Cyber security in the Saudi financial services sector: The SAMA Cyber Security Framework

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data - Riyadh

In May 2017, the Saudi Arabian Monetary Authority issued version 1.0 of its Cyber Security Framework. Noting the importance of the need to safeguard sensitive data and transactions to ensure confidence in the Saudi financial sector, the Framework was designed to enable SAMA regulated entities (basically, banks, insurance companies and finance companies) to identify and address cyber security risks. In this article, we summarise key aspects of the Framework.

The Framework is based on SAMA requirements and industry standards (including ISO, BASEL and PCI-DSS). Its stated objectives are to create a common approach for addressing cyber security, to achieve an appropriate maturity level of cyber security controls, and to ensure cyber security risks are properly managed. It supersedes all prior SAMA circulars relating to cyber security.

Entities subject to the Framework include all banks, all insurance and reinsurance companies, all financing companies, all credit bureaus, and the Saudi financial market infrastructure. The Framework also has some degree of application to subsidiaries and the personnel of such entities, as well as to third party contractors and customers.

Cyber security is defined in the Framework as:

the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.

The 'information assets' to which the Framework relates include electronic information, hardcopies, applications, software, databases, computers and machines such as ATMs, data storage devices, and networks and other technical infrastructure.

The three basic premises upon which the Framework has been developed are confidentiality, integrity and availability. More specifically, confidentiality refers to information assets being accessible only to those

who are authorised, and protected from unintended or unauthorised disclosure; integrity refers to information assets being accurate, complete and processed correctly, and protected from unauthorised modification; and availability refers to information assets being resilient and accessible, and protected from unauthorised disruption.

The Framework prescribes key cyber security principles and objectives to be embedded and achieved by each regulated entity. These are broken down in terms of four main cyber security 'domains': Leadership & Governance, Risk Management & Compliance, Operations & Technology, and Third Party considerations. The Framework also contemplates regulated entities meeting a minimum level of cyber security maturity (the criteria of which are specified in detail in the Framework), and to subject themselves to periodic self-assessments, reviewed by SAMA.

Leadership & Governance

The Framework contemplates the implementation of a board-endorsed, defined cyber security governance structure to lead the overall approach to cyber security within the regulated entity. As well as establishing a cybersecurity committee (with representatives from all relevant departments in the organisation), regulated entities also need to establish a cyber security function, independent of the information technology function, and led by a Chief Information Security Officer who is a Saudi national and sufficiently qualified for the CISO role.

Each regulated entity needs to define a cyber security strategy aligned with its own strategic objectives and the broader banking sector's cyber security strategy. It must also develop a cyber security policy to document and communicate its cyber security commitment and objectives. The policy should be considered in the development of other corporate policies (such as HR policies and IT policies), based on best practices, and supported by detailed security standards. The policy also needs to ensure that information is classified appropriate to its importance, and protected in line with the entity's risk appetite. Owners need to be appointed for all information assets, and all stakeholders need to be made aware of cyber security. The policy also needs to contain requirements that ensure compliance with regulatory and contractual obligations, and provide for reporting of cyber security breaches and suspected weaknesses.

The ultimate responsibility for cyber security lies with the regulated entity's board of directors. This responsibility ranges from ensuring an appropriate budget is available for cyber security measures, through to endorsing the entity's cyber security governance, strategy and policy. The entity's cyber security committee is responsible at a more operational level.

The Framework imposes an obligation on regulated entities to ensure that relevant stakeholders are aware of, and understand, their cyber security responsibilities. It requires the development of an organisational culture of cyber security risk awareness, enabling personnel, third parties and customers to protect the regulated entity's information assets. Additionally, it requires the implementation of training to ensure that personnel are equipped with the necessary skills and knowledge to protect the entity's information assets (including by operating the entity's systems securely) and to meet its cyber security responsibilities. Cyber security needs to be an integrated part of the regulated entity's project management methodology, enabling the entity to identify and address cyber security risks as part of any project.

Risk Management & Compliance

The Framework describes risk management as the ongoing process of identifying, analyzing, responding to, monitoring and reviewing risks. To manage cyber security risks, the Framework requires regulated entities to undertake cyber security risk identification (identification of their cyber security risks), risk analysis (assessment of the likelihood of occurrence, and the resulting impact), risk response (determining

the appropriate response to cyber security risks), and monitoring and review (monitoring the risk treatment and review of the effectiveness of the cyber security control).

In order to ensure cyber security risks are properly managed to protect the confidentiality, integrity and availability of a regulated entity's information assets, and to ensure alignment of the cyber security risk management process with the entity's enterprise risk management process, each regulated entity is required to define, approve and implement a cyber security risk management process.

