Conference Paper

Cybersecurity as Enterprise Risk Within and Beyond the Bahraini Legal Framework

Maria Casoria

College of Law, Royal University for Women, Riffa, Kingdom of Bahrain

Abstract

The article focuses on the legal framework regulating cybersecurity in the Kingdom of Bahrain, in comparison with the laws in force in the other Gulf Cooperation Council (GCC) Countries. It discusses, on one side, the existing rules applicable to the variety of possible cyber-attacks affecting the activity of the businesses that engage in electronic commerce and, on the other hand, the regulations for the intrinsic threats connected to the digitalisation of the banking system. The study starts with a brief overview of the evolution of cybersecurity, from purely Information Technology issue to an emerging area of law, and then analyses the legal grounds for enforcing specific rules in the field, especially in the Arabian Gulf Countries. It examines the status of the laws in Bahrain and GCC and highlights the necessity to implement a more comprehensive regulatory framework, along with the need for investments in cutting-edge technologies, to increase the degree of protection and, consequently, derail the cyber-threats.

Keywords: Banking Activities, Cyber security, E-commerce, Enterprise Risk, Digitalisation, Gulf Cooperation Council (GCC) Countries Laws

Corresponding Author:
Maria Casoria
mcasoria@ruw.edu.bh

Received: 18 September 2018
Accepted: 10 October 2018
Published: 15 October 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the Sustainability and Resilience Conference Committee.

1. Introduction

Cybersecurity can be defined as a subset of information developed in response to the progressive digitalisation of the society, which relates to the protection from outside attacks of all the data shared and maintained in the cyberspace. As defined by the Information Telecommunication Union, cybersecurity is 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 cyber environment and organisation and the user's assets (Anderson, 2016).

Historically, such phenomenon has been addressed only as an Information Technology problem and focused on preventing and mitigating unauthorized access or use of

the information stored in an organisation's digital system (Peretti and Abbas, 2017). However, as the digital society widened, the concrete risk of harmful cyber-attacks progressively required the proactive involvement of governments, international bodies and lawyers to prevent the data breaches, preserve the security of the networks, and deal with the associated litigation.

Since cybersecurity is mainly concerned with the confidential and mysterious information saved in the account of the computer users -both individual or corporate entities-, one of the core issues that arises when trying to regulate the sector is the lack of appropriate incentives for the users, because they bear in full the costs of their security precautions, but share with their network partners the benefits of the investments made (Orji, 2012). Nonetheless, even though it might be considered anti-economic at first glance, the prevention of cyber-threats begins with the daily behaviour of the individuals and expands to all the other stakeholders potentially involved in cybersecurity incidents, in either the public and private sectors.

In this landscape, alongside the Information Security specialists, the legislator seems to have a fundamental role to play, especially in core areas of the current economy, such as the commerce performed through online platforms -which, in some sectors, is replacing the brick and mortar dealings- and the digital banking and finance, spread worldwide like wild fire especially because of the recent growth of cryptocurrency transactions and, more generally, the FinTech.

2. Literature Review and Research Methodology

Over the past few years, the debate on cybersecurity among scholars and practitioners tackled a variety of technical issues, but quite recently cybersecurity has becoming a serious enterprise problem, leading to risk assessment and management, cyber risk mitigation and incident response plans, especially for those businesses which engage in international trade activities or operate in wealthy countries, such has the Arabian Gulf States (Shalhoub and Al Qasimi, 2010). Indeed, the vast availability of resources and the rapid adoption of digital technologies have made these countries a prime target for cyber- related activities and, consequently, cybersecurity is nowadays a priority for the Gulf Cooperation Council (GCC) governments, due to the high number of recent attacks on both public and private companies. The statistics highlight that cyber-attacks in the Gulf are a growing threat for the businesses operating in the region. By way of illustration, in May 2017 all the GCC States were subject to the Wannacry

ransomware cryptoworm attack; in August 2017 Saudi Aramco's (the world's largest oil company) safety system was attacked by a malicious software; the UAE also struggles with cybersecurity, with one in 238 e-mails blocked as a suspected malware attack in the first semester of the current year (The Economist – Intelligence Unit, 2018).

