Ryan Rubin is a senior managing director and Ahsan Qureshi is a managing director at Ankura. Mr Rubin can be contacted on +44 (0)20 7015 2385 or by email: ryan.rubin@ankura.com. Mr Qureshi can be contacted on +44 (0)20 3882 0551 or by email: ahsan.qureshi@ankura.com.

Published by Financier Worldwide Ltd

SPOTLIGHT REPRINT August 2023

Cyber security trends in 2023 and beyond

BY RYAN RUBIN AND AHSAN QURESHI

Technology continues to make remarkable advancements that enhance our lives. However, it also increases complexities in the risks we face to our digital-enhanced world. Given the relentless shifting threat landscape, the importance of robust cyber security resilience cannot be overstated.

From the increasing adoption of generative artificial intelligence (GenAI) and machine learning (ML) bolstering cyber security, to the challenges of obtaining insurance and maintaining adequate levels of staffing, this article casts a spotlight on key trends continuing to shape the market in 2023 and beyond.

GenAI and ML

GenAI and ML are wielding an unprecedented influence over cyber security. These technologies, while presenting tremendous potential for enhancing defence mechanisms, are simultaneously opening avenues for their own weaponisation.

Threat actors are already leveraging AI and ML to create malware and ransomware code to orchestrate basic cyber attacks – although rudimentary at this stage, they are an alarming precursor to future cyber warfare. Although AI tools and chatbot developers are making efforts to curb this emerging threat, malicious actors continue to adapt and identify exploitable loopholes.

As we look into the future, we expect the AI evolution to create more advanced and unpredictable cyber threats. To address these threats at machine speed, technologies and processes need to evolve and adapt as well. Automation and use of AI in decision making will rapidly detect anomalous behaviour and respond automatically to contain future threats.

The focus will be to reinforce technologies against the threats they were designed to counter, ensuring AI serves as a robust defence in our arsenal rather than being used to expose vulnerabilities.

Cloud technologies and zero trust

The shift toward cloud, coupled with the adoption of zero-trust frameworks, will continue to shape the cyber security landscape due to the increasing risk of cloud compromise and continued exposure of threats from within.

In early 2023, we observed cloud instances emerging as lucrative targets for threat actors, hacking cloud instances for data theft, crypto mining or to launch further cyber attacks. This highlights the critical need to implement comprehensive security measures, including zero trust, in cloud environments and on-premise to mitigate these evolving threats.

The zero-trust model, built on the principle of 'never trust, always verify', significantly reduces the ability of hackers to move laterally within networks and systems. We continue to observe ransomware threat actors successfully moving laterally once they gain a foothold into a network. We envisage organisations will increasingly align their security policies with established zero-trust frameworks, like the National Institute of Standards and Technology (NIST) zero-trust architecture, using them as a blueprint for securing their digital assets.

Cloud adoption and new security tools

As organisations migrate to cloud infrastructures, the necessity for investment in new, specialised security tools is becoming a prevalent trend. However, the adoption of these essential tools is lagging behind the pace of adoption, creating vulnerabilities during the transition from on-premise to the cloud.

Successful migration is driving the need for not only sophisticated tools but also cloud platform specific expertise to ensure a seamless and secure transition and ongoing security. For instance, Microsoft's Azure has gained significant traction, leading many organisations to opt for a comprehensive Microsoft security tool stack.

Despite these advancements, shortcomings in security monitoring, hygiene and logging in cloud deployments are still common. To close security gaps, organisations need to secure their cloud infrastructures with robust security measures and consistent monitoring. This ensures they embrace the cloud's efficiency and scalability without compromising on security.

Regulatory enforcement

The regulatory focus on enforcement has been another crucial trend shaping the cyber security landscape in 2023. This trend has been particularly prevalent in the US, where significant enforcement actions have been undertaken within the first five months of the year.

Simultaneously, data privacy laws are rapidly expanding across multiple states, exemplified by the California Consumer Privacy Act (CCPA). Moreover, data privacy laws in countries such as China, India and Saudi Arabia continue to evolve, leveraging European Union (EU) General Data Protection Regulation (GDPR) principles.

Europe is tightening cyber security regulations, introducing the Digital Operational Resilience Act (DORA), amending the EU Cyber Security Act and replacing the Network & Information Systems (NIS) Directive with NIS2.

These revisions aim to expand in-scope industries, such as managed security services, to help regulate the supply chain, and producers of hardware and software products and internet of things (IoT) devices to safeguard the EU ecosystem. DORA also introduces new requirements for penetration testing, cyber security providers and incident reporting.

These developments underscore the global regulatory trend toward greater transparency and accountability for cyber security across industries and the supply chain.

Consolidating cyber security and privacy programmes

The integration of cyber security, privacy and data governance programmes as well as integration of IoT, operational technology and IT remains a focus. Organisations are increasingly realising the value of consolidating these programmes under one umbrella, often with chief information security officers (CISOs) now taking on data protection, operational resilience and data governance responsibilities.

