CYBERCRIME AND ANALYSIS OF LAWS IN KINGDOME OF SAUDI ARABIA

A Thesis

Presented to

the Faculty of the Department of Information and Logistics Technology

University of Houston

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Information System Security

By

Afnan Alabdulatif

May 2018

SIGNATURE PAGE

_____

Afnan Alabdulatif

APPROVED

_____

Christopher Bronk, PhD
Committee Chair, Assistant Professor
Information and Logistics Technology

_____

Wm. Arthur Conklin, PhD
Associate Professor
Information and Logistics Technology

_____

Denise M Kinsey, PhD
Assistant Professor
Information and Logistics Technology

_____

George Zouridakis, PhD
Associate Dean for Research and Graduate Studies
College of Technology

_____

Daniel M Cassler, M.A
Department Chair, Information and
Logistics Technology

DEDICATION

This work is dedicated to my parents Mr. Abdullah M Alabdullatif and Mariam A Alabdullatif for their endless support. You two have been pillars of support, guidance and love in my life. I never would have made it here without you,

Love you both

ACKNOWLEDGMENT

I would like to sincerely thank my supervisor, *Dr. Christopher Bronk*, for his guidance and support throughout the process of writing this thesis, and especially for his confidence in me and his continues motivation. You have been an excellent mentor and a great inspiration for me. I would also like to thank *Dr. Wm. Arthur Conklin* for his support and treasured instructions. The knowledge and wisdom you have imparted upon me has been a great help and support throughout my journey.

I would also like to take this opportunity to thank my friends and classmates especially *Reem Sowayan, Mariam Bubshait, Annie Jamshed, and Pablo Delgado.* I want to express my deepest gratitude for you four for always believing in me, you all supported me to peruse my dreams in your own ways. You are a major contribution behind my success and achievements.

Last, I would like to thank my brothers, *Mohammad, Ahmed, Muhannad, and Yousif* for their endless love, support, and engorgements.

ABSTRACT

This thesis examined cybercrime and cybercrime legislation in Saudi Arabia. It introduced the Saudi Arabian background emphasizing on Internet. It Stated the current situation of cybercrime in the Kingdome. Moving forward, it Gave literature review of different sources relevant to this research area. This thesis has two main sections: one is the major cybercrimes in Saudi Arabia. This section included analysis of the major attacks that hit the kingdom. It explained the incident summary and the attack tactics techniques, and procedures used. The second section is an analysis of the current legislations and countermeasures used to combat cybercrime in the Kingdome. last gave the recommendations that can help resolving or enhancing the current situation as well as the challenges faced while conducting this research.

Table of Contents

Table of Figures

LEGISLATIONS

CHAPTER ONE

1. INTRODUCTION

1.1 Background of Saudi Arabia

The Kingdom of Saudi Arabia (KSA) is the largest country in the Arabian Peninsula and is located in the southwest corner of Asia. The Kingdom is at the crossroads of Europe, Asia and Africa. Saudi Arabia is about one-fourth the size of United States, it is spread over 2,150,000 square kilometers (830,000 square miles), occupying almost 80 % of the Arabian Peninsula. The total Saudi population as 2017 amounted is 32,552,336 million. (Ministry of foreign affairs n.d.)

1.2 Background of the Internet in KSA

Internet service was officially made available in the Kingdom of Saudi Arabia in 1997. The Internet has become an integral part of the Saudi society and its economy (CITC 2009). The annual report of Kingdome's Communication and Information Technology Commotion (CITC) during 2016 indicated that the percentage of Internet access has risen from 47% in 2011 to about 74.9% by the end of 2016. The number of current internet users in the Kingdom is estimated to be 24 million. Due to increased use of social media channels, content channels (like YouTube and Snapchat), and internet-based games, demand for internet and broadband services has increased. (CITC 2016).

According to the same annual report of 2016, It is expected that the spending growth on ICT services will continue with greater momentum, and information security will become an essential component of digital transformation strategies in the Kingdom. Moreover, there has been a rise in the number of businesses that aspire to implement advanced and proactive information security solutions (CITC 2016).

