Archives of Business Research – Vol.6, No.12
Publication Date: Dec. 25, 2018
DOI: 10.14738/abr.612.5771.
Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. *Archives of Business Research,* 6*(12),* 131-146.

Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index

Dr. Tareq Saeed Alshammari
Department of Management and Information Systems,
College of Business Administration,
University of Hail, Kingdom of Saudi Arabia

Dr. Harman Preet Singh
Department of Management and Information Systems,
College of Business Administration,
University of Hail, Kingdom of Saudi Arabia

(Both authors contributed equally to this work.)

ABSTRACT

With the increasing popularity of ICT, cyber-crimes have increased rapidly. Countries across the globe have made the necessary interventions to ensure cyber-security. Saudi Arabia has been the worst victim of cyber-crimes in the Gulf region. This article investigates the preparedness of Saudi Arabia to defend itself against cyber-crimes. In order to combat against cyber-crimes, Saudi Arabia formed the anti-cybercrimes law in 2007. Global Cyber-security Index of 2017 has placed Saudi Arabia in the maturing stage behind the leading nations. Anti-cybercrimes law covers essential areas to fight against cyber-crimes and states their punishments. However, it is found to be deficient to protect against identity theft, invasion of privacy, cyber-bullying etc. This research finds Saudi Arabia semi-prepared to defend itself against cyber-crimes. In order to be among the leading nations of cyber-security; Saudi Arabia needs to strengthen its anti-cybercrimes law, cyber-security regulations and national cyber-security authority. It needs to develop cyber-security strategy, standards, metrics and R&D programs. It should promote home-grown cyber-security industry, incentivize cyber-security companies and enter into multi-lateral agreements.

Keywords: Cyber-crime, cyber-security, global cyber-security index, Saudi anti-cybercrimes law

INTRODUCTION TO CYBER CRIMES

The use of Information and Communication Technology (ICT) networks, devices and services has been expanding rapidly. There were 1.991 billion users in 2010, which increased to 3.385 billion in 2016 (ICT Facts & Figures, 2017). The number of networked devices in 2016 were 17.1 billion, which is projected to increase to 27.1 billion in 2021 (Cisco, 2017). With the immense increase in connectivity, the exposure of cyber world to variety of security threats and consequently cyber-crimes is also increasing.

Cyber-crime is a criminal act related with computers and networks. Examples of cyber-crimes include hate crimes, telemarketing, Internet fraud, identity theft, cyber bullying, credit card account thefts etc. (http://nimachpolice.org/cyber-crime-define.php). Cyber-crimes can be committed against individuals or groups of individuals with a criminal motive to intentionally cause physical or mental harm, or loss, or damage the reputation of the victim directly or indirectly using ICTs (Halder & Jaishankar, 2011). Ransonware is increasingly used by

attackers to plague businesses and consumers with malicious emails. The average ransom demand worldwide has increased from USD 294 in 2015 to USD 1077 in 2016 (O'Brien, 2017).

Cyber-crimes have to potential to threaten a country's security and financial position. Countries have suffered due to cyber-crimes like hacking, copyright infringement, espionage, financial theft, intellectual property theft, cyber extortion, social engineering identity theft, online gambling, online sale of illegal articles, cyber fraud, forgery, spam, phishing, data diddling, steganography, cyber terrorism, child grooming, child pornography etc. Also, privacy violations have occurred when confidential information is intercepted or disclosed, lawfully or otherwise. Both governmental and non-governmental actors engage in cybercrimes. When one nation engages in cyber-crimes against another nation, it is called cyber-warfare. The international legal system is attempting to address cyber-crimes related to governmental and non-governmental actors through the International Criminal Court (Pitts, 2016).

Cyber-crimes are somehow different from computer crimes. Computer crime happens in physical space with or without the network. It can involve traditional criminal activities like theft, fraud, forgery and mischief. Cyber-crime takes place in a virtual space through digital environment. Computer misuse and abuse have significantly different implications. Annoying behavior is different from criminal behavior in Law (Boni & Kovacich, 1999).

CYBER CRIMES IN SAUDI ARABIA

Internet usage has rapidly expanded in Saudi Arabia. In 2001, the number of internet users were estimated by be 1.03 million. This increased to 4.95 million in 2006, 13.67 million in 2011 and 20.81 million in 2016 (http://www.internetlivestats.com/internet-users/saudi-arabia/).

With the increase in internet adoption, cyber-attacks have also increased in Saudi Arabia. Saudi Arabia faces the highest number of cyber-attacks in the Arab region followed by UAE (Forbes Middle East, 2018). Some of the major cyber-attacks in Saudi Arabia are stated in Table 1:

