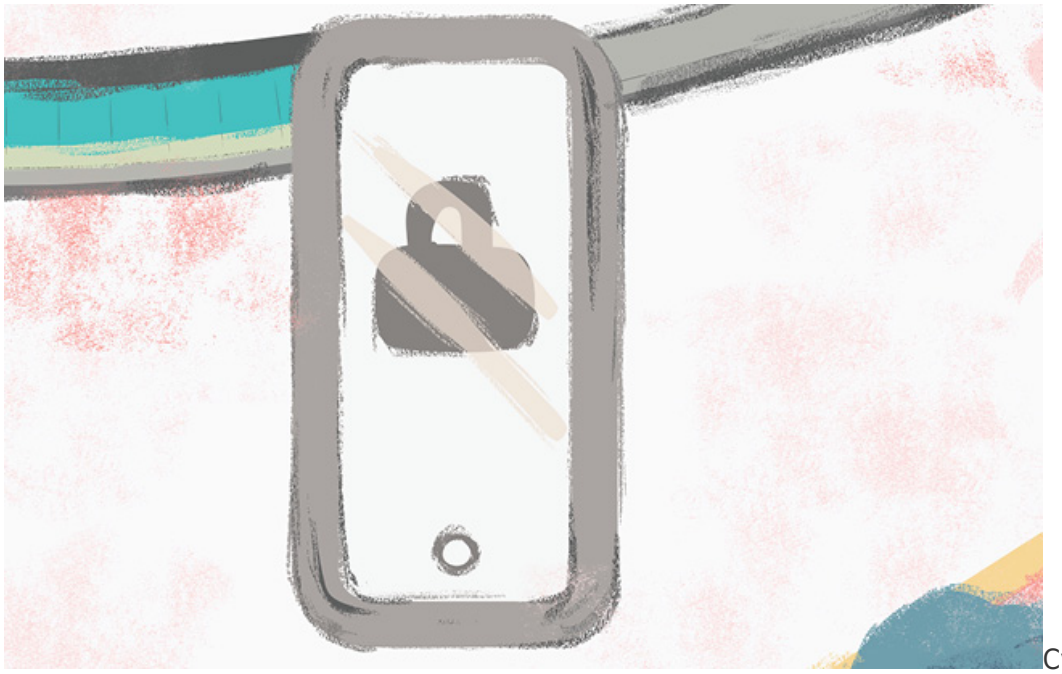
Cyberabia: Developments in the Cybersecurity Regulatory Landscape in Saudi Arabia

Amy Land-Pejoska - Associate - Digital & Data - Riyadh

Zil Ur Rehman - Senior Associate - Digital & Data - Riyadh



Cybersecurity can be summarised as the use of technology, and other measures, to ensure the safety of data and computer systems from incidents, both accidental and deliberate, that might compromise their integrity. For businesses, cybersecurity is of increasing importance. Besides the operational impact of a cybersecurity incident, such incidents can result in legal liability, reputational damage and financial loss. The urgent need to counter cybersecurity threats has resulted in greater measures being adopted by legislators and regulators around the world, and the situation in Saudi Arabia is no different.

In 2018, Saudi Arabia's National Cybersecurity Authority ('NCA') issued guidelines in the form of Essential Cybersecurity Controls ('ECC'). In 2019, the local telecoms regulator, the Communication and Information Technology Commission ('CITC'), proposed a cybersecurity framework, the Cybersecurity Regulatory Framework ('CFR') for the Information Communications and Technology Sector ('draft CRF'), aimed primarily at the telecommunications industry.

This article outlines the NCA's ECC, and the proposed CRF for the Information Communications and Technology Sector.

NCA'S Essential Cybersecurity Controls

The 'NCA Regulation' (the Regulation of the National Cybersecurity Authority, approved by Royal Decree No. 6801 dated 11/2/1439H (31 October 2017)) sets out the key features and responsibilities of the NCA.

These include:

- preparing a national cybersecurity strategy and supervising its implementation;
- developing and circulating policies, frameworks and standards for cybersecurity implementation, risk management, incident response and encryption, and supervising their implementation; and
- building, supervising and operating national and sectoral cybersecurity operation centres and platforms with the capability to command, control, investigate, monitor and exchange information and analysis on cybersecurity in the Kingdom.