The report also revealed the total capacities of the International Internet connectivity for 2016, which has risen to 114% or about 3185 gigabytes /sec as compared to 1484 gigabytes/sec in 2015. The reason for this rise is expected increase in demand for internet use. (CITC 2016).

1.3 Current Cybersecurity in Saudi Arabia

Kingdom of Saudi Arabia's National Cyber Security Center (NCSC) reported a threat overview of KSA during the period from July 1st to September 30th, 2017 "third quarter". Some 34 incidents were responded to by the NCSC's Incident Response team. In addition, total of 113 threat alerts were released to relevant CNI's for their action supported with Indicator of Compromise (IoC's) and proper mitigation plans (NCSC 2017).

Intrusion and Intrusion Attempts represented most of these threat alerts with 59 %, then malicious code as second highest with 19%. Intrusions and intrusion attempts typically exploit known vulnerabilities, brute force, New attack signature, privileged account compromise, unprivileged account compromise, application attacks, remote command execution, or remote access tool (RAT). As for malicious code, it is software code that was developed to run malicious commands including known forms of malware such as virus, worm, and Trojan (NCSC 2017). The report stated that most of the threat alerts were directed to government sector – about 65 %; may be due to the geopolitical to target KSA, and then Energy and Telecommunication sectors next as the most important to national economy with 8% and 7% alerts (NCSC 2017).

The NCSC reported another threat overview during the period from October 1st to December 31st, 2017 "fourth quarter" where the threat alert numbers were slightly higher (up 7 %) as compared to the prior quarter. This report showed that "Unauthorized Access, Modification and Usage" and "Malicious Code" threat categories represented the majority of the threat landscape in KSA. The intrusion attempts have decreased from the third quarter, while "Malicious Code", "Unauthorized

Access" and "Information Leakage" showed an increase, which indicates that the threat actors were successful in gaining access to affected systems. Moreover, it reflects a threat actors' objective in harvesting credential and identity information. Similar to the third quarter most of the threats were targeting government entities as well as Energy and Telecommunication sectors, which reflects the threat actors' intent in impacting the national economy. While threats directed towards government sector have slightly dropped during fourth quarter, an increase was observed in energy and telecommunication sectors. This clearly indicates that threat actors' intent has been shifted towards economic impact (NCSC 2017).

The use of computer and computer networks is evolving rapidly introducing new and more complicated technologies, like the Cloud and Internet of Things (IoT). Hence, the number of cyber security threats is increasing, and it becomes a necessity for the Kingdom to proactively keep up with this trend by providing the appropriate defense measures, technology and guidance to protect its information and communication systems against cyberattacks, and to work relentlessly to safeguard the confidentiality, integrity, and availability of national critical assets and infrastructure. Moreover, to fulfil the aim of the Kingdome's Vision 2030, better information sharing, and clear legal frameworks regarding data security and privacy is needed.

1.4 Statement of the Research Problem

The research focus for this thesis is on cybercrime in Saudi Arabia. A considerable number of those who become victims of cybercrimes still do not consider reporting their experiences to law enforcement agencies. This in some cases is due to the common perception that cybercrime is not a punishable offence in Saudi Arabia. In other cases, due to the lack of awareness of the existing laws related to cybercrimes, and a misconception that Saudi Arabia does not have a sufficient legal system regarding cybercrimes.

1.5 Objectives of the research

- Discover degree of cybercrime in Saudi Arabia.
- Identify Saudi Arabian law in regard to cybercrime.
- Examine to what extent the laws are effective to combat cybercrime.
- Cover the current countermeasures to combat cybercrimes

1.6 Scope of the Research

This research paper aims to identify how Saudi Arabia is combating cybercrime by analyzing the existing legal documents that can be used to defend against cybercrimes. Furthermore, the effort taken to make Saudi Arabia a safer place taking inconsideration the vital importance of cybersecurity in the lives of community members. This effort is represented through the countermeasures taken to contribute to the achievement of a technical renaissance serving the future of the Kingdom's national economy.