Table 1: Saudi Arabia Major Cyber Attacks

Attack Name	Details
Shamoon	On 15th August 2012, Saudi Aramco was hit with a malicious malware, named Shamoon. This malware had the capability to over-write data on computers and destroy master boot record files. This virus affected about 30,000 workstations of Saudi Aramco. This virus attack aimed to disrupt the global oil supply of Saudi Arabia. In order to recover from the attack, Aramco has to restrict remote internet access to its online resources for 10 days (Bronk & Tikk-Ringas, 2013).
Shamoon 2.0	Variants of Shamoon virus attacked Saudi Arabia on 17th November 2016, 29th November 2016 and 23rd January 2017. It was called Shamoon 2.0. It was estimated that this virus affected 15 Saudi government agencies and organizations (Smith, 2017).
StoneDrill	While investigating Shamoon 2.0 malware, Kaspersky Lab discovered a previously unknown wiper malware, called StoneDrill. StoneDrill had several style similarities to Shamoon 2.0. However, it had multiple embedded factors and techniques to allow for invasion of detection. Along with Shamoon 2.0, this malware also targeted Saudi organizations (Kaspersky Lab, 2017).
Cyber of emotion	On 15th August 2015, a Saudi group called "cyber of emotion" hacked more than 24 government websites over a period of 2 hours. Prior to hacking the websites, the hackers warned the administrators about the lack of security in websites and asked them to improve websites security. The websites that were hacked included those of government hospitals, municipalities, education departments, social development offices and health departments (HackRead, 2015).
APT	On 20th November 2017, Saudi Arabia's National Cyber Security Centre (NCSC) detected a Advanced Persistent Threat (APT) targeting Saudi Arabia. APT used spear phishing attacks to infiltrate computers in Saudi Arabia. Emails were found to contain infected Microsoft Office files (Walker, 2017).
Triton	In August 2017, a cyber-attack was launched against a petrochemical plant of Saudi Arabia. The attack caused the abrupt disruption of plant operations. Due to a flaw in the coding of the malware, it could not cause the intended damage (Sutton 2018).

According to a study by Kaspersky lab, nearly 60 percent of institutions in Saudi Arabia has experienced virus and malware attacks from August 2016 to August 2017 (Arab News, 2017). In 2012, 3.6 million people in Saudi Arabia fell victims to cyber-crimes and suffered an average of $195 (730 Saudi Riyals) in direct financial losses. In 2012, 40 percent of social networking users in Saudi Arabia have also fell victims to cyber-crime. Consumer cyber-crime cost Saudi Arabia approximately $693 million (2.6 billion Saudi Riyals) in 2012 (Ministry of Communications & Information Technology, 2012). The 2016 Internet Crime Report prepared by Federal Bureau of Investigation (FBI) estimated financial loss to United States in excess of $1.3 billion due to cyber-crimes (Masters, 2017). Globally, the cost of consumer cyber-crimes was estimated to be $110 billion in 2012 (Ministry of Communications & Information Technology, 2012).

CYBER CRIMES AND LEGAL FRAMEWORK

The incidents of cyber-crime have increased around the globe. So, it is necessary to ensure cyber-security. Developing adequate technological arrangements for cyber-security is essential. However, developing a legal framework that enables cyber-security is also essential.
Every country should develop basic criminal laws against cyber-crimes in order to promote the trust and confidence of users in cyberspace. Since, there are many types of cyber-crimes, so it is difficult to draft legislations for each of them. However, any cyber-security legislation should cover some essential areas. Sadowsky et al. (2005) contributed a paper to the United Nations ICT Task Force Global Forum on Internet Governance (New York, 25 - 26 March 2004). According to Sadowsky et al. (2005), countries cyber-security legal system should broadly

address data interception, data interference, system interference and illegal access. So, any anti-cybercrime legislation should address each one of them. These are discussed below:

- Data interception – It should be prohibited to intentionally intercept non-public transmission of computer data without authorization. This crime violates the confidentiality of communications and causes individuals to loose trust. It should be illegal to intercept the email and other electronic communications of another person. In some countries, interception of telephonic conversations (without prior legal sanction by a court order) is illegal (e.g., USA). The same laws may be extended to interception of electronic data.
- Data interference – No one should intentionally delete, damage, alter, degrade or suppress data in someone else's computer without authorization. So, intentionally sending viruses that delete files, hacking a computer, changing or deleting data without authorization, or hacking a web site and changing its appearance, would be examples of cyber-crimes. Here, the element of intentionality is important. Otherwise producing defective software or unintentionally forwarding a virus would be a cyber-crime.
- System interference – No one should input, transmit, damage, delete, deteriorate, alter or suppress data in another person's computer without right. If anyone causes serious hindrance in the working of a computer system without right, it should be a cyber-crime. So, denial of service attacks or introducing viruses into a system to disrupt its normal functioning are cyber-crimes. It is important that this offence is invoked when there is a significant harm (e.g., a certain threshold of monetary loss). Otherwise, ordinary online behavior, such as sending one or few unsolicited e-mails would also be a crime.
- Illegal access - This crime involves intentionally accessing other person's computer system without having rights. It is the cyberspace equivalent of trespassing. Illegal access compromises the confidentiality of the stored data and therefore is analogous to illegal interception. This crime must be carefully defined, otherwise it may include common and harmless activities. In the most serious cases, the act of illegal access is part of other crimes, such as data interference.

Common concepts of the criminal law such as "attempt" or "aiding and abetting" can also be applied to anti-cybercrime law. For example, launching a virus with intent to disrupt service might be a crime under the concept of "attempt" even if the virus didn't work as intended.

Similarly, if a nation's law has the concept of "aiding and abetting", it might be applied to cyber-crime. For example, if a person intentionally produces a virus and provides it to another person knowing that it will be used to destroy data or interfere with a system. Then first person may be guilty of data or network interference caused by the virus even if the virus was introduced into a network by someone else.

