RAPID7

Published by Financier Worldwide Ltd

ANNUAL REVIEW Reprint July 2019

Cyber Security & Risk Management

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

United Kingdom

MATTHIEU RIDER
Rapid7
International Engineering Director
+44 (0)118 3703530
mrider@rapid7.com

Matthieu Rider is a seasoned and passionate technology industry executive. He has spent the last 11 years helping organisations of all shapes and sizes defend against and learn from cyber attacks; firstly as Director of Strategic Support and Services at Sophos, and more recently as director of international engineering and spokesperson for Rapid7. His previous IT experience was at Microsoft where he played a vital role in architecting some of the firm's largest client deployments.

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?

RIDER: We are seeing a move away from ransomware as the attack *du jour*, to that of compromising individual's work email accounts, often due to password reuse. Our recent Industry Cyber Exposure Report found that organisations in every industry have serious issues with patch or version management of internet-facing systems. Keeping these kinds of outdated business-critical software packages connected to the internet can pose a serious risk for organisations of every size. In May, several UK organisations fell foul of attacks targeting the Microsoft SharePoint remote code vulnerability, though 2019 has yet to see anything comparable to any one of the high-profile, widespread attacks of recent years such as 'WannaCry', 'Heartbleed', 'Poodle', 'Shellshock', 'Meltdown' and 'Spectre'. Instead, the last six months have seen a swing toward stealthier attacks.

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?

RIDER: Every year, organisations are increasing their focus on cyber security. Encouragingly, security teams are working closer than ever with their colleagues in information technology (IT) and DevOps to reduce their attack surface and incident response times. While the European Union's (EU's) General Data Protection Regulation (GDPR) has helped drive the discussion at all levels, and board members are more informed than ever before, most organisations still lack the level of board participation and support needed. Cyber security is not a destination, it is an ever-evolving journey and it needs to be high on the agenda at every board meeting.

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?

RIDER: A third of UK organisations have reported making significant changes to their cyber security programmes as a result of the GDPR's implementation. This is extremely positive. Yet, compliance is no guarantee of security. The GDPR lens is focused on data and privacy, rather than security in its widest sense and it certainly has not changed attackers' behaviour in any way. Eighty-eight percent of the UK's FTSE 250-plus have weak or nonexistent anti-phishing defences in the public email configuration of their primary email domains. Additionally, secure sockets layer (SSL) and transport layer security (TLS) are not enforced on the primary websites of 19 percent of them, leaving their visitors open to a wide array of common and potentially devastating attacks.

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?

RIDER: First and foremost, companies must ensure that they are not an easy target. Hackers love low-hanging fruit. Companies should focus on the fundamentals: good anti-virus (AV) software, firewalling, vulnerability and patch management, and so on. They must also understand their data, people and processes. Look at them with an attacker's eyes: where are

the weaknesses? Companies must also implement a robust incident detection and response programme and test it regularly. Increasingly, this is being outsourced to a managed service provider which can be a far quicker and more cost-effective solution. UK organisations are primarily focused on compliance, rather than cyber security best practices, so if companies have these measures in place and know their security processes are good, they should consider implementing security orchestration, automation and response (SOAR) to increase efficiencies and free up valuable security experts for the more important and strategic tasks. The UK's National Cyber Security Centre (NCSC) has published a Board Toolkit to encourage essential cyber security discussions between boards and their technical experts.

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?

RIDER: The best response depends on a number of factors, many of which will be unique to particular industries, regulatory requirements and organisations. A firm's standard responses for varying severities and types of breach must be devised, tested and documented as part of its incident detection and response programme. However, we have never seen an organisation do well by trying to cover up a breach. Obviously, it is important that when a breach does occur firms do not rush a response, but communicate clearly, honestly and as frequently as appropriate during the initial period as the facts reveal themselves, keeping customers and partners as informed and as protected as possible. Remember, many organisations survive the direct consequences of a breach, only to be undone by the damage to their brand and the loss of customer loyalty.

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?

RIDER: One way to transfer financial risk is via a dedicated cyber security insurance policy. However, while this will provide for a portion of an organisation's direct and indirect financial losses to be covered, it will not include any compensation for damage to the organisation's brand, reputation or its customer and employee confidence. Additionally, cyber security insurance does not transfer or mitigate personal criminal liability imposed on the organisation's staff by compliance requirements. One thing that all organisations considering cyber liability insurance should be mindful of is whether they would even be covered after a breach. A key tenet of a well-run cyber security programme is the established governance policies and standards that must be followed by all employees, contractors and vendors. These policies are mandated with specificity by compliance obligations, insurance products and best practices. However, policy requirements will often not fully align with the actual capability of the information technology (IT) teams. If this is the case, and if the breach is the result of not following or being able to follow the established policy, then the insurance policy will not reimburse companies for any loss incurred. That puts the concept of risk transfer via insurance at odds with the real world complexities of managing a complex IT landscape and navigating the evolving threats presented to businesses worldwide. In summary, a business

> “Companies must implement a robust incident detection and response programme and test it regularly.”

can choose to transfer a portion of its financial risk to a cyber security insurance product, but must be mindful of what risks the product will protect against and what risks the company will continue to need to self-insure against. On the policy side, companies need to make sure that their policies meet the established requirements, but also that they are managing those policies and treating cyber risk thoughtfully so as not to be blindsided with denied policy claims.

Q. What are your predictions for cyber crime and data security in the UK over the coming years?

RIDER: As always, the greatest threat is the unknown: What will the hackers do next? Our belief is that building on the already extensive ‘businessifcation’ of hacking, such as published malware SDKs, automated malware quality assurance testing, and some stunning marketing efforts around fake AV, hackers and their paymasters will be investing heavily in AI to enable an explosion in malware creation and the crafting of sophisticated attacks; after all, quantity has a quality all of its own. The UK has always been good at prevention as a means of defence, yet if these same defences become overwhelmed due to the sheer volume of attacks, then our detection and critically our response need to be vastly improved. ■

www.rapid7.com

Rapid7 is advancing security with visibility, analytics and automation delivered through its Insight cloud. The firm’s solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behaviour, investigate and shut down attacks, and automate routine tasks. Over 7200 customers rely on Rapid7 technology, services and research to improve security outcomes and securely advance their organisations.

MATTHIEU RIDER
International Engineering Director
+44 (0)118 370 3530
mrider@rapid7.com