This involves identification (and treatment) of the entity's cyber security risks and threats, bearing in mind the relevant information assets of the entity, as well as its existing cyber security controls and vulnerabilities, and the likelihood of occurrence of the risks identified and the likely resulting impact. The Framework contemplates this exercise being performed on a rolling basis, so as to ensure its continued effectiveness.

Regulated entities are also required to establish a process whereby they identify, communicate and comply with the cyber security implications of relevant regulations, and adopt mandatory local and international industry standards.

There is an expectation that information assets of regulated entities will be subjected to thorough, independent and regular cyber security audits, in accordance with generally accepted auditing standards and the Framework.

Operations & Technology

The Framework makes it is necessary for regulated entities to ensure that security requirements for their information assets are defined, approved and implemented.

Regulated entities are required to incorporate cyber security requirements into their human resources processes. At a minimum, these should include: cyber security awareness training for personnel at induction and during their employment, personnel agreements setting out cyber security responsibilities and obligations of non-disclosure, post-employment cyber security implications (such as revocation of

access rights, and obligations to return access badge, tokens, mobile devices, all electronic and physical information). The Framework also provides for requirements relating to Bring Your Own Device (BYOD) policies, so as to ensure that business and sensitive information is securely handled by personnel when using personal devices.

There is also an obligation to ensure appropriate physical security, by ensuring that all facilities that host information assets are physically protected. These should include: physical entry controls, monitoring and surveillance (e.g., CCTV), protection of data centres and data rooms, environmental protection, and consideration of the physical protection of information assets during their lifecycles (such as during transportation and destruction, and by avoiding unauthorized access and data leakage). The secure disposal of information assets is also contemplated, so as to ensure that business, customer and other information, is protected from unintended or unauthorized disclosure when no longer required.

More generally, there is an obligation to ensure that access to information assets is restricted in line with need to know/have principles. This requirement brings with it a need to ensure that identity and access be managed and controlled.

Regulated entities need to know what information assets they have, and where (both physically and logically) they are located, in order to ensure cyber security. The Framework requires regulated entities to maintain an accurate and up-to-date inventory, including location and other relevant details, of all information assets.

Regulated entities are also required to define their cyber security architecture, outlining the cyber security requirements in their enterprise architecture and addressing the design principles for developing cyber security capabilities. They also need to make sure that they follow and review their cyber security architecture. Similarly, regulated entities need to make sure that cyber security controls are formally documented and implemented for all applications, and that the compliance is monitored and effectiveness evaluated on a regular basis.

Cyber security standards for infrastructure components need to be documented, and compliance monitored. This needs to include all instances of infrastructure (e.g., workstations, laptops, tablets, mobile devices, virtual machines, servers, operating systems, firewalls, network devices, wireless networks, email gateways, external connections, databases, file-shares, PBX), and it needs to cover all relevant locations, including data centres, disaster recovery sites and offices.

Regulated entities need to define, approve, implement and monitor cyber security standards for payment systems and electronic banking services in order to safeguard the confidentiality and integrity of shared banking systems and customer information and transactions.

Third party considerations

It is almost certain that regulated entities will need to engage with third party service providers (including the likes of information services providers, outsourcing providers, cloud computing service providers, technology vendors and governmental agencies) in order to deliver their services. If such engagements do not respect the types of cyber security mechanisms that the regulated entities have implemented, then such engagements could bring with them cyber security risks. With this in mind, the Framework introduces expectations with regard to the engagement of third parties. These can be broadly categorised as contract and vendor management considerations, outsourcing considerations and cloud computing considerations. We consider this in more detail in a separate article.

Conclusion

The SAMA Cyber Security Framework, which was developed in coordination with a leading consultancy firm, provides a very clear outline of what SAMA expects, in terms of cyber security, of the entities that it regulates. Just as the types of technology being used in the financial services sector will continue to develop, the volume and nature of cyber security risks to financial services sector business will continue to develop. SAMA's Cyber Security Framework should go some way to ensuring that businesses operating in the financial services sector are aware of the nature and scope of their information assets and the potential cyber risks to such assets. The processes implemented in compliance with the Framework will also provide a mechanism for future-proofing regulated financial services businesses against new cyber risks as they develop.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on issues relating to cyber security, including regulatory compliance and breach notification obligations. For further information please contact Nick O'Connell, Partner (n.oconnell@tamimi.com) or Andrew Fawcett, Senior Counsel (a.fawcett@tamimi.com)