SAUDI LAW ON CYBER CRIMES

Saudi Arabia formed the Anti-Cyber Crime Law (ACCL) in March 2007. ACCL defines un-authorized access as the deliberate, unauthorized access by any person to computers, websites, information systems and computer networks. This law identifies certain cyber-crimes and determines their punishments. The salient features of Saudi Anti-Cyber Crime Law (ACCL) along with its legal provisions are shown in Table 2 (ACCL, 2007):

Table 2: Salient Features and Legal Provisions of Saudi Anti-Cyber Crime Law of 2007

Feature(s)	Legal Provision(s) in Saudi Anti-Cyber Crime Law of 2007
Prevention of data interception	Spying on, interception or reception of data transmitted through an information network or a computer without legitimate authorization is a cyber-crime (Article 3(1)). Article 3 states the punishment for this offence as "imprisonment for a period not less than one year and a fine not exceeding five hundred thousand Saudi riyals or either punishment."
Prevention of data interference	Hacking a website with the intention to change its design, destroy, modify or occupy its URL is a cyber-crime (Article 3(3)). Article 3 requires its punishment as "imprisonment for a period not less than one year and a fine not exceeding five hundred thousand Saudi riyals or either punishment."
	It is a cyber-crime to halt an information network, or destroy, delete, leak or alter existing or stored programs or data (Article 5(2)). Article 5 specifies the punishment for this offence as "imprisonment for a period not exceeding four years and a fine not exceeding three million Saudi riyals or either punishment."
Prevention of system interference	Unlawful access to an information system with the intention to obtain data to jeopardize the internal or external security of the state or its national economy is a cyber-crime (Article 7(2)). Article 7 states the punishment for this cyber-crime as "imprisonment for a period not exceeding ten years and a fine not exceeding five million riyals or either punishment."
Prevention of illegal access	Unlawful access to computers with intention to threaten or blackmail any person to compel him to take or refrain from taking any action is a cyber-crime (Article 3(2)). Article 3 stipulates the punishment for this crime as "imprisonment for a period not less than one year and a fine not exceeding five hundred thousand Saudi riyals or either punishment."
	Illegally accessing bank or credit data or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services is a cyber-crime (Article 4(2)). Article 4 specifies punishment for this cyber-crime as "imprisonment for a period not exceeding three years and a fine not exceeding two million Saudi riyals or either punishment."
	Unlawful access to computers with intention to delete, erase, destroy, leak, damage, alter or redistribute private data is a cyber-crime (Article 5(1)). Article 5 states punishment for this cyber-crime as "punishment for a period not exceeding four years and a fine not exceeding three million Saudi riyals or either punishment."
Prevention of invasion of privacy	Invasion of privacy through the misuse of camera-equipped mobile phone and other equipments is a cyber-crime (Article 3(4)). For this cyber-crime, article 3 stipulates the punishment for this cyber-crime as "imprisonment for a period not less than one year and a fine not exceeding five hundred thousand Saudi riyals or either punishment."
Maintenance of public order and morals	Production, preparation, transmission, or storage of electronic material which has a negative effect on public order and public morality is a cyber-crime (Article 6(1)). The construction of any website that promotes or facilitates human trafficking is a cyber-crime (Article 6(2)). The preparation, publication and promotion of material for pornographic or gambling sites that violates public morals is a cyber-crime (Article 6(3)). The construction of any website that demonstrates methods of use or facilitates dealing in narcotic or psychotropic drugs in a cyber-crime (Article 6(4)). Article 6 determines the punishment of these crimes as "imprisonment for a period not exceeding five years and a fine not exceeding three million riyals or either punishment."
Prevention of cyber-terrorism	The construction of a website to facilitate communication among members of terrorist organizations, financing them, promoting their ideologies etc. is a cyber-crime (Article 7(1)). Article 7 stipulates the punishment for this cyber-crime as

Feature(s)	Legal Provision(s) in Saudi Anti-Cyber Crime Law of 2007
	"imprisonment for a period not exceeding ten years and a fine not exceeding five million riyals or either punishment."
Prevention of attempt to commit cyber-crime	Any person who attempts to do any cyber-crime mentioned in Saudi ACCL shall be subject to a punishment not exceeding half of the maximum punishment designated for that crime (Article 10). So, Saudi ACCL prevents the attempt to commit cyber-crimes even if they were unsuccessful.
Investigation and prosecution bodies	According to Article 14 of the Saudi ACCL, the Communications and Information Technology Commission will provide the assistance and support to competent security agencies during the investigation and trial of cyber-crimes.
	The Bureau of Investigation and Public Prosecution will carry out the investigation and prosecution of cyber-crimes (Article 15).

