.

Reddig: A cyber attack can affect the very ability of an organisation to fulfil its mandate. At best, security breaches are a costly distraction from core business activities. At worst, they can lead to catastrophic failure. In between, there is a broad range of business impacts which threaten operations, production capabilities, customer and employee data, liability exposure and intellectual property, any one of which could jeopardise business continuity and integrity. The potential for reputational damage – in the market, among shareholders and with partners

– cannot be overstated. Yet, when boards and senior leadership are unaware of the wider context of risk exposure, they remain recklessly oblivious to the very hazards they should be identifying and mitigating. Rather than let risks escalate, the matter of cyber security must be propelled to the boardroom – only here can it take its rightful place as an essential part of the organisation's overall risk management strategy.

Gu: It is hard to say if boards and senior management always have sufficient resources available. But companies need to consider industry risk appetite, risk trends and external threat intelligences to help boards and senior management to allocate sufficient resources to handle risk responses and maintain cyber risks at an acceptable level.

Lanois: Companies can invest heavily in top-of-the-line software and state-of the-art systems, but if there is a lack of resources dedicated to security awareness within the organisation, all of these efforts will be for naught. It is crucial for the tone to be set at the top in order to demonstrate that the board and C-suite care about building and maintaining an effective cyber security risk management programme. One way to achieve this is to establish a cross-organisational team which would be a forum to discuss, coordinate and communicate on cyber security issues.

Hanna: Most boards and senior managers are aware of the general need for increased cyber security, although they have very little idea what that means, how to go about implementing it and how much the different options cost. For that matter, one of the biggest concerns is that you can never know if you are completely secure. Proper cyber security requires constant vigilance and maintenance of system. So in the absence of a clear solution to 'the cyber security problem', boards and senior managers are frequently reluctant to take any action, lest it be inadequate. This puts a business between a rock and a hard place.

Bullwinkel: It is increasingly clear to business leaders that cyber security is a boardroom-level issue, and, as a result, we are seeing greater attention and increasing investment in this area. Providing sufficient budget, staff talent and management time to cyber security is clearly an indispensable first step. But it is also important not to fall into the trap of believing that allocating resources alone is enough to guarantee safety from cyber attack. Organisational culture and individual behaviour are as important as money and technology in fighting cyber attackers. The reality is that most major data breaches begin with avoidable mistakes by well-intentioned users.

> "IT IS INCREASINGLY CLEAR TO BUSINESS LEADERS THAT CYBER SECURITY IS A BOARDROOM-LEVEL ISSUE, AND, AS A RESULT, WE ARE SEEING GREATER ATTENTION AND INCREASING INVESTMENT IN THIS AREA."
>
> JEFF BULLWINKEL
> Microsoft Europe

FW: Generally speaking, do the IT systems operated by business, organisations and governments require significant reconfiguration to cope with the breadth of the cyber risks that exist today? How significant are the cost implications?

Lanois: As vulnerabilities are discovered in existing software and systems, it is crucial to always keep up and install the latest software updates and patches. For example, in the UK, the National Audit Office's official investigation into the WannaCry outbreak found that "all organisations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves", since the WannaCry ransomware relied on a vulnerability in the Windows code which had already been fixed via a software patch. The same investigation found that "whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded organisations against infection".

Hanna: Information technology is a technical component of an entity's operations. Most business leaders who are not involved in IT know very little about IT. Ultimately, IT leaders must be given leeway to address cyber security risks. Yes, cyber security costs money, resources and capital. But costs cannot be measured in a vacuum. To determine the cost of anything, ask 'what is the alternative?' In this case, what if you do not protect your IT systems from cyber attacks? What if the entire system goes down and is unrecoverable, or if 50 of your employees receive ransomware to which they have to pay $50,000 each or their files will be destroyed? Address those questions and you have your answer to the significance of the cost implications.

Bullwinkel: The most important thing is to correctly execute on the fundamental

security measures that you already know you should be doing. A very common mistake is for an IT organisation to fall behind in applying security patches to critical software. This can sometimes be a burdensome and thankless task, and it costs money too because it is labour intensive and it sometimes means you also need to upgrade your software or hardware. But it is absolutely imperative that all patches be applied promptly and that you keep your software and hardware up-to-date. It is really striking how many of the biggest and worst data breaches in history have been directly caused by failure to patch.