Part of the scholars and specialists in the field has drawn attention to the various technology options and information security management standards available to enhance cybersecurity and protect the online users (Knapp, 2009); a few have discussed the possible interconnections between cybersecurity and other sectors, such as privacy and human rights (Cleary and Felici, 2014). Indeed, the international production on the legal facets of cybersecurity is in hectic development, whereas the topic is still not much investigated by the legal scholars and practitioners in the GCC, which calls for the necessity to make additions to the literature regarding law and technology, in order to shed lights on the effective perspectives for legal compliance in the field. On the other hand, the local governments, conscious of the challenges connected to the digital economy, have adopted multi-steps actions, seeking to strengthen their national cybersecurity infrastructure, assess and rectify weaknesses, and enforce specific laws (Mahfizah, Nurul, Jamaludin, 2016).

Within the aforementioned scenario, the research critically analyses the legal grounds for enforcing a more comprehensive rule of law in the field, with particular reference to electronic commerce and banking activities, and examines the legislation in force in the Kingdom of Bahrain, in comparison with other GCC countries. Moreover, it assesses the gaps in the existing legal framework and suggests ways to implement the regulatory apparatus. As an outcome, the study also aims at raising more awareness on the recent trends in technology and regulation in the GCC region, and on the new areas of risks deriving from the technological advancement in the performance of the commercial activities.

3. Conceptual Framework: The Interface between Law and Technology in the Vision of the Arabian Gulf Economies

In recent years the cyber ecosystem has changed its nature, evolving from a mere research environment to a borderless commercial space where companies operate and compete to serve millions of consumers across the globe. It is undeniable that the World Wide Web has altered the way in which the business activities are conceived and performed. Yet, as technologies evolve, the need for a new rule of law progressively

originates, inasmuch the regulations implemented for the off-line markets are mostly unsuitable to set standards for the online marketplace. Indeed, several countries have already been reforming their existing laws to govern the cyberspace, but the process is still ongoing, especially in the light of the fact that legislators around the world have approached this field in a sectorial way, mainly focusing on cybercrimes or electronic transactions.

The development of the e-commerce is undoubtedly a driving force for the globalisation of the world economy and this is the reason why some developing countries, in the attempt to increment their incomes, diversify their economies and promote sustainable growth, have initiated a process towards the modernisation of their infrastructure, which includes an increased use of electronic transactions in the supply chains (Shalhoub and Al Qasimi, 2010). Nonetheless, the technological improvements trigger threats for the consumers and the businesses operating in Internet and require urgent actions to delimit the side effects associated with the commerce in the digital market, such as fraud, unauthorized access to data, malware, cyber espionage, payment card skimmers, databases and Web Server threats just to refer to the major ones.

In the regional area targeted by this study, all the countries are striving towards the notion of digital economy as a tool for diversification beyond the wealth deriving from the exploitation of gas and oil. However, although the digitalisation holds the prospective for vast benefits, it also comes with risks from the ever-growing number of cyber related attacks and, consequently, governments across the Gulf have implemented national cybersecurity strategies to secure the cyberspace, safeguard their interests and hinder the risk of cyber-threats.

As for Bahrain, the National Cybersecurity Strategy outlines the Kingdom's vision to create a safe digital environment, respectful of the individual's rights and values, and to improve the information security in both public and private organisations. It identifies the following key objectives for its achievement: - to safeguard the critical national infrastructure, by protecting organisations that provide essential services to the nation such as oil, electricity and water, government services and finance; - to respond to the cyber-threats combining efforts from the public and private sector; - to develop the existing cyber-laws in line with international standards; - to develop a cybersecurity ecosystem through the involvement of experts able to prepare plans for a resilient infrastructure and safer cyberspace; - to boost safety in order to encourage the citizens to use online services; - to increase international cooperation to combat cyber-threats

and to promote the exchange of cyber laws and regulations. The strategy also envisages the establishment of a National Cybersecurity Committee in charge of monitoring its implementation, coordinating the development of cybersecurity policies, leading activities in the sector and overseeing the status of the cybersecurity initiatives in the country.