From Table 2, it is clear that Saudi ACCL has the necessary features to ensure cyber-security. However, there are still areas of improvement for the Saudi ACCL to become more effective. They are discussed in Table 3 (ACCL, 2007):

Table 3: Areas of Improvement for Saudi Anti-Cyber Crime Law of 2007

Area(s)	Details
Identity theft	Article 4(2) of ACCL of 2007 limits the criminalization to obtaining financial data, information or services. So, it covers the identity theft only in financial matters. So, it would not be an offense under ACCL to obtain identity related information for non-financial motivations, such as, to tarnish the image of another person (Almerdas, 2014).
	ACCL of 2007 does not criminalize transferring and possessing of data and programs for the purpose of identity theft. So, ACCL cannot deal with those who transfer or sell credit card details of individuals (Almerdas, 2014).
Privacy of data	The term "personal data" is not defined by the ACCL. There are no formal registration requirements before the processing of data. Also, it does not define data controller. So, the provisions to protect the privacy of data are inadequate.
Cyber bullying	Saudi Arabia faces the problem of cyber bullying. However, it is not defined in ACCL of 2007.
Aiding and abetting	Saudi ACCL does not contain provisions related to "aiding and abetting" to commit cyber-crimes.

COMPARISON OF SAUDI CYBER SECURITY PREPAREDNESS WITH LEADING COUNTRIES

All countries face the threat of cyber-crimes. However, all countries are not equally prepared to counter cyber-crimes. There are differences among countries in terms of awareness, understanding, knowledge, strategies, capabilities and programs for cyber security. So, International Telecommunication Union (ITU) with help of international partners in public and private sectors has prepared the Global Cyber-security Index (GCI) in 2017. Each country's level of preparedness for cyber-security is assessed by commitment to 5 pillars given in GCI – legal, technical, organizational, capacity building and cooperation (GCI, 2017).

GCI has classified countries into 3 categories based on their cyber-security preparedness. It is shown below (Financial Express, 2017):

- Initiating stage – This category contains countries that have started to make commitments to cyber-security. There are 96 countries in this category. Examples of countries in this category include Ethiopia (rank 99), Afghanistan (rank 101), Libya (rank 105), Bhutan (rank 110), Chad (rank 148), Iraq (rank 159), Yemen (rank 164) etc.
- Maturing stage – The countries in this category engage in cyber-security programs and initiatives, and have developed complex commitments. There are 77 countries in this

category. Examples of countries in this category include India (rank 23), Germany (rank 24), China (rank 32), Brazil (rank 38), Tunisia (rank 40), Kenya (rank 45), Saudi Arabia (rank 46) etc.

- Leading stage – The countries in this category demonstrate high commitment to all 5 pillars of cyber-security. There are 21 countries in this category. Examples of countries in this category include Singapore (rank 1), United States (rank 2), Malaysia (rank 3), Oman (rank 4), Mauritius (rank 6), Australia (rank 7), Russia (rank 10), Egypt (rank 14) etc.

Saudi Arabia is in the maturing stage and ranked 46 in the GCI (2017). It needs to further strengthen its cyber-security mechanisms to be among the leading nations.

ASSESSMENT OF SAUDI ARABIA'S PERFORMANCE ON 5 PILLARS OF GLOBAL CYBER SECURITY INDEX

The performance of Saudi Arabia is assessed on the 5 pillars of cyber-security of GCI index. The best practices adopted by the countries that are leading in the particular indicator of the respective cyber-security pillar are investigated. Subsequently, the performance of Saudi Arabia in each indicator of the respective cyber-security pillar is compared with leading nations.

Legal Pillar

The legal pillar considers practices in national cyber-crime legislation regarding unauthorized access, data and system interference, and mis-use of computer systems. The performance of Saudi Arabia as per the indicators of legal pillar is assessed in Table 4 (GCI, 2017):

Table 4: Assessment of Performance of Saudi Arabia in Legal Pillar

SNo	Indicator	Performance	Assessment Details
1	Cybercriminal legislation	Average	138 countries have enacted anti-cybercrime legislation worldwide. More than 30 countries does not have an anti-cybercrimes legislation. United States (US) has strong legislations to combat cyber-crimes like Computer Fraud and Abuse Act (CFAA) of 1986, Wiretap Act and Network Crime Statutes (Floyd, 2016). US National Information Infrastructure Protection Act (NIIA) of 1996 amended CFAA and contained provisions related to unauthorized access to computer systems. The Saudi ACCL of 2007 contains provisions against hacking, illegal access to data, pornography, denial of service and cyber terrorism etc. However, it is deficient in preventing identity theft, protecting privacy of individuals, preventing cyber bullying etc. So, the performance of Saudi Arabia is assessed as average.
2	Cyber-security regulation	Average	Oman has laid out comprehensive cyber-security regulations under the e.Oman strategy. It has established e-governance framework, set of standards, best practices and process management systems to enhance the delivery of government services (Omanuna, 2018). Saudi Arabia has established information security policies and procedures development framework for government agencies (CITC, 2018). However, Saudi Arabia needs to further strengthen its cyber-security regulations as it has performed average in this indicator.
3	Cyber-security training on regulation and laws	High	Mauritius has deployed good framework for cyber-security training on regulations and laws for officers working under law enforcement and judiciary under GLACY project (Council of Europe, 2015). New Zealand has a developed a 3-tiered training programs for specialist cyber staff, investigators and frontline staff (New Zealand's Cyber Security Strategy, 2016). Saudi Arabia also has a good setup to provide training on regulations and laws. So, its performance is assessed as high in this indicator.
4	Overall	High	Overall, Saudi Arabia has performed satisfactorily in the legal pillar of cyber-security. However, it needs to strengthen its anti-cybercrimes legislation and cyber-security regulations.