CHAPTER TWO

2. Literature Review

2010 - Is a Shari'ah-based Law Compatible with Cybercrime? An Inquiry into the Saudi Regulations on Internet Fraud

This paper provides a detailed analysis of Saudi regulations on Internet fraud, in an attempt to assess the extent to which the Kingdom's legal system, which is based primarily on Islamic principles, is compatible with cybercrime. The author defined Internet fraud in details. After that he discussed and analyzed the Islamic perspective on fraudulent and deceptive activities.

The author concluded that Shari'ah law, which is concerned with protecting property, incriminates those acquiring wealth through unlawful means and imposes penalties on them, but leaves the specification of these penalties to the judgment of rulers and judges. On this basis, Saudi legislators have created a number of laws, which have provisions pertaining to Internet fraud. Then he reviewed these laws to assess the extent to which they address Internet fraudulent crimes in the Kingdom. As a result, he found that the Anti-Cybercrime Act constitutes the main legal reference for controlling Internet fraud in Saudi Arabia. However, it does not tackle the crime in all its detail. The discussion in this paper revealed that the Act falls short in addressing many aspects of Internet fraud. He also concluded that it is evident that significant gaps still exist in the law with regard to issues like jurisdiction and enforcement mechanism.

The author's recommendation to address this problem was by highlighting two possible legislative approaches in response to Internet fraud: one is augmentation of existing criminal provisions through amendments. Second, is the creation of new legislation, whether in the form of an omnibus statute which comprehensively deals with Internet fraud, or specific statutes addressing specific forms of electronically perpetrated fraud (Algarni 2010).

2013 - Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future

This paper discussed the position of Saudi Arabian government against cybercrime and its Information Technology Act. It analyzed the cybercrime in the Kingdom and the anti-cybercrime law. The author discussed the current situation of cybercrime in Saudi Arabia at that time by stating some statistics about Internet users in the Kingdom. The penetration rate was 54.1%, Cybercrime has cost the Kingdom $ 700 million in year 2012, more than 3.6 million people fell victim to cybercrime in year 2012. The study found 40 % of adults in KSA do not know that malware can operate in a discreet fashion, making it hard to know if a computer has been compromised, and more than half (55 %) are not certain that their computer is currently clean and free of viruses.

The authors then talked about the Cyber laws that exist in the Kingdom, and conclude that although the law existed since 2007, non-awareness among youth has created potential imbalance between safe internet usage and vulnerability against crime. Most of the people know about cybercrime but very less is aware of the associated legislation to combat these crimes (Elnaim 2013).

The Criminalization of Identity Theft under the Saudi Anti-Cybercrime Law 2007

The author discussed that Saudi Arabia enacted the Anti-Cybercrime Law 2007 to handle various harmful activities that occur in cyberspace, including identity theft. The author found that article 4(2) of the 2007 Anti-Cybercrime Law is capable of encompassing all possible methods of obtaining the personal information of others including phishing, pharming, using malware and hacking. With any of these methods, once the perpetrator attains the financial information of the victims without lawful cause, she would be liable for committing an offence under article 4(2), irrespective of whether he/she uses it for further crimes or not. Moreover, he added, that the broad

meaning of ‘attaining’ in article 4(2) seems able to encompass any method that might be created in the future to acquire the confidential information of people. However, the author believes that article 4(2) clearly limits the criminalization to only attaining information that relates to ‘bank or credit data, or data pertaining to ownership of securities’. By this condition, the Anti- Cybercrime Law limits the application of Article 4(2) to only identity theft related to financial matters. According to the author, this means that acquiring the identity-related information of others for non-financial motivations – such as to impersonate another person in order to tarnish his or her reputation – is not an offence under the Anti-Cybercrime Law. However, this paper argued that because the former is more widespread than the later and the former not only causes harm to the victim but also may threaten the economy as whole, it seems understandable that the Saudi legislators focused on the first type and makes it an offence through article 4(2) of the Anti-Cybercrime Law. (Almerdas 2014).

