An overview and update

This article discusses recent updates to cybersecurity regulation in the Kingdom of Saudi Arabia.

As part of the Saudi Vision 2030, the Kingdom of Saudi Arabia (KSA) has stated its intentions to diversify its economy away from its current reliance on oil and to develop public service sectors such as health, education, infrastructure, recreation and tourism. Underpinning this initiative is an increased focus on technology, digital transformation and the development of digital infrastructure. As such, the state is acutely aware of the cybersecurity threat it will face as its economy becomes increasingly digitalised.

The National Cybersecurity Authority (NCA) has been established as the body responsible for matters pertaining to cybersecurity in KSA. Although individual entities remain responsible for their own cybersecurity (as confirmed with regards to government entities in Royal Order number 57231 dated 10/11/1439 H), government entities (and their affiliates) and private companies providing critical national infrastructure (as described below) are now also required to comply with the NCA’s essential cybersecurity controls (the Controls).

Additionally, Government entities (and their affiliates) must implement an information security policy in line with the framework provided by the Communications and Information Technology Commission (CITC), the telecoms regulator, which also has the mandate to develop information security policies and guidelines (including minimum requirements) to assist Government agencies in KSA to manage their information security risks.

Following the recent developments, it is useful to take stock and consider the current position of cybersecurity in KSA. The applicability of the legislation and guidelines in this area is dependent on the nature of the entity involved: of relevance are the Anti-Cyber Crime Law (the Cyber Crime Law), the NCA’s whitepaper on Essential Cybersecurity Controls (ECC -1 : 2018) (the Whitepaper), The Controls of the Use of Computers and Information Networks in Government Entities (Government Mandate number (81) - 191430/3/H) (Government Mandate), the Information Security Policies and Procedures Development Framework for Government Agencies (the Framework), the National Cybersecurity Authority legislation (“NCA Legislation”) and the Royal Order number 57231 dated 10/11/1439 H (Royal Order). Additional sector specific guidance also makes up the regulatory fabric which is noteworthy for cybersecurity compliance in KSA, for example in the banking sector, the SAMA Cyber Security Framework (the SAMA Framework) must be considered.
Affected actors
Cyber Crime Law: applies to any person who commits a cybercrime in KSA, as detailed in the Cyber Crime Law. The offences listed are considered criminal offences and may be punishable by a fine or imprisonment (both of which vary depending on the nature of the offence). Whilst the Cyber Crime Law sets out the types of actions that would constitute a cybercrime and the sanctions that are associated with those actions, it does not enforce any specific actions that persons should take in order to be in compliance with the Cyber Crime Law.

Government entities (and their affiliates)
Government entities (and their affiliates) must comply with the Cyber Crime Law, the Controls, the Government Mandate and the Framework (if they are regulated by the Saudi Arabian Monetary Authority (SAMA) then they will also be subject to the SAMA Framework, see below).

- Cyber Crime Law: as stated above, every person in KSA - including government entities (and their affiliates) - are subject to the Cyber Crime Law.

- Whitepaper:
  - The cybersecurity Controls listed in the Whitepaper represent the minimum standards with which the relevant organisations must comply.
  - Not all Controls are applicable to all relevant organisations: The Controls framework consists of 5 main domains, 29 subdomains and 114 controls. The applicability of this framework depends on the nature of the business activities that the relevant organisation is carrying out. For example, an organisation that has deployed a cloud hosted solution, would be subject to the Controls subdomain 4.2 (Cloud Computing and Hosting Cybersecurity). There is currently no guidance on how organisations should self-assess as to whether they are subject to a particular Controls or not.
  - There is still some uncertainty as to how the NCA will assess compliance with the Controls, notably, there is currently no guidance as to what the NCA's assessment and compliance tool or field visits (both discussed briefly in the Whitepaper) will consist of, nor is the list of assessment methods stated to be complete at this stage. However, it is clear that self-assessment against the Controls will be a significant part of the compliance framework. Organisations that are subject to the Controls should note that the NCA will update (and provide notifications of such updates) the Controls on a periodic basis and cybersecurity policies should therefore be amended in line with such updates where relevant.
  - The Controls stated in the Whitepaper include numerous steps that organisations must take to comply with the requirements of the NCA. These requirements are divided between cybersecurity governance, cybersecurity defence, cybersecurity resilience, third-party and cloud computing, and industrial control systems cybersecurity, the full extent of these requirements are stated in Whitepaper, but it is useful to particularly highlight the following:
    - A cybersecurity administration must be set up and this must be independent from the ICT/IT function (pursuant to Royal Order number 37140 dated 14/8/1438 H). The posts of cybersecurity administration chairman and other supervisory and critical positions must be held by KSA nationals, who are highly competent in the field of cybersecurity (Controls 1-2-1 and 1-2-2).
    - Any cybersecurity operations or monitoring services that are performed by third parties through remote access must be provided from a location in KSA (Controls 4-1-3).
    - The hosting and storage of any of an entity’s information or technical assets must be within KSA (Control 4-2-3).