In the Gulf Cooperation Council (GCC), Oman seems to be the most developed country in the field. Indeed, according to the 2017 Global Security Index, it has been ranked fourth in the world for its infrastructure and readiness to manage cyber-attacks because of the measures outlined in the Cyber Security Strategy and Master Plan, and in the Comprehensive Roadmap. The focal points of the Omani actions include the establishment of a solid organisational structure, the adoption of legal measures, the implementation of capacity building, technical and procedural measures, and regional and international cooperation.

In the light of the strategic thrusts of the Qatar's National ICT Plan 2015 to protect the national critical information infrastructure and to procure a safe online environment for the different sectors, the National Cyber Security Committee, established in 2013, developed the Qatar National Cyber Security Strategy. Such plan encompasses some core objectives and activities to be achieved between 2014 and the end of 2018, which range from the promotion of cybersecurity intelligence, to the implementation of policies and legislations, and the protection of the information assets in critical sectors, such as energy and finance. Based on the data for 2016, Qatar was ranked twenty-fifth in the Arab World on the Global Cybersecurity Index by the International Telecommunication Union.

The Dubai Cybersecurity Strategy highlights the need for joint efforts by institutions and individuals to provide a secure cyberspace, with the vision to transform Dubai in the safest electronic city in the world. The strategy identifies five main areas of intervention. The first, called "cyber smart nation', aims at raising public awareness and developing the skills required to manage the cybersecurity risks in public and public sector and for individuals as well; the second area is innovation, in order to establish a secure and safe cyberspace characterized by freedom and justice; the third domain focuses on establishing controls to protect the confidentiality, integrity, availability and privacy of data; Cyber Resilience is the fourth key area to ensuring the continuity and availability of IT systems in the cyberspace and it is strictly related to the last domain, concerned with the establishment of national and international networks to face the cyber threats and adopt regulatory standards universally implementable.

A quite comprehensive National Cybersecurity Strategy for the triennium 2017-2020 has been adopted by the State of Kuwait and serves as a road map towards strengthening information security in all different forms and ensuring the adoption of all effective precautions needed. The plan dwells around three main objectives, which are promoting a culture of cybersecurity by supporting a safe and a proper usage for the cyberspace; safeguarding the security of national assets including critical infrastructure, national data, communication technologies and Internet; promote cooperation, coordination and information exchange among local and international bodies. The vision prescribes also the establishment of a National Cyber Security Center.

In November 2017, the Kingdom of Saudi Arabia, the GCC country that seems less prepared in terms of cybersecurity, has established a National Authority for Cybersecurity to increase safety and protect sensitive infrastructures. The authority is a development of the Saudi National Cyber Security Center, set up earlier that same year, which sought to improve government and critical national infrastructure resilience to cyber-threats, as well as develop internal capabilities. Among the duties of the new authority, enhancing the protection of networks, IT systems, operating systems, hardware and software components, data and services and the creation of a national cybersecurity industry to establish the Kingdom's leadership in the field, in line with the 2030 economic vision, are the major ones (Hathaway, Melissa, Spidalieri, Francesca, and Alsowailm Fahad).

4. Research Findings: The Domestic Laws in Force in the Gulf Cooperation Council Countries

Although cybersecurity is a global issue which might require a harmonised regulatory action at international level -aiming at the adoption of preventive measures in the global market and, in case of incidents and consequential damages for the market operators, at the enforcement of mitigation measures-, the legislators in the GCC have passed laws to regulate some of the challenges stemming from the increased use of the cyberspace as primary communication and economic channel and to assure information security.

Indeed, some of these laws relate to cybercrimes (and, as such, fall outside the scope of the research); others address the electronic transactions; and a few are specifically concerned with the banking sector. Anyhow, the existing legal framework is surely in need of further development.

4.1. Electronic commerce and rule of law

In today's economy any company is required to protect critical business and customer information from the exposure to the public domain to preserve privacy and reputation, and safeguard core enterprise values. This seems to be especially true for those entities which, as a result of the globalisation of markets, intertwined with the rapid adoption of the digital technology, largely rely upon the use of Internet to perform commercial activities and increase competitiveness and profits. Always more frequently, businesses renounce to brick and mortar stores and opt for online platforms to reach a wider consumer audience and save the costs to be borne for maintaining off-line shops.