The author highlighted a notable weakness in dealing with identity theft under Saudi law, which is the Anti-Cybercrime Law has failed to criminalize another act related to identity theft, namely transferring and possessing materials (data and programs) for the purpose of identity theft. Thus, the Anti-Cybercrime Law would not be able to deal with those who transfer or sell, for instance, the credit card details of individuals or with those who, for example, possess other people’s identity-related information. The author recommendation was the Anti-Cybercrime Law needs to criminalize the identity theft of transferring and possessing materials to fill the gap in the existing law, which would strengthen the legal response against this form of cybercrime (Almerdas 2014).

2017 - Cybercrime in Saudi Arabia: fact or fiction?

This paper addresses the following questions:

- What is the actual situation of computer crime in the Kingdom of Saudi Arabia?
- Are the existing systems a sufficient deterrent? What are the most prominent disadvantages, and why?
- Who is responsible for the failure of the system to deal with computer crime?

This paper has shown that it is apparent that the number of cybercrimes and financial losses incurred by the government has increased annually. Two Norton (a U.S. security firm) reports from 2012 and 2016 have shown an increase in the number of people affected by cybercrime, from 3.6 million in 2012 to 5.6 million people in 2016. The fight against cybercrime requires both states and individuals to take a long-term and strong stance against it (Amro 2017).

2017 - Kingdom of Saudi Arabia Cyber Readiness at A Glance

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Saudi Arabia's current preparedness levels for cyber risks. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0, which are: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development, diplomacy and trade, and Defense and crisis response. According to this assessment, Saudi Arabia is still insufficiently prepared in all of the CRI essential elements, although it has made considerable progress in becoming more cyber ready.

There is still a lack of sufficiently trained court judges, prosecutors, lawyers, and law enforcement officials to address different elements of cybercrime and successfully investigate and prosecute offenders. (Melissa Hathaway 2017)

There is no formal customer notification or registration requirement before the government or a company can collect or process data. The lack of data governance processes or regulations leaves data transfer and data residency requirements ambiguous. There is no clear definition of "personal data," and no requirement to notify data security breaches to any individual or entity in Saudi Arabia (Melissa Hathaway 2017)

CHAPTER THREE

3. RESEARCH DESIGN AND METHODOLOGY

3.1 Research Design

The design used in this research is combination of a descriptive design and an exploratory design. According to University of Sothern California (USC) the descriptive research is used to obtain information concerning the current status of the topic. Descriptive studies can yield rich data that lead to important recommendations in practice. It is an approach to collects a large amount of data for detailed analysis. While an exploratory design is conducted about a research problem when there are few or no earlier studies to refer to or rely upon to predict an outcome. The focus is on gaining insights and familiarity for later investigation or undertaken when research problems are in a preliminary stage of investigation. Exploratory designs are often used to establish an understanding of how best to proceed in studying an issue or what methodology would effectively apply to gather information about the issue. This design is a useful approach for gaining background information on a particular topic (USC n.d.)

This research follows the descriptive design. However, since there are only few research papers about this topic which are mentioned in the literature review chapter, this research also follows the exploratory design. Therefore, it is a combination of both designs.

3.2 Research Instrument

The research instrument used in this research paper is the collection and analysis of legal documents.

3.3 Data Collection Method

Primary data are legal documents from governmental websites, and secondary data is material available through the internet, like articles reports, newspapers and some other kinds of publications on matters relating to the subject. Collected data through unstructured interview with legal Cyber Security professionals in Saudi Arabia

3.4 Challenges of the Research

Lack of public resources represents a significant gap for conducting this research. This includes:

- Lack of publicly available official documentation about attacks technical reports; and
- Lack of publicly available official documentation about cybercrimes cases.

CHAPTER FOUR

4. Saudi Arabia's Major Cybercrimes

4.1 Shammon - 2012

4.1.1 Summary of the incident

On 15 August 2012, the computer network of Saudi Aramco was struck by a self-replicating virus that infected as many as 30,000 of its Windows- based machines. Despite its vast resources as Saudi Arabia's national oil and gas firm, Aramco, according to reports, took almost two weeks to recover from the damage. The virus erased data on the infected computers by replacing all of it with an image of a burning American flag. (Bronk 2013)

