Cybersecurity in Saudi Arabia: Threats, Compliance and Risk Management

Post-Event Report: SBJBC x CRMG Cyber Series Webinar 8 September 2024

By Robert McNamara, SBJBC Research Officer

Preface

This scene setting webinar will be repeated on Thursday, 2nd October 2025. If you missed the first edition then please consider registering to better understand the cyber landscape in Saudi Arabia and why knowledge of cyber regulations, compliance, and security is more important than ever. Registration can be completed through the events page on SBJBC's website.

If you or your company are interested in learning more about the cyber space and the steps that can be taken to ensure compliance and security, then contact CRMG through the links in the webpage of this article.

Summary

The Saudi British Joint Business Council (SBJBC), in partnership with Cyber Risk Management Group (CRMG), hosted the first in a series of cybersecurity webinars on 8 September 2024. The session provided a comprehensive overview of the cyber threat landscape, with particular focus on Saudi Arabia's regulatory environment and the importance of risk-based approaches to cybersecurity management.

CRMG, a specialist cybersecurity consultancy focused on cyber risk management and regulatory compliance, brings extensive experience in helping organisations navigate complex cybersecurity challenges. The company works across the Middle East and globally, providing services ranging from risk assessments to compliance frameworks implementation.

Robert McNamara, SBJBC Research Officer, opened the session and introduced the speakers. Simon Rycroft (Co-Founder and CEO, CRMG) and Tom Everard (Director, CRMG) shared their professional backgrounds before outlining the non-technical, governance, and people focused nature of the discussion.

The Current Threat Landscape

Simon Rycroft, CEO of CRMG, opened the session by describing how phishing remains the predominant cyber-attack vector globally, followed by impersonation, social engineering, and malware deployment. These attack methods are interconnected; phishing emails often serve as the initial access point for ransomware attacks. According to UK Cyber Breaches Survey data referenced, organisations face a complex web of threats where human error plays a significant role.

Ransomware has emerged as the primary concern for most organisations. The World Economic Forum reports that businesses worry most about operational disruption from cyber-attacks. Rycroft noted that ransomware has become increasingly commoditised. Many criminal organisations now operate with surprising professionalism, ensuring that victims who pay receive assistance in recovering their

systems. One organisation reported being connected to a professional help desk after paying a ransom, receiving step-by-step guidance to reinstate their systems.

The economic impact can prove severe. Rycroft noted that a considerable proportion of small businesses hit by ransomware or other attacks will cease operations within two years, which while an anecdotal point, underscores the existential threat cyber-attacks pose to smaller organisations. Rycroft also cautioned against over-interpreting individual statistics, noting that methodologies differ. Instead, organisations should focus on overall trends.

Saudi Arabia's Unique Risk Factors

Six factors amplify cyber threats in Saudi Arabia. First, the pace of change driven by Vision 2030 and projects like NEOM creates extensive digitisation opportunities but simultaneously expands the attack surface. Rapid technological innovation, while essential for economic transformation, introduces vulnerabilities that threat actors exploit. Entities such as the Saudi Data and Artificial Intelligence Authority (SDAIA) play a critical role in both enabling and regulating digitisation.

Second, Saudi Arabia's leading role in global energy markets makes it an attractive target for state-sponsored actors seeking to cause economic disruption. Third, the kingdom's wealth, both organisational and individual, attracts financially motivated criminals targeting high-value ransomware payments and fraud schemes. Cyber awareness and security should be a paramount concern for family offices in particular, as they professionalise and expand their operations.

Fourth, Saudi Arabia's geopolitical position influences the threat landscape differently than in Europe or North America. While European organisations primarily face threats from Russia, China, and North Korea, Saudi organisations must particularly consider threats originating from China and regional actors. Fifth, the kingdom's geographic position creates physical vulnerabilities. The recent cable cutting incident under the Red Sea, likely by Houthi forces, disrupted Microsoft Azure services across the region.

Sixth, cloud service restrictions add complexity. Certain Saudi organisations face limitations on where they can access cloud-hosted services. While Azure and AWS are establishing presence in Saudi Arabia, many services currently route through other GCC countries, particularly the UAE, opening them up to third party risks.

The Human Factor in Cybersecurity

Tom Everard, Director at CRMG, emphasised that human elements remain cybersecurity's "soft underbelly." For two decades, organisations have invested heavily in technological defences whilst underinvesting in people-focused security measures. Verizon's 2023 report estimated that 74 per cent of all cyber breaches involved human error, while Mimecast raised this figure to 95 per cent.

This human dimension extends beyond malicious attacks. Accidental events cause as much cyber-related impact as deliberate attacks. Rycroft described witnessing an organisation's payment systems fail for three hours because staff deployed a critical patch during peak operational hours. The unintended consequences of change represent a substantial cyber threat that organisations often overlook.

Supply chain risks compound these challenges. Even organisations with strong internal security practices remain vulnerable through their suppliers and partners. The recent Marks & Spencer cyber incident originated through an IT supplier via social engineering. Poor security practices anywhere in the supply chain can impact organisations throughout the entire chain. Best practice requires understanding third-party relationships' importance, classifying them by criticality, and applying

appropriate scrutiny levels. For particularly critical suppliers, organisations should demand contractual rights to audit cybersecurity arrangements.

Regulatory Landscape in Saudi Arabia

Saudi Arabia has developed a comprehensive cybersecurity regulatory framework. The National Cybersecurity Authority (NCA) released the Essential Cybersecurity Controls (ECC) in 2018, with an updated English version published in July 2025. The ECC serves as the hub of Saudi cybersecurity regulation, containing nearly 200 individual controls covering baseline cybersecurity practices.