In 2018, the NCA published the ECC the minimum cybersecurity requirements for Saudi government organisations (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organisations owning, operating or hosting critical national infrastructure. The NCA encourages all other organisations in Saudi Arabia to utilise the ECCs to improve their cybersecurity.

The ECCs consist of 114 cybersecurity controls, linked to national and international regulatory requirements, structured into five main domains, comprising:

- cybersecurity governance;
- cybersecurity defence;
- cybersecurity resilience;
- third party and cloud computing cybersecurity; and
- industrial control systems cybersecurity

Cybersecurity Governance

The ECC's governance requirements contemplate the development and implementation of a cybersecurity strategy that contributes to compliance with relevant laws and regulations. They set out the personnel, processes and other steps that organisations, that are subject to the ECCs, need to put in place to achieve effective cybersecurity.

Cybersecurity roles and responsibilities are to be set out clearly and kept up to date. Cybersecurity is to be managed with the support of an 'organisation head', delegated to oversee the organisation's cybersecurity strategy. Cybersecurity policies and procedures are to be adopted, supported by technical security standards and kept up to date. A risk management process is to be documented and implemented at key risk points and reviewed as necessary.

Project and change management present a cybersecurity risk for organisations. The ECCs require the adoption of cybersecurity policies and procedures relating to these activities. Personnel can also represent a significant risk to cybersecurity. Protocols to ensure that these risks are managed must be in place. Examples include employee vetting and cybersecurity awareness and training.

Finally, the ECCs require organisations to have a system in place so that cybersecurity controls are reviewed and audited.

Cybersecurity Defence

Organisations subject to the ECCs need to have physical security and other measures in place to protect their information and technology assets from various threats. As a preliminary step, an inventory of all IT assets should be kept. Only authorised personnel should access information as required to perform their roles and access to other information should be restricted. Unauthorised access should be prevented by having systems to log on and establish credentials.

Organisations are required to take measures to protect information systems against cyber risks. As well as protecting workstations, devices and careful handling of external storage media, the email service and external web applications need to be protected appropriately. Various minimum requirements to manage the security of an organisation's network are mandated. The use of mobile devices and employees' own devices pose their own additional cybersecurity risks, and the organisation must define and implement cybersecurity requirements including minimum controls as set out in the ECCs.

Data and information are to be classified and protected accordingly. Encryption is to be used in line with the organisation's policies and relevant laws, and measures must be in place relating to back-up and recovery. This extends to measures to detect vulnerabilities and conduct penetration testing.

Cybersecurity events are to be logged and analysed, while systems to identify incidents and mitigate their effects must be in place.

Cybersecurity Resilience

Cybersecurity resilience aspects of the ECC's main controls contemplate the incorporation of cybersecurity resiliency requirements into business continuity processes, thus minimising the impact of cybersecurity incidents on systems, data processing facilities and critical services.

Third-Party and Cloud Computing Cybersecurity

In terms of third-party risks, the ECC's main controls are focussed on issues relating to outsourcing and managed services, including the need to ensure that outsourcing and managed services follow organisational policies and procedures, as well as related laws and regulations.

With regard to cloud computing, the focus is on protecting cloud-hosted data and IT assets, as well as those processed or managed by third parties. For entities subject to the ECCs, the ECCs contemplate some degree of localisation, in that data hosting and storage sites need to be located in the Kingdom.

Industrial Control System Cybersecurity

Entities subject to the ECCs are required to ensure that industrial control systems are managed appropriately to protect the confidentiality, integrity and availability of their assets against unauthorised access and destruction.

Proposed Cybersecurity Standards For ICT Service Providers

In May 2019, the CITC invited feedback on its draft Cybersecurity Regulatory Framework for the Information Communications and Technology Sector. The draft CRF sets out requirements to increase effectiveness in cybersecurity risk management in line with international best practices. The draft CRF would apply to all service providers licensed by the CITC (i.e. any person licensed by the CITC who either provides a telecommunications service to the public, operates a telecommunications network used by such person or by another person to provide a telecommunications service to the public, or both) their affiliates, staff, related third parties and customers.