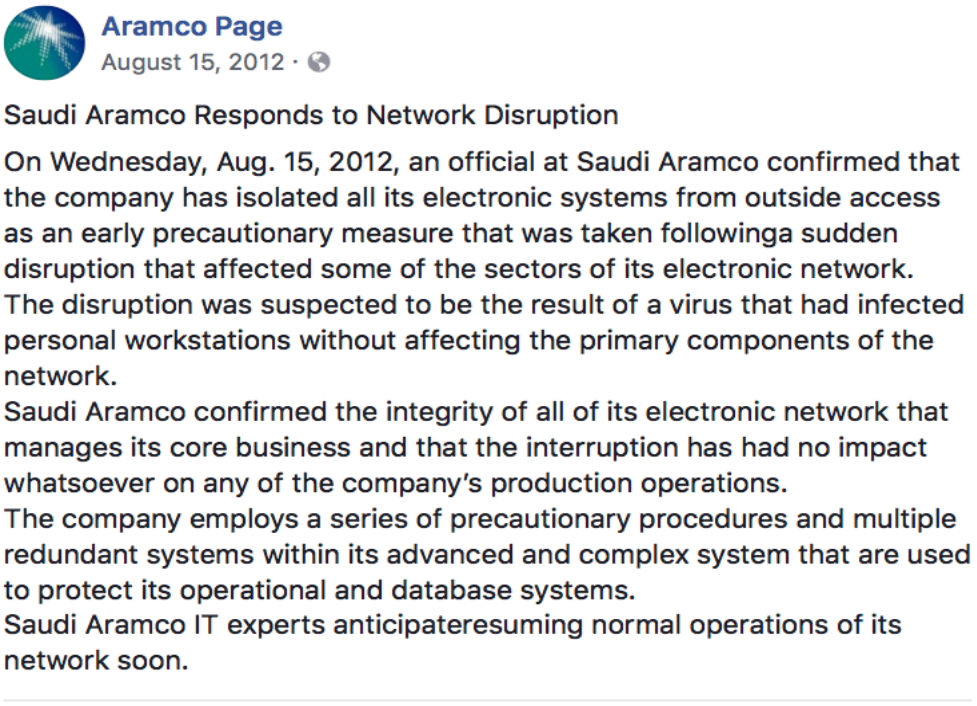

Figure 1 Aramco Page - Saudi Aramco Responds to Network Disruption (Aramco 2012)

The malware that spread across Aramco's computers, Shamoon, enabled its creators to delete files and contents of entire hard drives. The virus corrupted files on infected computers and overwrote their master boot records, rendering the machines unusable (Bronk 2013).

It has been suggested that introducing Shamoon onto Aramco's network required physical access to an internal computer, which raises concerns about the company's physical security. (Bronk 2013)

Aramco was able to restore its main internal network services by 26 August 2012, reporting that it had cleaned all affected workstations and resumed normal business (Bronk 2013). Former U.S. CIA director Leon Panetta described Shamoon as "one of the first viruses that can actually take down and destroy computers to the point that they had to be replaced."

4.1.2 Tactics and Techniques

The name Shamoon comes from a folder name within the malware executable. Shamoon is also known as W32.Disttrack. According to Symantec, Shamoon consists of three components (Symantec 2012):

1. Dropper—the main component and source of the original infection. It drops a number of other modules.
2. Wiper—this module is responsible for the destructive functionality of the threat.
3. Reporter—this module is responsible for reporting infection information back to the attacker.

Symantec further explained each component:

The dropper copies itself to %System%\trksvr.exe, then drops the following files embedded into resources:

- A 64-bit version of the dropper component: %System%\trksrv.exe (contained in the “X509” resource)
- Reporter component: %System%\netinit.exe (contained in the "PKCS7" resource)
- Wiper component: %System%\[NAME SELECTED FROM LIST].exe (contained in the "PKCS12" resource)

The Wiper involves the following functionality:

- Deletes an existing driver from the following location and overwrites it with another legitimate driver:
    - %System%\drivers\drdisk.sys
    - The device driver is a clean disk driver that enables user-mode applications to read and write to disk sectors. The driver is used to overwrite the computer’s MBR but may be used for legitimate purposes.
    - The file is digitally signed
- Executes the set of commands that collect file names, which will be overwritten and writes them to f1.inf and f2.inf:
- Files from the f1.inf and f2.inf will be overwritten with the JPEG image of burning American flag. Overwritten files are thus rendered useless.
- Finally, the component will overwrite the MBR so that the compromised computer can no longer start