In the Arab Gulf States the e-commerce phenomenon has experience an exponential rise in the turn of just few years due to the massive privatization of the economic activities. However, because Internet gives rise to security issues mostly associated to hacking activities, cyber espionage, fraud, malware and payment card skimmers, the companies deciding to engage in e-commerce must consider the external costs arising out of the cyber-attacks, which are becoming an inner part of the enterprise risk assessment and management.

The research conducted reveals that, aware of being a hot target for cyber related activity, almost all the GCC States have passed laws on electronic transactions, establishing the conditions under which documents exchanged online and signed electronically have legal value among the concerned parties. Yet, none of the countries has enforced an effective regulation on key aspects for the protection of companies and consumers operating in the digital marketplace, such as rules on electronic payments, that play a critical role with the emergence of new technologies. Moreover, the respective laws on consumer protection and anticompetitive conducts do not incorporate any provision regulating the e-commerce *per se*.

In this scenario, Bahrain has been among the first to promulgate, with the 'Legislative Decree No. 28 of 2002 with Respect to Electronic Transactions', overhauled with Law No. 34 of 2017, a set of rules which applies to electronic records and signatures, but not to the matters in the jurisdiction of the Sharia' courts, the personal affairs of non-Muslims, negotiable bonds, and title deeds. One of the amendments to the law has included, among the possible forms of electronic records, the official documents, i.e. those issued by public officers, which can be used -as the ones between private entities, as a mean of evidence in Civil and Commercial Law disputes.

The law broadly defines the word 'electronic' as any 'technology of using electrical, magnetic, electromagnetic, optical, and biometric or photon means or any other similar technological devices'; the word 'record' as 'any information (i.e. data, text, images, figures, sounds, codes, computer programmes, software, databases, speech) that is inscribed on a tangible medium or stored in an electronic or any other medium and is retrievable in an intelligible form'; and the expression 'electronic record' as a record created, sent, received or communicated, stored by electronic means. Consequently, the law might apply to a broad spectrum of dealings negotiated and contained in documents exchanged over the 'net'. Indeed, the legislator equalises the legal effects of the contracts entered into, in whole or in part, by means of electronic records with the agreements concluded with physical tools, and explicitly excludes that the validity and enforceability of the declaration of the contractual intention can be questioned by alleging its voidance because of the electronic approval.

Following, in chronological order, the 'Saudi Electronic Transactions Law promulgated by Royal Decree No. M/8 of 8 Rabi' I 1428H (March 26, 2007)'. Scope of application and legal principles are very similar to those in force under the Bahraini law, apart for the documents requiring notarisation or authentication. In addition, the decree prescribes the establishment of a National Center for Digital Certification within the Ministry of Communications and Information Technology as the body in charge of overseeing and managing tasks relating to issuance of the digital certificates.

The law legalizing electronic transactions in Oman has been issued by 'His Majesty's Royal Decree No. 69/2008', which applies in the same cases as those of the countries previously examined. The main aims of the law are facilitating the implementation of electronic transactions, by ensuring reliable and secured electronic messages or records and removing obstacles and challenges in the use of electronic transactions resulting from ambiguities associated with writing and signature. To increase the volume of the transactions concluded via Internet, the legislator establishes that the validity of the contracts concluded by electronic means is subject only to the agreement of the parties, whose consent can be explicit or inferred from their conduct. As under the Bahraini rules, offer and acceptance can be communicated electronically and are considered binding upon the parties. Moreover, the electronic contracts shall have the same legal effects associated with the contracts concluded in the traditional ways, whether in its validity or evidential value or enforceability and any other rules. Specific sections regulate the technical methods to keep confidential the information and the data exchanged while performing electronic transactions and to prevent their

corruption. Another part sets rules about role and powers of the authority in charge of license, control, inspection and supervision, that is the Omani Information Technology Authority under the same law.

Qatar has enacted a regulation on electronic commerce and transactions with the 'Decree Law No. 16 of 2010' implemented by the Qatari Supreme Council for Information and Communication Technology. At its inception, the law provides a list of definitions and establishes that an electronic transaction is 'any deal, contract or agreement concluded or performed, in whole or in part, through electronic communications'. The scope of application, the requirements of the electronic transactions, the rules for data privacy and storage and the powers of the authority competent to oversee the respect of the law are consistent with those of the countries analysed hitherto. However, the decree also comprises a section on the protection of the consumers engaging in electronic commerce and establishes criteria that the service providers must meet. Penalties for the cases of breach are equally regulated under the law.