- Government Mandate:
  - The Government Mandate establishes that government entities must develop an information security programme. This programme must include an information security policy and procedures document that include policies on risk assessment, property management, information access and security incidents. The full details of how this programme should be
implemented are outlined in the Framework (clause 2.1). Whilst “government entities” are not defined in the Government Mandate, it seems reasonable to assume – based on the remit of the Framework (to Government Agencies) – that this is limited to direct government departments and their affiliates.

- Of particular note in the Government Mandate is the requirement that the websites of government entities must either be hosted by that government entity themselves, by another government entity or by a hosting service provider that is licensed by CITC and located in the KSA.

  - Framework: provides structure of how the information security programme required of government entities under the Government Mandate should be implemented in practice.

**Private entities providing critical national infrastructure**

Critical national infrastructure is defined as “infrastructure whose loss or susceptibility to security violations may result in significant negative impact on the availability, integration or delivery of basic services or may have a significant impact on national security, national defence, the KSA economy or KSA national capabilities”. Whilst the Whitepaper does not expressly state what is considered to constitute a “significant negative impact” or a “significant impact”, the concept of critical infrastructure is a common feature of cybersecurity laws in developed jurisdictions and so, to the extent that it is unclear in KSA, this is one of the many areas where equivalent concepts from other jurisdictions could help establish a sensible point of reference.

- Private entities providing critical national must comply with the Cyber Crime Law and the Controls (both as described above).

**Financial institutions**

Organisations affiliated with SAMA (this includes all banks, insurance companies, reinsurance companies, finance companies, credit bureaus and all Saudi financial market infrastructure that are regulated by SAMA) must comply with the SAMA Framework.

- The requirements are broadly similar to those under the Controls, such as the need to establish a cybersecurity function and a cybersecurity strategy. It is therefore likely that organisations affiliated with SAMA, which are now also within the remit of the Controls (i.e., they are government entities, their affiliates or private entities providing critical national infrastructure), will - at least to some degree - already be in compliance with many of the Controls.

- Notably, the cybersecurity function must be led by a Chief Information Security Officer who is a KSA national and sufficiently qualified for the role.

- Financial institutions that are subject to the SAMA Framework will also be subject to Cyber Crime Law and may, depending on their nature and/or service provision, be subject to the Controls.

**Other**

Organisations that are not either government entities (or their affiliates) or providing critical national infrastructure, are not currently required to adhere to the Controls (note, however, that they may still be subject to sector-specific rules such as the SAMA Framework). However, the NCA has stated that such organisations are nonetheless strongly encouraged to do so. It will therefore be a commercial decision as to whether these organisations decide to adopt compliant controls at this stage or wait to see if they are obligated to do so in the future.
Some outstanding questions

Despite the increasing interaction that the KSA has been pursuing with cybersecurity, there remain a number of questions that remain unanswered, such as:

1. Besides complying with the Controls, Royal Order 57231 dated 10/11/1439 H states that “[we] shall be requested to enhance [our] cybersecurity measures in order to protect [our] systems, and electronic data” - how will we know if what we have done is sufficient (and what is the penalty if it is not)? Are there guidelines to assist organisations in assessing which Controls they are obliged to comply with?

2. What is the Assessment and Compliance tool? What does it test? How does it do this?

3. How regular are the “periodical reviews” of the Controls? And what will they consist of?

4. How can organisations contact the NCA with ad hoc queries regarding the adequacy of their cybersecurity strategies?

To discuss the underlying trends and practical risk mitigation/compliance strategies for business in KSA and other gulf states, please contact Raza Rizvi, Nick Roudev or Ben Lyons.