Technical Pillar

The technical pillar illustrates practices in areas like existence of technical institutions, industry standards, certification, child online protection etc. In order to assess the performance of Saudi Arabia in technical pillar, we state a few terms used in Table 5. CERT stands for Computer Emergency Response Team. CIRT stands for Computer Incidence Response Team. CSIRT stands for Computer Security Incidence Response Team (Shierka et al., 2015). The performance of Saudi Arabia as per the indicators of technical pillar is shown in Table 5 (GCI, 2017):

Table 5: Assessment of Performance of Saudi Arabia in Technical Pillar

SNo	Indicator	Performance	Assessment Details
1	National CERT / CIRT / CSIRT	High	Countries like United States (https://www.us-cert.gov/), Singapore (https://www.csa.gov.sg/singcert), Australia (https://www.cert.gov.au/) have established their respective CERT. Saudi Arabia has also established a national CERT (CERT-SA, 2018). So, its performance is assessed as high in this indicator.
2	Government CERT / CIRT / CSIRT	High	The Saudi national CERT is under the government. So, Saudi Arabia's performance is assessed as high in this indicator.
3	Sectoral CERT / CIRT / CSIRT	Low	United States has established the Industrial Control Systems (ICS) CERT to address risks related to critical infrastructure sectors (https://ics-cert.us-cert.gov/). Sri Lanka established the Financial Sector Computer Security Incident Response Team (FINCSIRT) in 2014. It checks the computer security alerts and incidents affecting banks and other financial institutions in Sri Lanka (https://www.fincsirt.lk/). Saudi Arabia has not established any sectoral CERT. So, it has a low performance in this indictor.
4	Standards implementation framework for organizations	High	Malaysia established the Information Security Certification Body (http://www.cybersecurity.my/en/) to manage information security certifications as per international standards and guidelines. Saudi Arabia has established standards for organizations (CITC, 2018). So, it has a high score in this indicator.
5	Standards and certifications for professionals	Low	Saudi Arabia needs to establish standards and certifications for professionals like USA, Singapore etc. So, it has scored low in this indicator.
6	Child online Protection	High	Singapore has established Internet Code of Practice for Internet Service Providers to protect children online (Infocomm Media Development Authority, 2017). Saudi Arabia has adopted an executive resolution on child protection in 2015 (NATLEX, 2015). So, it has scored high in this indicator.
7	Overall	High	Overall, Saudi Arabia has performed satisfactorily in the technical pillar of cyber-security. However, it needs to establish sectoral specific CERTs as well as develop standards and certifications for professionals.

Organizational Pillar

The organizational pillar depicts practices in areas like existence of a cyber-security strategy, responsible agency and cyber-security metrics. The performance of Saudi Arabia as per the indicators of organizational pillar is shown in Table 6 (GCI, 2017):

Table 6: Assessment of Performance of Saudi Arabia in Organizational Pillar

SNo	Indicator	Performance	Assessment Details
1	Cyber-security Strategy	Low	United Kingdom (UK) has established its second national cyber-security strategy 2016-2021. This strategy aims to secure UK from cyber-threats in collaboration with private sector (UK Government, 2016). Russia adopted its doctrine of information security in 2000 and updated it in 2016. Each government entity in Russia performs an annual audit of its networks and systems in line with this doctrine (MoFA, 2016). Canada also possesses a cyber-security strategy and updated it in 2016 using public consultation (Solomon, 2016). However, Saudi Arabia is still developing its national cyber-security strategy. So, it scores low in this indicator.
2	Responsible agency	Average	Singapore has established cyber-security council in 2015 to oversee the implementation of cyber-security strategy, operations, education, outreach and eco-system development (https://www.csa.gov.sg/#). Saudi Arabia has set up a national authority for cyber security to protect its networks, systems and data. The authority aims to defend national security and sensitive infrastructure. This authority is headed by the Minister of Interior (Reuters, 2017). However, Saudi Arabia needs to further strengthen this authority. So, Saudi Arabia scores average in this indicator.
3	Cyber-security metrics	Low	Netherland uses cyber-security metrics to annually review cyber-security threats and development of cyber-security counter measures. This review is published in the annual publication called Cyber Security Assessment Netherlands (2018). Saudi Arabia has yet to implement any such measure. So, it scores low in this indicator.
4	Overall	Low	Overall, Saudi Arabia has scored low in organizational pillar. It needs to develop its cyber-security strategy, strengthen its cyber-security authority and develop pertinent cyber-security metrics.

