ankura

INDEPTH FEATURE Reprint April 2023

CYBER SECURITY & RISK MANAGEMENT

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

UNITED KINGDOM

Ankura Consulting Group, LLC

Respondents

RYAN RUBIN
Senior Managing Director
Ankura Consulting Group, LLC
+44 (0)20 7015 2385
ryan.rubin@ankura.com

Ryan Rubin is a senior managing director at Ankura, based in London, and leads the firm's EMEA cyber security and privacy practice. He brings over 26 years of global Big Four and boutique experience to help clients holistically manage complex cyber and privacy challenges from the boardroom to the network. He has collaborated with senior management and boards to address emerging cyber security threats and regulatory compliance matters. He has also supported companies across the cyber insurance ecosystem delivering global pre and post breach services with insurers, corporate and mid-market clients and brokers.

AHSAN QURESHI
Managing Director
Ankura Consulting Group, LLC
+44 (0)20 3882 0551
ahsan.qureshi@ankura.com

Ahsan Qureshi is a managing director in the cyber security team within the data and technology practice. He has over 15 years of experience in assisting organisations establish robust cyber security postures. He has led a number of strategic initiatives to advise on, build, review and enhance cyber security strategies and transformation programmes for organisations. He has extensive experience in delivering cyber maturity reviews, developing security control environments, and helping organisations develop cyber incident response and recovery capabilities. Prior to joining Ankura, he worked with a Big Four and a boutique global consulting firm and holds an MSc in information systems security.

Ankura Consulting Group, LLC

Q. In your opinion, what are the major cyber threats to which today's companies are vulnerable?

A. Ransomware remains the top threat to organisations in the UK. Indeed, we saw a resurgence of ransomware in Q1 2023. Attackers not only continue to encrypt valuable data and demand ransom payments for unlocking the data, they are also extorting victims to avoid publishing stolen data in the public domain – so called 'double extortion'. Phishing and social engineering remains another top threat due to the increased sophistication of the malicious campaigns that these threat actors use to trick users to divulge sensitive information or install malware. Companies also continue to suffer from poor cyber security hygiene. Even large enterprises suffer from a lack of effective security monitoring, a lack of patch management, a lack of multifactor authentication, ineffective security hardening and a lack of proper employee awareness programmes.

Q. Given the risks, do you believe companies in the UK are placing enough importance on cyber security? Are board members taking a proactive, hands-on approach to improving policies and processes?

A. The UK government's 2022 Cyber Security Breaches Survey reported senior management in eight out of 10 businesses made cyber security a high priority. The same survey reported that one-third of businesses have board members accountable for cyber security, however the percentage of companies that regularly update senior management on cyber security has declined over the last four years. We have noticed an increase in cyber security awareness at board level in the UK. Several high-profile breaches and Information Commissioner's Office (ICO) fines, along with a maturing cyber insurance market, are helping to drive this awareness forward. However, the key challenge is translating awareness into action. Elevating the role and responsibility of the chief information security officer (CISO) is key, as well as prioritising the right activities to address cyber security debt. Initiatives need to be more business risk driven rather than light touch, 'watered down tick box' compliance exercises or led by technology spend,

Ankura Consulting Group, LLC

and need more of a focused approach on driving improved business resilience.

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?

A. In recent years, the UK has been proactive in its approach to updating cyber security and privacy regulations protecting citizens, businesses and the digital economy. The UK Data Protection Act (DPA) and Network & Information Systems (NIS) Regulations marked turning points in safeguarding the personal data of UK citizens and improving the resilience of critical national infrastructure. UK regulators have stepped into more of a supervisory role with the authority to impose fines, require ongoing validation of an organisation's approach and overseeing mandatory incident reporting requirements. The equivalency of the UK General Data Protection Regulation (UK GDPR) and the EU GDPR was welcome, ensuring regional alignment continued post-Brexit. These changes have significantly impacted how UK companies report data breaches and cyber security incidents. Although they have put additional burdens on companies, requiring the implementation of additional security standards, they are also raising the 'acceptable cyber bar', making them more resilient against cyber threats.

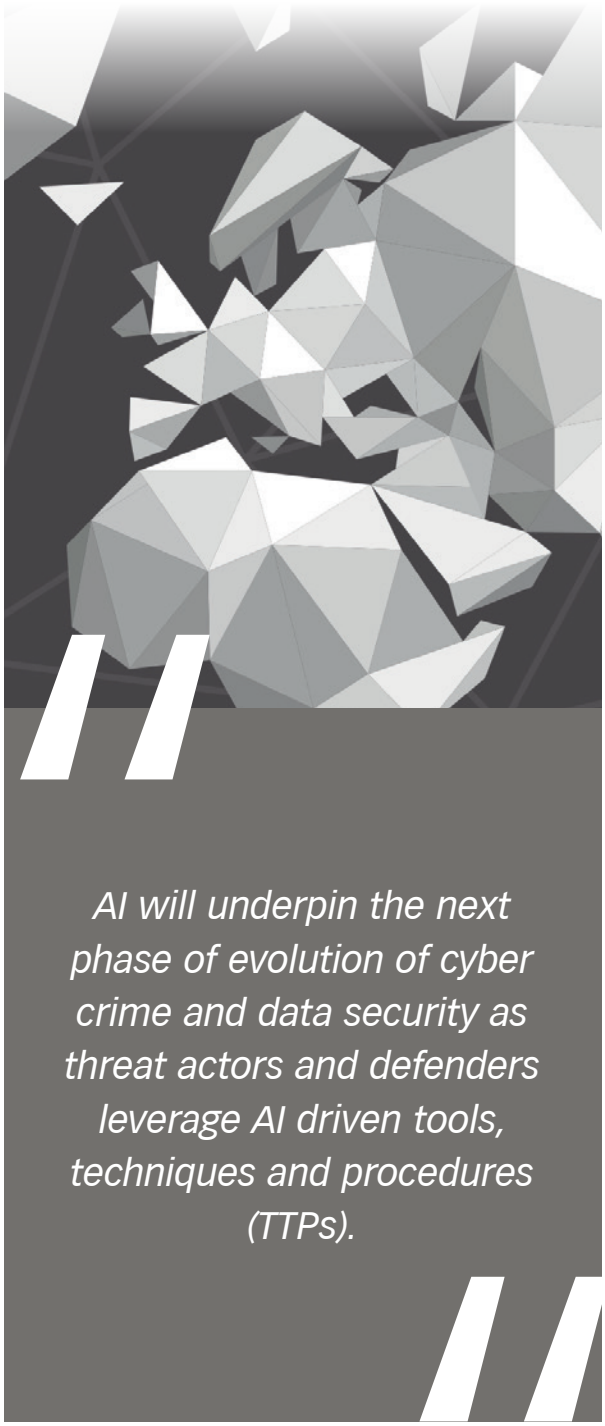
Q. In your experience, what steps should companies take to avoid potential cyber breaches – either from external sources such as hackers or internal sources such as rogue employees?