> "THERE IS THE OBVIOUS NEED TO FIND NEW WAYS OF RUNNING LARGE NETWORKS SO THAT SECURITY MEASURES COVER THE WHOLE NETWORK AND THAT EVERY SINGLE DEVICE IS AS SECURE AS THE WHOLE SYSTEM."
>
> DR JOCHEN LEHMANN
> GÖRG

Gu: All IT systems operated by businesses, organisations and governments should be compliant with local regulations, international standards and industry best practices. The cost of safeguarding and implementing countermeasures must effectively reflect the business merits, whether tangible or intangible.

Reddig: Over one third of companies are not even looking at their internet-facing security posture – often the lowest hanging fruit for attackers. Global organisations have the added complexity of managing cyber security across regions or sectors with different standards, leading to conflict and inconsistencies. Similarly, different enterprise units may also have security frameworks that collide or compete, as is so often the case in entities created through mergers and acquisitions. The potential for cyber crime to strike a fatal blow has never been greater. Fast-growing and increasingly complex threats driven by external or internal adversaries are only exacerbated by systemic gaps. An entirely new approach to understanding organisational cyber security is needed to stay ahead of today's hackers.

Lehmann: Given the number of successful attacks in the recent past, there is the obvious need to find new ways of running large networks so that security measures cover the whole network and that every single device is as secure as the whole system. The same applies to businesses that are connected to one system. The key is the strict rules applied by central security management, as well as the same level of security being applied across the board, although this might result in a significant loss of convenience. Then the users have to be trained more intensively and have to be given strict and easy to comply with rules, without exception. On the whole, the costs are considerable but unavoidable, not the least due to the GDPR.

FW: In your opinion, how important is it to screen and risk assess vendors and other third parties to eliminate cyber vulnerabilities in the supply chain? What recommendations would you make in this regard?

Gu: It is vital that companies screen and risk assess all vendors and third parties. As ISO 27001 indicates, supplier service delivery management is to maintain an agreed level of information security and service delivery, in line with supplier management. Through this procedure, companies can eliminate potential cyber vulnerabilities in the supply chain.

Bullwinkel: The nature of the screening you need to do of your supply chain will depend on your line of business. A manufacturer of complex equipment that incorporates sophisticated components or software from dozens or hundreds of independent suppliers scattered around the globe will need to devote substantial resources and management attention to its screening programme. A large financial institution may not have such a big physical supply chain, but it likely uses a lot of outside software, and of course it uses devices such as ATMs or smart phones. In all these cases, a key principle is to be careful when selecting your master vendors, those of your suppliers who integrate the products of many other sub-vendors.

Hanna: Although businesses wish otherwise, they are responsible for the data they put in the hands of their vendors and third-party service providers. Now more than ever, proper screening processes are essential components of any cyber security plan, especially with the proliferation of cloud-based providers. The first priority should be to identify the information each vendor and third-party service provider may have access to – understanding that the levels of access will allow a business to properly craft and prioritise screening measures for each vendor. Such measures can include reviewing the vendors' own cyber security protocols, breach history and insurance coverage.

Reddig: One important pillar in cyber security is a strong identity access management strategy that can isolate,

monitor and record all privileged sessions to help enterprises and their partners meet GDPR accountability, notification and reporting requirements. It will also improve their overall security posture by enabling them to protect critical corporate data, such as financial information, contracts and legal documents.

Lehmann: Screening third parties is essential for two reasons. First, businesses with a secure IT landscape are frequently attacked through their suppliers, rather than directly. So, more attention has to be given to suppliers and their level of cyber security. Second, Article 25 of the GDPR requires data controllers to implement data protection through the technical means they employ. However, that would require suppliers to be able to deliver GDPR-compliant software and hardware, and that seems to be problem. Anyone who has tried to get confirmation from a supplier that its product is GDPR-compliant knows this.

Lanois: It is no longer sufficient, in today's globally connected world, for an organisation to only protect its own network. It is crucial to ensure that the networks used by third-party vendors are also secured, since these may be used as an entry point by hackers. For example, a 2015 attack affecting a large fast food restaurant chain was conducted through the login credentials of a third-party service provider, gaining the hackers access to the point-of-sale system used by over a thousand restaurants of the franchise and customers' debit and credit card information.

FW: Should an entity find itself the victim of a cyber attack, what general steps need to be taken at the outset and on an ongoing basis to manage the fallout?

Bullwinkel: You need to have a well thought out plan and you need to make sure that all the key participants in the plan understand it and can play their part without mistakes or hesitation. You need a crisis response team that includes your security people, your IT people and your legal and compliance staff, as well as public relations and marketing. You need to promptly address the concerns of all stakeholders, which includes regulators and customers, but may also include employees or business partners. But perhaps the most important thing of all, and this can be a very difficult idea to accept, is that you must assume you will one day be breached. Thinking that 'it cannot happen here' is the most dangerous possible way to operate.