Capacity Building Pillar

The capacity building pillar involves technical elements and human resources to combat cyber-crimes. It includes standardization bodies, best practices of cyber-security, research and development programs, raising public awareness, cyber-security education and training, cyber-security incentives for organizations etc. The performance of Saudi Arabia as per the indicators of capacity building pillar is shown in Table 7 (GCI, 2017):

Table 7: Assessment of Performance of Saudi Arabia in Capacity Building Pillar

SNo	Indicator	Performance	Assessment Details
1	Standardization bodies	High	In United States (US), Federal Information Processing Standards (https://www.nist.gov/) and American National Standards Institute (https://www.ansi.org/cyber/) standards are used for cyber-security. ANSI acts as a standardization body in US. Saudi Arabia has developed cyber-security framework and it is overseen by Saudi Arabia Monitory Authority (2017). This framework helps banking, insurance and financing companies to withstand against cyber-security threats in Saudi Arabia. So, Saudi Arabia is assessed as high in this indicator.
2	Cyber-security best practices	High	Canada has established the Investment Industry Regulatory Organization (IIROC). IIROC published cyber-security best practices guide in 2015 (IIROC, 2015). Saudi Arabia has also created cyber-security best practices (CITC, 2018). So, it is assessed as high in this indicator.
3	Research and development programs	Low	Singapore has established the national cyber-security research and development (R&D) program. This program endeavors to develop R&D expertise in cyber-security for Singapore (National Research Foundation, 2018). Saudi Arabia has still to develop such R&D programs. So, it scores low in this indicator.
4	Public awareness campaigns	High	Latvia has conducted a series of public awareness campaigns regarding cyber-security. Such campaigns have included awareness about anti-viruses, firewalls, NoScript etc. (Esidross, 2018). According to "Kingdom of Saudi Arabia – Cyber Readiness at a Glance" report from the Potomac Institute of Policy Studies, Saudi Arabia has increased its cyber-security awareness and capability (Hathaway et al., 2017). So, it ranks high in this indicator.
5	Professional training courses	High	Bulgaria has established International Cyber Investigation Training Academy (ICITA) in 2009 to improve the qualifications of cyber-security specialists. ICITA has conducted a number of professional training courses to achieve its aims (https://e-crimeacademy.com/). Saudi Arabia has also made good progress in conducting professional training courses in cyber-security. So, it ranks high in this indicator.
6	National education programs and academic curricula	High	Germany has several education programs and academic curricula related to information security (IS). Several German universities and institutes provides degrees and certificates in IS (https://www.kastel.kit.edu/). Saudi Arabia has Department of Forensic Computing and Cyber Security in University of Prince Mugrin (https://www.upm.edu.sa/). Prince Sultan University in Saud Arabia is offering Master of Science in Cyber-security (http://www.psu.edu.sa/en). So, Saudi Arabia has been doing well in creating national education programs and academic curricula for cyber-security. Therefore, it ranks as high in this indicator.
7	Incentive mechanisms	Low	Korea Internet Service Agency (https://www.kisa.or.kr/eng/main.jsp) supports new companies to commercialize their business models and enhance cyber-security through various programs. It has also established service to support new companies to gain global competitive advantage in cyber-security. Saudi Arabia

SNo	Indicator	Performance	Assessment Details
			has yet to establish such incentive programs for its companies. So, it ranks low in this indicator.
8	Home grown cyber-security industry	Low	Ireland has a favorable business environment, low taxes, talented pool of highly-skilled cyber-security individuals and good base for access to European markets. So, it has made a good progress in developing a home-grown cyber-security industry (Hunt, 2016). Saudi Arabia has yet to made progress in developing a home-grown cyber-security industry. So, it scores low in this indicator.
9	Overall	High	Overall, Saudi Arabia has scored high in capacity building pillar of GCI (2017). However, it needs to develop cyber-security R&D programs. It needs to provide incentives to its companies to adopt cyber-security framework. Also, it needs to develop home-grown cyber-security industry.

Cooperation Pillar

Cooperation pillar considers collaborative efforts in cyber-security among nations in national and international domains. It also considers collaborations between public and private sector, as well as inter-agency partnerships. The performance of Saudi Arabia as per the indicators of cooperation pillar is shown in Table 8 (GCI, 2017):

Table 8: Assessment of Performance of Saudi Arabia in Cooperation Pillar

SNo	Indicator	Performance	Assessment Details
1	Bilateral agreements	High	Singapore has signed 7 agreements on cyber-security (Bhunia, 2017). Saudi Arabia has also signed bilateral agreements on cyber-security. It has signed cyber-security agreements with United States (Bureau of Political-Military Affairs, 2018) and United Kingdom (Saudi Gazette, 2018). So, it scores high in this indicator.
2	Multilateral agreements	Low	Nordic National CERT collaboration has enabled Denmark, Finland, Iceland, Norway and Sweden to collaborate with each other in the area of cyber-security (Swedish Civil Contingencies Agency, 2015). Saudi Arabia has not entered into multi-lateral agreements in the area of cyber-security. So, it scores low in this indicator.
3	International forums participation	High	Most of the countries score high in the indicator of international forums participation. The Forum for Incidence Response and Security Teams (FIRST) was founded in 1990 and has members from 90 countries. The number of teams of countries in FIRST are: United States – 89, Japan - 33, Germany - 31, Spain - 23, United Kingdom - 18, Norway – 13, Singapore - 11 teams etc. Saudi Arabia has 1 team from Saudi Telecom Company (https://www.first.org/). So, it scores high in this indicator.
4	Public-private partnerships	High	United Kingdom is working with its local company Netcraft to improve cyber-security (https://www.news.netcraft.com/). The Saudi National Authority for Cyber-Security is focusing on building public-private partnerships in accordance with Saudi Vision 2030 (Center for International Communication, 2017). So, it scores high in this indicator.
5	Interagency partnerships	High	United States has developed inter-agency security information sharing agreement in 2015. The Multi-lateral Information Sharing Agreement (MISA) binds agencies from defense, health, justice, intelligence and energy to work collaboratively to improve cyber-security (https://www.dni.gov/). South Africa has established national cyber-security hub under the National Cyber-security Policy Framework of 2012. This hub fosters collaboration between industry, government and civil society on all cyber-security incidents (https://www.cybersecurityhub.gov.za/). Saudi National Authority for Cyber-Security is also promoting inter-agency partnerships (Center for International Communication, 2017). So, it scores high in this indicator.
6	Overall	High	Overall, Saudi Arabia has scored high in cooperation pillar of GCI (2017). However, it needs to work on developing multi-lateral agreements on cyber-security.