A. A comprehensive approach should be adopted to safeguard companies against cyber threats. Establishing a robust security strategy supported by a prioritised action plan and adopting a multilayered approach covering people, process and technology is key. To get ahead of the threat, we advocate companies carry out proactive monitoring and threat and vulnerability management programmes, helping to better understand exposure and identifying weak spots quicker so action can be taken to reduce risks on the horizon. Robust security hygiene should be implemented by actively monitoring for threats, updating, patching and hardening

technology. The use of endpoint protection and supporting processes, effective vulnerability management and multifactor authentication are critical to defending against weaknesses exploited by threat actors. Cyber awareness and employee training is also crucial, and often acts as the first line of defence. Following the principle of least privilege, segregation of duties and maintaining strict access controls is also important.

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?

A. Should a cyber incident occur, containment is a key priority, immediately following its identification, in order to minimise damage. This involves assembling a team that can assess the business risk and start isolating and disconnecting or shutting down affected systems. Experts should be engaged to conduct forensic analysis to determine the nature and extent of the breach. Companies that do not have these capabilities in-house should refer to



AI will underpin the next phase of evolution of cyber crime and data security as threat actors and defenders leverage AI driven tools, techniques and procedures (TTPs).

Ankura Consulting Group, LLC

specialist digital forensics and incident response (DFIR) firms immediately following a breach or should already have a retainer relationship with such a firm, so they can provide the right level of support quickly. DFIR firms assist with initial response and containment but also with forensic analysis, evidence preservation, threat intelligence and expert witness services should any legal matters arise. Early engagement with counsel and communications professionals is also critical as part of a well-rounded response, depending on the nature of the security 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?

A. To weather the storm of a cyber incident and its longer-term impact, cyber insurance is key. Insurers increasingly offer specialist services through their ecosystems. These include access to specialist DFIR and media and communication firms and incident handlers. This can help companies respond effectively to cyber security incidents. Cyber insurance and risk transfer offer a critical safety net to minimise the impact of an incident covering financial losses and offering specialist services and support. Dealing with the longer tail impact of an incident is where insurance truly comes into play. Cyber incidents lead to not only data loss but also business disruption resulting in financial losses, reputational damage, and legal and regulatory repercussions. Cyber insurance enables businesses to transfer some or all of these costs, providing coverage in various scenarios. However, policies are not always comprehensive and have exclusions that companies must be aware of.

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

A. We foresee a rapid shift in cyber crime due to increased digitalisation and technology advancement. These changes will require the adoption of ever more robust security measures. There are threats on the horizon as companies migrate their IT into the cloud. Many companies do not have in-house cloud skills and rely heavily on third parties but cannot

Ankura Consulting Group, LLC

assess the effectiveness of their own cloud security controls. Ransomware attacks will increase in sophistication with criminals requiring higher ransom payments. Threat actors will continue to take advantage of the rapid increase in adoption of cloud infrastructure and software as a service (SaaS) solutions, internet of things (IOT) and the 'API economy' to target companies and their supply chains. AI will underpin the next phase of evolution of cyber crime and data security as threat actors and defenders leverage AI driven tools, techniques and procedures (TTPs). In turn, this will put pressure on skills gaps which will likely make it harder to hire and retain cyber security specialists and defend against future threats. ❑

www.ankura.com

ANKURA CONSULTING GROUP, LLC is an independent global expert services and advisory firm that delivers end-to-end solutions to help clients at critical inflection points related to change, risk, disputes, finance, performance, distress and transformation. The Ankura team consists of more than 1800 professionals in over 35 offices globally who are leaders in their respective fields and areas of expertise. The firm's collaborative lateral thinking, experience, expertise and multidisciplinary capabilities drive results and Ankura is unrivalled in its ability to assist clients to protect, create and recover value.

RYAN RUBIN Senior Managing Director
+44 (0)20 7015 2385
ryan.rubin@ankura.com

AHSAN QURESHI Managing Director
+44 (0)20 3882 0551
ahsan.qureshi@ankura.com

ROBERT OLSEN Senior Managing Director
+1 (443) 948 6812
robert.olsen@ankura.com