The State of Kuwait has passed the 'Law No. 20 of 2014', which incorporates norms regulating the electronic transactions as a way to conclude contracts on legal basis similar to the paper transactions. Like other regulations in the GCC, the law grants legally binding status to original electronic documents and signatures and regulates the requirements for their validity. The regulatory aspects are, contrary to the solution adopted in the other regional States, entrusted to both the Public Authority for Civil Information and any other body as per the decision of the Council of Ministers. Moreover, it contains a set of rules on the payments made electronically and explicitly refers to the regulations issued by the Central Bank of Kuwait relating to payment methods and banking services.

The United Arab Emirates is the country with the most recent law on electronic transactions, i.e. the Law DIFC No. 2 of 2017, which applies in the jurisdiction of the Dubai International Financial Centre. Being in force only in the DIFC free-zone, it differs from the other laws passed in the region mainly with reference to the matters not included under its scope of application. In fact, there is no reference to the exclusion of the legal issues falling within the jurisdiction of the Sharia' courts and the parties are given the power to exclude the operability or derogate from or vary the effect of any of the provisions of the law, unless otherwise provided. Moreover, the Board of Directors of the Centre is entrusted with the power to issue regulations and standards or codes of practice in respect of any matter related to the application of the law.

4.2. Cybersecurity and banking activities

An area where cybersecurity has lately gained importance is the banking sector, inasmuch the technological advancement affects nowadays every segment of the banking industry, from the retail transactions to the market operations. For example, in the field of trading, autonomous, high-frequency trading programs powered by complex algorithms move daily billions of dollars of financial instruments across the world in fractions of a second. On the other side, the emergence of the FinTech seems to suggest that machines have replaced humans in trading securities. In the realm of the monetary services, the recent rapid spread of cryptocurrency transactions, mainly unregulated or banned in some jurisdictions or uncontrolled by the banking authorities, represents a major concern for the global financial community and entails the adoption of a risk management approach not focused, like in the past, on a single malicious agent, but tailored to combat large scale cyber-attacks. In fact, cyber-attacks threaten the economic stability and demand a meticulous pre-assessment and a prudent enterprise risk management by the banking and financial institutions.

To address properly the current challenges, the companies operating in the field must make more investments. Indeed, as the financial industry becomes ever more dependent on technology, timely and thoughtful investment in financial cybersecurity becomes ever more important (Lin). Undoubtedly, the regulation of the major revolution connected to the increased digitalisation in banking and finance passes through the enhancement of the awareness of the operators -both private and public-, that should prearrange plans to address the vulnerabilities of the informatic system and implement proactive remedies in case of information security breach. Yet, a second key step to deal with this phenomenon seems to be the regulatory intervention by the policy makers.

The lack of clear guidance provided by the economic theory on the new transformation in the field of banking and information security implies that the starting point for any regulatory attempt is the analysis of the *status quo* in the GCC countries, in order to understand whether the existing rules can be adjusted to face the troubles arising out of the large use of the digital asset and to protect both banks and customers while exchanging information over the 'net'. Indeed, if it cannot be denied that the digitalisation brings benefits for the individuals, the professional operators and the economy of the countries which are moving towards the new frontiers of the online banking and finance, it is equally self-evident that the threats deriving from the possible intrusion

of hackers and criminals, with consequential theft of sensitive information, represent a concrete risk not to be overlooked.

At first glance, the scenario looks quite nebulous, since the matter is entirely left to the regulatory power of the respective central banks. For instance, the Central Bank of Bahrain (CBB) in its Rulebook incorporates rules on electronic banking, electronic money, and cybersecurity risk management, aligning itself to the guidelines laid down by international bodies, particularly the Basel Committee on Banking Supervision. The section on the risk management for electronic banking and electronic money activities basically establishes that the banks should identify, assess, manage and control the risks associated with electronic banking and money and, with reference to the risks connected to the digital banking, it prescribes that these should be recognized and managed in prudent manner. The responsibility for managing the cyber risks is entrusted to the Board and senior directors of the financial institutions due to the high impact that such type of risks can produce. As regard to the cybersecurity risk management, the Rulebook requires all the financial institutions to prepare themselves for cyberattacks by implementing appropriate response mechanisms, which must be regularly tested to ensure the capability of the licensed institutions to deal with cyber-attacks. Moreover, to improve the banking sector and meet the international payment and settlement system standards, in the first quarter of 2018 the Central Bank has launched a secure private network to connect all the retail banks in Bahrain with the CBB, that is now used as the primary communication hub to perform real-time inter-bank payments settlement.