The draft CRF contemplates CITC setting security targets by defining compliance levels pursuant to a risk

based approach. Each level comprises a set of cybersecurity controls of varying complexity. Fulfilment of the preceding requirements will be necessary to achieve the next level of cybersecurity compliance. The draft CRF contemplates service providers being classified according to criticality in order to determine the applicable target compliance levels:

- Level One will comprise basic security controls;
- Level Two is to set out advanced requirements, in addition to the Level One requirements; and
- Level Three is to include requirements focusing on efficiency monitoring and continuous improvement to the Level One and Level Two controls.

Service Providers' Obligations

The essential responsibilities of licensed service providers include measures to be undertaken in the areas of governance, asset management, cybersecurity risk management, logical security, physical security and third party security.

Governance

- Licensed service providers are required to:
- adopt appropriate strategies and roadmaps to help achieve the compliance requirements;
- implement the CRF requirements and ensure the compliance targets specified by the CITC are met;
- undertake independent cybersecurity audits to measure compliance;
- train staff and personnel to ensure necessary qualification and skill;
- promote awareness among customers;
- fulfil reporting obligations through self-assessment or as requested by the CITC; and
- provide information to and co-operate with the CITC as and when required.

Asset Management

Licensed service providers are required to:

- maintain up-to-date asset inventories of all information assets;
- classify such assets and adopt a risk-based protection approach;
- appropriately manage personnel devices;
- prepare and enforce acceptable use policies of information assets; and
- establish proper disposal methods for information assets.

Cybersecurity Risk Management:

Licensed service providers are required to prepare and enforce an appropriate cybersecurity risk assessment approach; and an appropriate approach to monitor and treat cybersecurity risk.

Logical Security

The draft CRF sets out obligations applicable to licensed service providers in developing software applications. These obligations include fulfilling the following requirements:

- implementing appropriate encryption techniques to ensure confidentiality, integrity, authentication and non-repudiation of information at all times;
- taking appropriate measures to prevent unauthorised and accidental modification to information;
- identifying vulnerabilities and prescribing remedial actions;
- ensuring time constraints are met in applying security patches;
- ensuring protection of their networks from malicious threats and building resilience;

- effectively monitoring event logs for suspicious activities;
- properly managing access rights;
- maintaining an authorised list of software applications;
- increasing effective response to cybersecurity breach events and minimising their impact;
- preventing the spread of malware;
- ensuring information recovery; and
- conducting penetration tests to assess defensive capabilities.

Physical Security

Licensed service providers will need to protect their information assets against physical damage and threats, manage physical access to facilities hosting such assets, address any environmental threats to such assets, and extend the same protection to such assets located outside their premises.

Third Party Security

The draft CRF proposes making it mandatory for licensed service providers to require third party cloud service providers and third party outsourced service providers to adopt the cybersecurity requirements stipulated by the CITC.

CITC's Role

Pursuant to the draft CRF, the CITC will have the overall role of the regulator and will be empowered to monitor and enforce compliance of the stipulated requirements. For such purposes, it may undertake inspections of service provider facilities, carry out workshops for training and awareness, and undertake active and reactive audits. It will also be responsible for setting compliance targets and deadlines.

The draft CRF does not propose any penalties for licensed service providers who may be in violation of the stipulated requirements. Under its founding statute, the CITC is empowered to impose penalties for violations of the laws and regulations pertaining to the telecommunications sector, and we expect that this will provide the basis under which the CRF, if it comes into effect, will be enforced.

Future Outlook

The public consultation process on the draft CRF was completed as of June 27, 2019. It is unclear when the finalised version of the draft CRF will become effective, or if any changes will be adopted in the interim. Industry participants are encouraged to watch this space.

Meanwhile, government agencies and critical national infrastructure operators will need to review their cybersecurity arrangements for compliance with the Essential Cybersecurity Controls.

Al Tamimi & Company's Technology, Media & Telecommunication team regularly advises on regulatory issues concerning technology, telecommunications and cybersecurity in Saudi Arabia and the Middle East. For further information please contact Nick O'Connell (n.oconnell@tamimi.com), Amy Land Pejoska (a.pejoska@tamimi.com) or Zil Ur Rehman (z.rehman@tamimi.com).