CONCLUSION

With the expansion of ICT networks, devices and services; cyber-crimes are also increasing. Cyber-crimes threaten any nation's financial position and security. Billions of dollars are lost each year globally in cyber-crimes. Millions of people world-wide have been the victims of various kinds of cyber-crimes. So, it is essential for countries to develop the necessary defense mechanisms against cyber-crimes. The countries need to ensure that they have the necessary technological and legal framework to protect themselves against cyber-crimes.

Over the years, Saudi Arabia has witnessed multi-fold increase in the number of internet users. It is also victim of rising cyber-attacks. Saudi Arabia has faced the highest number of cyber-attacks among the Arab countries. Most Saudi institutions have experienced some form of cyber-crime.

In order to defend against cyber-crimes, Saudi Arabia formed the anti-cybercrimes law in 2007. This law identifies various cyber-crimes and determines their punishments. This law covers essential areas to combat cyber-crimes like prevention of data interception, data interference, system interference and illegal access. It also contains provisions to protect against invasion of privacy, maintenance of public order and morals, and prevention of cyber-terrorism. At the same time, it penalizes attempt to commit cyber-crimes even if they were unsuccessful. It also states the investigation and prosecution bodies against cyber-crimes. However, this law does not protect adequately against identity theft in non-financial matters and transferring and possessing of data. It does not protect privacy of data sufficiently. Cyber bullying is not defined in this law. Also, it does not contain provisions regarding "aiding and abetting" to commit cyber-crimes.

In order to determine the preparedness of countries to defend against cyber-crimes, ITU has developed the Global Cyber-security Index (GCI). Singapore is ranked 1st, US is ranked 2nd and Saudi Arabia is ranked 46th in GCI. Saudi Arabia is grouped in maturing stage of GCI. The performance of Saudi Arabia is assessed against the 5 pillars of cyber-security given by GCI – viz. legal, technical, organizational, capacity building and cooperation. Saudi Arabia has performed satisfactorily in the legal, technical, capacity building and cooperation pillars. But its performance is assessed as low in the organizational pillar.

Saudi Arabia has set up good training programs on its cyber-security law and regulations. It has established a national CERT, developed cyber-security standards for organizations and adopted an executive resolution on child protection in 2015. It has developed a cyber-security framework, created cyber-security best practices, launched cyber-security public awareness campaigns, conducted cyber-security professional training courses, and created cyber-security national education programs and academic curricula. It has signed bilateral agreements on cyber-security with leading nations and participates actively in international forums. It is also developing public-private as well as inter-agency partnerships regarding cyber-security.

However, Saudi Arabia needs to improve in certain areas to be among the leading nations of cyber-security. It needs strengthen its anti-cybercrimes law and cyber-security regulations. It needs to establish sectoral CERTs, and develop standards and certifications for professionals. Further, it needs to create a national cyber-security strategy, strengthen its national authority for cyber-security and develop cyber-security metrics. It needs to develop R&D programs, provide incentives to its companies to enhance cyber-security, and promote home-grown cyber-security industry. Also, it should enter into multi-lateral agreements in cyber-security.Based on the above, it can be stated that currently Saudi Arabia is semi-prepared to defend itself against cyber-crimes. By improving in the necessary areas, it can be among the leading nations of cyber-security.

References

ACCL (2007, March 26). Saudi Anti-Cyber Crime Law. Retrieved from https://www.boe.gov.sa/

Almerdas, S. (2014). The Criminalisation of Identity Theft under the Saudi Anti-Cybercrime Law 2007. *Journal of International Commercial Law and Technology*, 9(2), 80-93.

Arab News (2017, September 30). Study: 60% of Saudi institutions hit by virus attacks, malware. Retrieved from http://www.arabnews.com/

Bhunia, P. (2017, October 27). Singapore enters into seventh bilateral agreement on cyber-security cooperation. Retrieved from https://www.opengovasia.com/

Boni, W.C., & Kovacich, G.L. (1999). *I-Way Robbery: Crime on the Internet*. 1st ed. UK: Butterworth Heinemann.