Very recently, the Qatar Central Bank (QCB) has published a policy to defeat cyber-threats whose highlights are management of technology risks; defined technology risk organizational structure; defined roadmap for business continuity; framework for incident and fraud management; detailed process risk controls. Like in Bahrain, the QCB requires all the banks to implement all the necessary actions to ensure proper protection of data and records and a comprehensive cyber security circular has been issued to provide guidance to bank users, employees, contractors and other authorised users in Qatar, of their obligatory requirements for protecting the technology and information assets of the bank. Furthermore, in QCB second Strategic Plan for Financial Sector Regulation 2017- 2022, one of the core objectives to maintain integrity and confidence in the Qatari financial system is strengthening the cybersecurity capabilities within the financial sector by the enhancement, among others, of specific regulations applicable to banks and financial institutions.

As for the United Arab Emirates, the UAE Central Bank is currently in the process of establishing a dedicated department to ensure that a minimum set of required standards of cybersecurity controls, fixed by the Central Bank in coordination with the National Electronic Security Authority, are implemented by all the licensed banking and financial operators. On the other hand, the Omani Central Bank is dealing with the vulnerabilities of the cyber-attacks by requiring the banks to invest in cutting-edge technologies and services for the safety of the customers, upgrade their cybersecurity protocols and identify the existing gaps. A similar approach is adopted by both the Kuwaiti Central Bank and the Saudi Arabian Monetary Authority. Overall, it emerges the necessity to adopt an approach more hard-law oriented in this field, due to the vital role of the banking and financial sectors for the economy of any country.

5. Conclusions: Looking for a More Comprehensive Legal Framework

The protection against cyber-threats is in spotlight. Cybersecurity has risen indeed to a major national and global concern, both generally and with specific reference to the performance of commercial and banking transactions through online platforms, for which the market and the legal systems may fail to provide a comprehensive solution. The problem is complex because the digital networks expand far beyond the jurisdiction of one or even a bunch of states and, therefore, the implementation of joint initiatives by governments and private operators in specific regional areas seems to be the starting point for any regulatory attempt.

None of the laws currently in force in the GCC countries regulates specifically the enterprise risk when dealing with cybers-threats. Rather, they govern the electronic transactions, by establishing rules on contract formation and validity from a consumer perspective, and the digital banking and financial operations, by shifting -explicitly or implicitly- the norms issued for the services tendered in the offline market to the realm of online monetary and financial activities. Unquestionably, there is a need for the implementation of a most effective set of rules, which should adopt a preventing approach rather than a strategy *ex-post*, aiming at the punishment of the cybercrimes as under the most part of legislations passed worldwide. Moreover, as the technology evolves, the rule of law not only must be updated, but should be ahead of its time, to accommodate any future technological developments.

Regarding the GCC countries, in the light of the similarities among the cybersecurity strategies already implemented, the necessity to face common cyber-attacks to the regional infrastructures and the commonality of economic, social, political and religious ties, the adoption of a regulatory framework harmonised for the states object of this study seems to be the key to ensure legal certainty and defeat cyber-threats. As for the e- commerce, it seems essential for the Gulf legislators to identify and adopt best international practices in the field, in order to boost economic growth and to increase the intra-regional trade, which is one of the main goals for the economic sustainability of the GCC. Hence, the e-commerce legislation should move beyond the mere legal recognition of the electronic transactions and regulates other aspects, such as the governance of the companies for implementing decisions, rights and supporting mechanisms to guarantee the accuracy, integrity, consistency, accessibility, privacy, retention and security of information across the enterprise.

On the other hand, because the cyber risk becomes amplified due to the inter- connectedness of the global financial system and the progressive move to a new way of dealing with banking and finance, such as the blockchain and Fintech -which are tools to promote the GCC countries as leading arenas for the advancement of the financial services-, specific legal standards should be set for the financial intermediaries willing to operate in the digital market, requiring them to invest in technologies to increase their cyber preparedness and the degree of protection.