However, there are still gaps in good practices relating to governing data management as well as operational technology (where appropriate) that need to be addressed to reduce the impact of ransomware attacks. Ransomware investigations continue to uncover alarming deficiencies in data retention housekeeping and segregation between IT and OT. It is not uncommon to find organisations with poor network segregation as well as those who are unaware of data exfiltration activity or lack robust data retention policies and controls, which dramatically increases the impact of a breach. The absence of comprehensive risk assessments, network segregation, accurate data inventories and effective data system discovery mechanisms remains a significant concern.

These challenges underscore the importance of a holistic approach, integrating all digital technologies and adopting strong data governance practices to ensure not just the security, but the accountability, integrity and privacy of data across all operational processes to properly futureproof cyber posture.

From prevention to rapid response

The cyber security paradigm is experiencing a significant shift from a traditional prevention-centric approach to one focusing on rapid detection, response and overall resilience. This change is being positively reinforced by insurance carriers that reward organisations which demonstrate robust detection mechanisms and resilience strategies.

Extended detection and response is rising to the forefront of this trend, effectively becoming the new multifactor authentication in terms of its indispensability. Its ability to rapidly detect and respond to cyber threats significantly raises the bar for security standards. In addition, insurers and brokers are considering the introduction of pre-breach proactive services to boost resilience and overall readiness against cyber attacks.

As we move forward, the focus will remain on enhancing rapid detection capabilities and overall resilience, not just for direct benefit but also for the insurance advantages they present.

Obtaining cyber insurance

Another trend that continues in 2023 is the ongoing challenge for organisations to secure cyber insurance, at an appropriate coverage level, as carriers tighten their underwriting requirements and expand their coverage exclusions and restrictions.

This is a result of the increasing complexity and frequency of cyber attacks, requiring a more cautious approach to underwriting. However, this challenging environment has also resulted in innovation within the insurance market. New entrants are devising fresh ways to assess risk

and offer insurance, creating alternative pathways to coverage.

These new approaches include offering policies with lower barriers to entry at reduced coverage levels or adopting shared risk models. These provide flexible options for organisations to secure the necessary coverage, adding a new dimension to the relationship between cyber security and the insurance industry.

Staffing challenges

Addressing cyber security staffing levels continues to be a challenge in 2023. Although the surge in layoffs in the US has led to an influx of qualified candidates, this trend is not mirrored globally, resulting in a persistent shortage of skilled cyber professionals in other regions.

As a response, companies are increasingly leaning on managed service providers to mitigate the impacts of staff attrition and maintain effective security operations. Moreover, the industry is on the cusp of a disruptive wave driven by AI, especially in key cyber security disciplines.

AI tools can automate and streamline tasks such as malware analysis, penetration testing and general operations within cloud technologies. By leveraging these advances, organisations will be able to alleviate some of the cyber personnel shortages, particularly around security operations centres and incident response teams.

The focus of threat actors

An observable trend in 2023 has been the resurgence of threat actors (e.g., BlackCat, Black Basta and CI0p) refocusing their attention on European and US entities more consistently. This shift has been particularly noticeable since March 2023, with ransomware attacks making a strong comeback.

Threat actors are diversifying their methods, employing new attack vectors to gain unauthorised access to companies beyond the traditionally used spear-phishing. These novel tactics include 'malvertising', the use of 'stealer logs' and leveraging access brokers. They are also escalating their attacks through triple extortion strategies including engaging directly with victims to add further pressure on them.

Additionally, vulnerabilities in VMWare, on-premise Microsoft exchange systems, software such as MOVEit, and as well as 'sys dev' attacks, are increasingly exploited, contributing to the rise in security breaches – often global in nature and requiring a global response.

In this evolving threat landscape, cyber security teams must remain vigilant and responsive, adapting their strategies and toolsets to the changing tactics and focus of these threat actors. This readiness is essential to protect the integrity of our digital spaces.

Consolidation of the cyber security vendor space

As 2023 unfolds, we have started to witness increased consolidation within the cyber security vendor space, both in the realm of tools and services. The recent pullback in venture capital funding for security tools will further drive this trend, resulting in decreased valuations for many vendors. This, coupled with resultant financial constraints, will make consolidation not just probable but, in many cases, inevitable.

However, consolidation could streamline the cyber security market, reducing fragmentation and potentially leading to more robust, comprehensive solutions. We anticipate that the long-term implications could yield stronger, more integrated cyber security solutions, better equipped to protect organisations against evolving threats.

Summary

2023 is turning out to be another interesting year for cyber security and data privacy professionals. The double-edged sword of exciting digital technology enhancements and advancement in the fields of cloud, AI and IoT will bring new risks and opportunities to all. Adopting a cyber-resilient approach will help those looking to take advantage of the benefits this evolution brings while minimising the potential downside risks that arise from it.