Currently, the ECC is mandatory for governmental entities and organisations involved in delivering or hosting national critical infrastructure, including banking, food production, and energy sectors. However, Saudi authorities strongly encourage all organisations to comply, and the implementation remit will likely expand over time.

Beyond the ECC, the NCA has developed a suite of related standards. The Teleworking Cybersecurity Controls (TCC) address remote working security. The Organisational Social Media Cybersecurity Controls (OSMACC) govern social media usage. The Cloud Cybersecurity Controls (CCC) split between controls for cloud service consumers and providers. The Critical System Cybersecurity Controls (CSCC) apply to particularly important systems. The Data Cybersecurity Controls (DCC) focus on data protection. The Operational Technology Cybersecurity Controls (OTCC) address operational technology connected to digitised systems (e.g. in manufacturing and production environments).

Together, these standards contain approaching 700 individual controls. Additional regulations include the Personal Data Protection Law (PDPL), the Saudi Arabian Monetary Authority (SAMA) Cybersecurity Framework, and the Capital Markets Authority Cybersecurity Guidelines. These regulations overlap significantly, expressing fundamentally similar disciplines but sometimes using different terminology.

This regulatory complexity creates challenges. Organisations attempting to comply with multiple regulations separately risk organisational paralysis. CRMG advocates for a harmonised approach using a common control framework that aligns with multiple regulations simultaneously. This orchestrated approach reduces compliance burden whilst ensuring comprehensive coverage.

Risk Management Approaches

In addition to complying with regulation, effective cybersecurity must be aligned with the cyber risk profile of the organisation, including an understanding of both the impact and probability related to potential adverse cyber events. Risk assessment follows a logical process: determining asset criticality across operational, financial, reputational, and regulatory dimensions; identifying relevant cyber threats using established threat taxonomies; mapping appropriate controls to mitigate identified threats; assessing current control implementation; and calculating residual risk. This then equips the organisation to make pragmatic decisions about cyber risk treatment. It should be noted that the NCA Essential Cybersecurity Controls require that a risk management approach such as this should be implemented.

This risk-based approach helps organisations focus resources effectively. Rather than attempting to implement every possible security control, organisations can prioritise based on their specific risk profile. Tom Everard stressed that risk management does not create additional work but helps organisations do the most important things well. Rycroft illustrates this with a metaphor of navigating

puddles, potholes, and chasms, highlighting how organisations must balance probability and impact when allocating resources.

Heat maps remain the most prevalent risk visualisation tool because boards understand them intuitively. By plotting threats based on impact and likelihood, organisations can overlay risk appetite lines to identify which risks require immediate attention versus those that can be accepted temporarily. The process enables creation of credible risk registers based on structured assessment rather than subjective judgment. Too many organisations populate risk registers through informal assessment, undermining their value for decision-making.

Artificial Intelligence Considerations

AI presents a double-edged sword for cybersecurity. It enhances defensive capabilities, particularly in security operations centres where AI excels at identifying attack patterns invisible to human analysts. However, AI simultaneously amplifies threats through enhanced deepfakes, sophisticated phishing attacks, and automated malware generation.

Rycroft advised evaluating AI deployment through a criticality lens. For operationally critical activities, organisations should either avoid AI entirely or apply extensive scrutiny and stress testing. For less critical applications, various technical and procedural controls can mitigate risks.

Key AI risks include data poisoning, where corrupted training data produces unreliable outputs, and ethical bias, where AI systems perpetuate or amplify existing prejudices. The principle of "garbage in, garbage out" applies strongly to AI systems. Organisations must assure input data quality and understand why AI produces specific outputs.

The EU AI Act currently leads global AI regulation, taking a risk-based approach that many countries are voluntarily adopting as the de facto standard. Saudi Arabia will likely follow this regulatory trend.

Practical Implementation

Effective cybersecurity extends far beyond technology. It requires board-level recognition that cyber risk management is a whole-business activity, not merely an IT concern. Boards need appropriate information and reporting to make informed risk treatment decisions. Regulators increasingly require boards to demonstrate cyber risk oversight capabilities.

Baseline technical protections remain essential. These include business continuity planning, employee lifecycle management (ensuring appropriate access rights for joiners, movers, and leavers), information classification, privileged access management, vulnerability management, and supplier assurance. However, these technical controls must operate within a broader framework encompassing governance, culture, and process.

The human dimension requires particular attention. Security awareness programmes, while sometimes viewed sceptically, prove essential in combating phishing and social engineering. Modern approaches can measure security behaviours, tracking how people interact with systems and whether they follow secure processes. This data-driven approach moves beyond traditional awareness training towards measurable behaviour change.

Future Webinars and Engagement

This webinar established baseline understanding across the cybersecurity landscape. Subsequent sessions will explore compliance and risk management in greater detail. CRMG will also be talking

during a workshop at the British Embassy in Riyadh on 14 October 2025, providing hands-on exploration of these concepts.

The session demonstrated that while Saudi Arabia faces similar cyber threats to other nations, unique factors amplify certain risks. The kingdom's rapid digitalisation, economic importance, and geopolitical position create a complex threat environment. Concurrently, comprehensive but overlapping regulations require careful navigation.

Success requires balancing compliance with risk management, technical controls with human factors, and innovation with security. Organisations must move beyond viewing cybersecurity as purely technical, embracing it as a fundamental business risk requiring holistic management approaches. Rycroft concluded that cybersecurity must be treated as a holistic business risk, not just an IT issue.