Overall, while some of the Gulf States appear technologically equipped to facing the cyber-attacks, since they have invested resources to tackle the growing number and frequency of threats, regulatory challenges persist despite the sectorial policies and procedures already in force and analysed by this research. Yet, dealing with such issues from both a domestic as well as supranational standpoint is one area that the GCC will have to focus on in the coming years. In the meantime, companies and financial institutions must be aware that, being technologies in hectic evolution, one of their key sectors of intervention must be the pre-assessment of possible threats which, alongside a risk-mitigation plan, should minimise the impact of cyber-attacks on the business operations and help safeguarding the exchange of data and the economic interests of consumers and professional operators engaging in the online marketplace.

References

[1] Anderson, Charletta. 2016. "Cyber Security and the Need for International Governance". http://dx.doi.org/10.2139/ssrn.2769579.

[2] Bahrain National Cybersecurity Strategy. Accessed June 24. https://www.bahrain.bh/CyberSecurity.

[3] Cleary, Frances, and Felici, Massimo (Eds.). 2014. *Cyber Security and Privacy*. Switzerland: Springer.

[4] Cyberwellness Profile Bahrain. Accessed July 25, 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Bahrain.pdf.

[5] Cyberwellness Profile Oman. Accessed July 25, 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Oman.pdf.

[6] Cyberwellness Profile Kuwait. Accessed July 25, 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Kuwait.pdf.

[7] Cyberwellness Profile Qatar. Accessed July 25, 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Qatar.pdf.

[8] Cyberwellness Profile Saudi Arabia. Accessed July 25, 2018. https://www.itu.int/en/ITU- D/Cybersecurity/Documents/Country_Profiles/Saudi_Arabia.pdf.

[9] Cyberwellness Profile United Arab Emirates. Accessed July 25, 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_Arab_Emirates.pdf.

[10] Dubai Cybersecurity Strategy. Accessed June 24, 2018. file:///C:/Users/mcasoria/Downloads/Dubai%20Cyber%20Security%20Strategy.pdf.

[11] Hathaway, Melissa, Spidalieri, Francesca, and Alsowailm Fahad. 2017. "Kingdom of Saudi Arabia Cyber Readiness at a Glance". https://www.belfercenter.org/publication/kingdom-saudi-arabia-cyber-readiness-glance.

[12] International Telecommunication Union. 2017. "Global Cybersecurity Index". Accessed June 18, 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01- 2017-PDF-E.pdf.

[13] Knapp, Kenneth J. (Eds.) 2009. *Cyber Security and Global Information Assurance. Threat Analysis and Response Solutions*. Hershey: Information Science Reference.

[14] Lin, Tom (2016). "Compliance, Technology, and Modern Finance". *Brooklyn Journal of Corporate, Financial & Commercial Law* 11: 159-183.

[15] Mahfizah, Mazlan, Nurul, Aqilah Mohd Zarani, and Jamaludin, Ibrahim. 2016. "A Cyber Security Assessment of Muslim Countries." *International Journal of Information and Communication Technology Research* 6 (12): 1-8.

[16] National Cyber Security Strategy for the State of Kuwait 2017-2020. Accessed July 25, 2018. https://citra.gov.kw/sites/en/LegalReferences/English%20Cyber%20Security%20Strategy.pdf.

[17] Orji, Uchenna Jerome. 2012. *Cybersecurity Law and Regulation*. Netherlands: Wolf Legal Publisher.

[18] Peretti, Kim, and Abbas Nameir. 2017. "Lawyers and Cybersecurity: A Brief History, Yet a Rapidly Expanding and Evolving Role." *Antitrust* 31 (3): 56-59.

[19] Qatar National Cyber Security Strategy. Accessed June 24. http://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf.

[20] Shalhoub, Zeinab Karake, and Al Qasimi, Sheikha Lubna. 2010. *Cyber Law and Cyber Security in Developing and Emerging Economies*. Cheltenham: Edward Elgar.

[21] The Economist – Intelligence Unit, 2018. Business reality check. Accessed August 3, 2018.