> IT IS NO LONGER SUFFICIENT, IN TODAY'S GLOBALLY CONNECTED WORLD, FOR AN ORGANISATION TO ONLY PROTECT ITS OWN NETWORK.
>
> PAUL LANOIS
> Credit Suisse AG

Hanna: Businesses put themselves in the best position when they plan for a potential breach. This includes developing a written incident response plan setting forth who in the organisation will be responsible for the investigation and response, what types of incidents trigger the plan, what notification is required, and the process for engaging outside counsel, forensics experts, insurance carriers and, potentially, law enforcement. If you do not already know much of this information, you are late to the dance.

Reddig: Responsibility for business recovery after a breach is often unclear and frequently unrehearsed. This means executives are unaware of the commercial consequences that could cascade through their company during a cyber attack. Most CEOs have unrealistic expectations about how quickly breaches will be identified, let alone remediated. The lack of automation and orchestration within IT security means many boardrooms will be disappointed at their time of greatest need. Yet an investment of a few hours simulating the business decisions that will confront executives during a breach, can transform the board's appreciation of their IT resources. Leadership is required from the executives who recognise the threat to reputation and revenue that cyber attacks now pose. In particular, progressive leaders will invest in three areas: commercial simulations of breach response in the boardroom, security automation and orchestration, and independent scorecards of how hackers view the business.

Lehmann: The first step is not the identification of the culprit, but the mitigation of the effects. Malware has to be stopped from spreading. Systems not already infected have to be disconnected or shut down. Then companies must determine what is required to get the business running again. After that, the effects of the attack have to be assessed. And then the communications with the competent authorities and the public have to be prepared. Only then is it possible for companies to bring in forensic specialists who try to find the one responsible and to

find out what measures could be taken to prevent such an attack in the future.

Lanois: As soon as a cyber attack is identified, it is important to determine what damage – if any – has been caused, whether any data has been breached or leaked and whether any breach notification requirements have been triggered. Most states in the US require organisations to notify their customers, immediately or without unnecessary delay, if personal data has been exposed. Depending on the state, a notification sent to law enforcement, consumer reporting agencies and state attorney general or other regulators may also be required. In the European Union, the GDPR also requires organisations to communicate the data breach to customers "without undue delay" and to the regulator within 72 hours after having become aware of the data breach. Sanctions may be high if an organisation fails to disclose a data breach, including fines of up to €20m or up to 4 percent of the total worldwide annual turnover, whichever is higher.

Gu: When a company finds itself the victim or target of a cyber attack, generally the incident response stages are identification, containment, investigation, eradication, recovery and follow-up. First, the company needs to identify the actual incident. Once the scale of the incident is identified, the next move is to contain the issue. Then it must determine what actually happened to the system, computer or network. Eradication, whereby the company removes the threat from the computer, system or network, is the next step. A period of recovery will allow the company to return to business as normal. Finally, after everything has been returned to normal, the company should ensure that the process was sufficient and effective.

FW: If an entity does experience a data breach, how should the nature of the attack, and its impact, be communicated to stakeholders?

Hanna: Whenever a breach occurs, honesty is a priority for all communications. Fake news can be devastating. Few things can get a company into trouble quicker than providing misinformation regarding a breach. While it is important to get information out quickly, it is even more important to be right. From there, what facts are disclosed and how they are presented will depend on the audience, as levels of sophistication regarding cyber security will vary depending on who is receiving the message.

> "WHEN A COMPANY FINDS ITSELF THE VICTIM OR TARGET OF A CYBER ATTACK, GENERALLY THE INCIDENT RESPONSE STAGES ARE IDENTIFICATION, CONTAINMENT, INVESTIGATION, ERADICATION, RECOVERY AND FOLLOW-UP."
>
> GREAT GU
> AstraZeneca China

Lanois: How and when an organisation communicates a breach is critical. In the age of social media, organisations are under a lot of scrutiny and how the organisation responds can have a significant and long-term impact on its reputation. Misstatements and misinformation can generate confusion and mistrust from consumers and cause more harm. In addition, informing consumers as soon as possible allows them to take steps to protect themselves and can help prevent damage to the organisation's reputation.

Reddig: A customised commercial response plan, prepared in advance of a major data breach, will make the response much more timely and effective. It provides directors with simple checklists, templates and instructions about each of the decisions they must face. Crucially, it will document where sensitive data is held, including information held by third-party suppliers and information processors, so that breaches caused by partners are considered during the initial forensic stage of a response. The plan must be easy for executives to use. A section for each designated executive should be provided, highlighting the resources they can call upon, the consequences of alternative actions they must choose between, and even the text of communications they may need to urgently issue.