Bronk, C. & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival: Global Politics and Strategy*, 5(22), 81-86. https://doi.org/10.1080/00396338.2013.784468

Bureau of Political-Military Affairs. (2018, March 23). U.S. Security Cooperation With Saudi Arabia. Retrieved from https://www.state.gov/

Center for International Communication (2017, November 1). Saudi Arabia Sets Up Cyber Security Authority To Boost National Security. Retrieved from https://cic.org.sa/

CERT-SA (2018). Computer Emergency Response Team for Saudi Arabia. Retrieved from https://www.cybersecurityintelligence.com/

Cisco (2017, June 7). The Zettabyte Era: Trends and Analysis. Retrieved from https://www.cisco.com/c/en/us/solutions/

Council of Europe (2015, September 4). GLACY support to Mauritius: Judicial training courses on cybercrime delivered. Retrieved from https://www.coe.int/en/

Cyber Security Assessment Netherlands (2018, August 7). Retrieved from https://www.ncsc.nl/english/

Esidross (2018). Retrieved from https://www.esidross.lv/category/bezmaksas-risinajumi/page/2/

Financial Express (2017, July 13). UN cyber security index 2017: At 23rd, India ahead of Germany, China, but Singapore on top. Retrieved from https://www.financialexpress.com/

Floyd, J.T. (2006, March 8). A Guide to Cyber Crime Laws. Retrieved from https://www.johntfloyd.com/\

Forbes Middle East (2018, March 28). Arab Countries Facing The Highest Number Of Cyber Attacks. Retrieved from https://www.forbesmiddleeast.com/en/

GCI (2017). Global Cyber-security Index 2017. Retrieved from https://www.itu.int/en/

HachRead (2015, August 17). Hackers Target Saudi Government Websites with "Good Intentions". Retrieved from https://www.hackread.com/

Halder, D., & Jaishankar, K. (2011). *Cyber-crime and the Victimization of Women: Laws, Rights and Regulations*. Hershey, PA, USA: IGI Global. https://doi.org/10.4018/978-1-60960-830-9

Hathaway, M., Spidalieri, F., & Alsowalim, F. (2018, September). Kingdom of Saudi Arabia: Cyber Readiness at a Glance. Retrieved from http://www.potomacinstitute.org/

Hunt, G. (2016, February 24). Ireland can be cyber-security capital of the world – report. Retrieved from https://www.siliconrepublic.com/

ICT Facts & Figures (2017). New data visualization on Internet users by region and country, 2010-2016. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

IIROC (2015). Cyber-security Best Practices Guide - For IIROC Dealer Members. Retrieved from http://www.iiroc.ca/

Infocomm Media Development Authority (2017, November 3). Internet Content Regulation. Retrieved from https://www.imda.gov.sg/

Kaspersky Lab (2017, March 7). From Shamoon to Stonedrill - Wipers attacking Saudi organizations and beyond. Retrieved from https://media.kasperskycontenthub.com/

Masters, G. (2017, June 26). Loss from cybercrime exceeded $1.3B in 2016, FBI report. Retrieved from https://www.scmagazine.com/

Ministry of Communications & Information Technology (2012). Cybercrime Costs Saudi Arabia SR 2.6 Bn A Year. Retrieved from https://www.mcit.gov.sa/en/

MoFA (2016, December 5). Doctrine of Information Security of the Russian Federation. Retrieved from http://www.mid.ru/en

National Research Foundation (2018, January 15). National Cyber-security R&D Programme. Retrieved from https://www.nrf.gov.sg/

NATLEX (2015). Saudi Arabia - Elimination of child labor, protection of children and young persons. Retrieved from http://www.ilo.org/

New Zealand's Cyber Security Strategy (2016). Action Plan Annual Report. Retrieved from https://www.dpmc.govt.nz/

O'Brien, D. (2017, July). Internet Security Threat Report: Ransomware 2017. Retrieved from https://www.symantec.com/

Omanua (2018). Oman Digital Strategy. Retrieved from http://www.oman.om/

Pitts, V. (2016). *Cyber Crimes: History of World's Worst Cyber Attacks*. 1st ed. India: Alpha Editions.

Reuters (2017, November 1). Saudi Arabia sets up new authority for cyber security. Retrieved from https://www.reuters.com/

Sadowsky, G., Zambrano, R., & Dandjinou, P. (2004). Internet Governance: A Discussion Document. In D. MacLean, *Internet Governance: A Grand Collaboration*. New York, USA: United Nations ICT Task Force

Saudi Arabian Monetary Authority (2017, May). Cyber Security Framework. Retrieved from http://www.sama.gov.sa/en-US/

Saudi Gazette (2018, March 10). Saudi Arabia, UK announce strategic partnership in joint communiqué. Retrieved from http://saudigazette.com.sa/

Shierka, I., Morgus, R., Hohmann, M. & Maurer, T. (2015, May). *CSIRT Basics for Policy-Makers - The History, Types & Culture of Computer Security Incident Response Teams*. Retrieved from http://www.digitaldebates.org/

Smith (2017, January 24). Saudi Arabia again hit with disk-wiping malware Shamoon 2. Retrieved from https://www.csoonline.com/

Solomon, H. (2016, August 16). Ottawa announces public consultation on cyber security strategy. Retrieved from https://www.itworldcanada.com/

Sutton, M. (2018, March 17). Cyber-attack on Saudi plant designed to cause explosion. Retrieved from http://www.itp.net/

Swedish Civil Contingencies Agency (2015, March 19). Nordic cyber security exercise was conducted in Linköping. Retrieved from https://www.msb.se/en/

UK Government (2016). National Cyber Security Strategy 2016 to 2021. Retrieved from https://www.gov.uk/

Walker, J. (2017, November 23). APT targeting Saudi Arabian government. Retrieved from https://portswigger.net/