Lehmann: Communicating a breach depends on who the stakeholders are. As to the owners of the business, it seems to be most important to communicate the impact on the business and the possible loss of turnover. However, one could also consider the customers as stakeholders in data breaches too. Customers should be informed fairly and truthfully, particularly about whether there is any danger to their interests. Finally, the data protection authorities must be informed, as legally prescribed.

Gu: Regarding data breaches, we need to get a clear understanding of the jurisdiction of data protection and privacy protection laws. For example, under the GDPR, when a personal data breach has occurred, the controller should alert the supervisory authority of the breach without undue delay, no later than 72 hours after the

event. The controller should notify a data subject when there has been a personal data breach, where that breach is likely to result in a high risk to the rights and freedoms of the person, without undue delay.

Bullwinkel: The most important thing is to tell the truth and do it quickly. Past experience in large data breaches shows that the longer senior leaders delay telling stakeholders the truth, the more damaging the fallout is for the organisation. Of course, there may be some critical technical details that you disclose only to law enforcement or regulators, because disclosing that information publicly might help the hackers or others like them. But it is a mistake to withhold details simply because they are embarrassing. The reality is that if you suffer a major breach involving sensitive data relating to a large number of individuals, you have got a responsibility to address and remediate the problem as well as you can and as quickly as you can.

FW: What steps should a company take to monitor and review cyber threats in order to detect any changes and maintain an overview of security management processes?

Reddig: CEOs and their boards need to know that their enterprise security is being managed effectively. With the rapid growth of new attacks, this requires an investment in security automation and orchestration. Good investments in this area help companies identify, understand and recover from cyber attacks.

Lehmann: Companies should keep up with the news from government agencies, such as the German Federal Office for Information Security. That office always publishes the latest information on viruses and other threats. Then there should be a central body in the business, at the managerial level, whose task it is to regularly monitor the latest developments and which has the power and the budget to adapt the business strategy and structure to such developments. Also, it is necessary to instruct the company's staff to report any new developments and any new problems that may occur within the usual process of business.

Hanna: The first step in effective security management is to fully understand a business's data and how it is created, received, stored and transmitted. Knowing vulnerabilities to that data and implementing a plan to address the identified risks are key steps. Once all this is up and running, the use of threat intelligence is a significant way businesses can monitor and review existing and new cyber threats specific to their industry. Information sharing and analysis centres (ISACS) have been formed to provide industry members with opportunities to share threat information and collaborate on responses.

Gu: A company should proactively set up a security operations centre (SOC) or security information and event management (SIEM) solution to provide sufficient monitoring and searching capability to prevent and detect cyber attacks caused by cyber threats, and through SOC or SIEM solutions to maintain a suitable security level with enhancement of security management processes.

Bullwinkel: You cannot guarantee you will never be breached. But you can set up your defences in such a way that your chances of detecting breaches swiftly and shutting them down before they inflict major damage are high. For example, you can encrypt your sensitive files. You can restrict access rights of users to the strictly necessary. You can constantly scan your network for signs of breach. And if fraudsters do breach your defences and steal sensitive data, you can take measures to limit the damage they can do.

Lanois: Since the threat environment is always changing, it is important to continually monitor and review the risk environment in order to ensure that the security management process is still relevant and up to date. In order to do that, specific objectives of the security programme should be defined so that measures can be developed and monitored to gauge performance over time. All organisations should also regularly conduct vulnerability scanning and penetration testing in order to test the security configuration and identify, among others, weak security configurations or missing system security patches. A penetration test is an authorised, simulated attack which is performed to evaluate the security of the system. The results of vulnerability scanning and penetration testing will enable the organisation to identify security gaps.

FW: What essential piece of advice would you offer to companies when it comes to managing their cyber risk and security policies and procedures in today's business world?

Lehmann: It is essential that companies and their management take cyber risks and the rules of the GDPR seriously and review their whole business process with regard to data security, even at the management level. Without the right tone from the top, without a sufficient budget and without the willingness to change or at least amend routine procedures, management will achieve less than the desired results because the company will end up with partial security and will also fail to convince staff, which is crucial for any security system because people will always remain the greatest risk.

Gu: My advice would be to focus on protecting core data and assets, based on your risk management procedure. Remember, cyber security is not only dealing with hackers, it also requires companies to deal with business barriers and cultural ambiguities.

Bullwinkel: An important piece of advice is to adopt multi-factor authentication (MFA) and require that everyone in your organisation uses it. The passwords that we have become used to – long strings of upper and lower case letters and numbers with a few odd symbols thrown in – do not represent the future. Substantially greater security can be achieved through MFA

using biometrics and public key encryption. The idea is that we should no longer make users type in a password or phrase that is sent over the network to be compared with the user's password stored on a server. Instead, we use public key encryption to allow the server to verify the identity of the user's device cryptographically, and then use a biometric like a fingerprint or face scan, perhaps in combination with a simple password like a PIN, to prove the user's identity to the local device.

Lanois: The biggest threat often comes from within the organisation, so it is crucial for organisations to regularly conduct awareness training with employees in relation to cyber risks, including the risks associated with phishing attacks and fraudulent email solicitations.

Hanna: Cyber security is always evolving and changing. To effectively manage risk, businesses cannot rest on their laurels – they must remain vigilant. Businesses need to be aware that new vulnerabilities present themselves anytime the organisation adopts new technology, software or applications, or begins to collect data or contracts with new vendors. As part of their continuing risk assessment and management efforts, businesses should conduct regular audits of their information security procedures and controls.

Reddig: Multi-dimensional IoT security analytics are key to the rapid detection of threats. Machine learning helps identify anomalous behaviours that indicate a compromise by using threat intelligence information across the network, device and cloud layers. When infused with contextual knowledge about the IoT service and business value, an appropriate automated rapid response can be initiated. By leveraging security orchestration, analytics and response technologies, organisations can scale to meet the increasing challenges IoT creates while creating new value-added monetisation opportunities.

FW: To what extent are legal and regulatory imperatives driving companies to evolve their cyber security strategies? Do you expect this dynamic to increase over the months and years ahead?

Reddig: The GDPR aims to protect Europeans from privacy and data breaches. It covers all data that can be directly or indirectly linked to an individual. All organisations that process or control the personal data of EU citizens will face heavy fines – €20m or 4 percent of global turnover, whichever is greater – if they fail to comply with the GDPR when it takes effect on 25 May 2018. Organisations can take important steps toward GDPR compliance by deploying solutions that enable them carry out a number of functions. The first allows companies to monitor identity and access to privileged accounts and establish individual accountability by requiring users to 'check out' shared account credentials. The second function is to assess environmental risks and distinguish between normal and abnormal user and entity behaviour. The third function is the ability to generate audit logs that show exactly which people, applications or processes accessed personal data. The fourth function is to provide tamper-resistant audit logs and session recordings to demonstrate compliance.

Bullwinkel: Regulators and legislators around the world are responding to the internet era and its risks with new regulations and laws to protect data and personal privacy. This is a good and necessary development that is likely to increase, and it is also going to drive a lot of change in the way organisations approach cyber security. One of the most important examples of this trend is the GDPR, which is certainly the most important new data privacy law to come along in decades. We are just at the start of the GDPR era, and many details about how it will operate in practice remain to be worked out, but we are already seeing profound changes in the way organisations handle personal data in response to GDPR.

Lanois: The GDPR has attracted media attention and business awareness due to the increased fines. In addition, recent high profile data breaches, such as those which occurred at Equifax, Yahoo and Uber, have attracted scrutiny from both regulators and legislators, which could lead to additional legal and regulatory requirements being imposed.

Hanna: In the US, the impact of regulatory guidance on businesses can vary greatly depending on the relevant industry. Some industry regulations go into significant detail, whereas others can be quite vague, requiring nothing more than 'reasonable efforts' to safeguard data. The lack of a uniform standard is a source of great frustration. While there has been a longstanding push for greater guidance regarding what constitutes appropriate cyber security measures, it is unclear if regulators will ever be able to keep up with ever-changing technology and security risks.

Gu: Today, the legal and regulatory imperatives are driving companies to integrate their cyber security strategies. We can see them from the GDPR and the China Security Law. What we need to do is to utilise cyber security strategies to endow data protection abilities and privacy protection compliance. 2018 will be the year of cyber security due to the GDPR. Later on this year, more and more companies will be getting nervous about the cost and the preparation work required to be compliant with these laws.

Lehmann: Currently, regulatory imperatives are probably the main drivers. Without the threat of the rather draconian fines contained within the GDPR – up to €20m or 4 percent of the worldwide turnover of the group of companies, whichever is larger. The security issue, even with the experience gained from 'WannaCry' and 'Petya', would not have risen to the current level of prominence and would not have generated the allocation of considerable funds, not least because cyber security has become a compliance issue. This is all the more true for those businesses that operate critical infrastructure in Germany and are the object of scrutiny for the German Federal Office for Information Security. ■