The Reporter is responsible for sending infection information back to the attacker. Information is sent as HTTP GET request and is structured as follows:

http://[DOMAIN]/ajax_modal/modal/data.asp?mydata=[MYDATA]&uid=[UID]&state=[STATE]

The following data is sent to the attacker:

- [DOMAIN]—a domain name
- [MYDATA]—a number that specifies how many files were overwritten
- [UID]—the IP address of the compromised computer
- [STATE]—a random number

4.2 Shamoon2 – 2016/2017

Shamoon made a surprise return and attacked different targets in Saudi Arabia in 2016 and 2017. Shamoon2 shares many similarities with the previous Shamoon of 2012, introducing new tools and techniques. Shamoon2 was used in several waves of attacks

- Attack Wave 1: Wipe systems on November 17, 2016, at 20:45 Saudi time.
- Attack Wave 2: Wipe systems on November 29, 2016, at 01:30 Saudi time.
- Attack Wave 3: Began January 23, 2017, and ongoing, with similar samples and methods as in Waves 1 and 2 (Samani 2017).

This time, Shamoon2 used a photo of the body of Alan Kurdi, the three years old Syrian refugee who drowned in the Mediterranean last year (Symantec 2016)

The malware had a default configuration that triggered the disk-wiping payload at 8:45pm local time on Thursday, November 17, 2016. The Saudi Arabian working week runs from Sunday to Thursday. The attack was scheduled to hit during the weekend, at a time when most employees had gone home. This was to decrease the chance of detection (Symantec 2016).

Palo Alto researchers said:

We have found evidence that the actors use a combination of legitimate tools and batch scripts to deploy the Disttrack payload to hostnames known to the attackers to exist in the targeted network (Falcone 2017).

Our analysis shows that the actors likely gathered the list of known hostnames directly from Active Directory or during their network reconnaissance activities conducted from a compromised host. This network reconnaissance, coupled with the credential theft needed to hardcode Disttrack payloads with legitimate username and password credentials, leads us to believe that it is highly likely the threat actors had sustained access to the targeted networks prior to Shamoon2 attacks. Our research confirms that successful credential theft from targeted organizations was an integral part of the Shamoon2 attackers' playbook, and they used these stolen credentials for remote access and lateral movement (Falcone 2017).

Our analysis also shows an actor distributes Disttrack within the targeted network by first compromising a system that is used as the Disttrack distribution server on that network. The actor then uses this server to compromise other systems on the network by using the hostname to copy over and execute the Disttrack malware. On each of these named systems that are successfully compromised, the Disttrack malware will attempt to propagate itself to 256 additional IP addresses on the local network. This rudimentary, but effective, distribution system can enable Disttrack to propagate to additional systems from a single, initially compromised system in a semi-automated fashion (Falcone 2017).

Shamoon2 worked in a similar way as Shamoon of 2012 as it used three components to infect computers.

- **A dropper**, which creates a service with the name 'NtsSrv' to remain persistent on the infected computer. It spreads across a local network by copying itself on to other computers

and will drop additional components to infected computers. The dropper comes in 32-bit and 64-bit versions. If the 32-bit dropper detects a 64-bit architecture, it will drop the 64-bit version (Symantec 2016).

- **The wiper**, which drops a third component, known as the Eldos driver. This enables access to the hard disk directly from user-mode without the need of Windows APIs. The wiper uses the Eldos driver to overwrite the hard disk with the aforementioned photos of the Syrian boy (Symantec 2016).
- **The reporter**, both Shamoon variant used HTTP request to send the information back to the attacker. However, in case of Shamoon2, according to Palo Alto It appears that the purpose of the new Disttrack, which is Shamoon2, samples were solely focused on destruction, as the samples were configured with a non-operational command and control (C&C) server for communication. Symantec said, the reporter is responsible for handling communications with a C&C server operated by the attackers. It can download additional binaries from the C&C server and change the pre-configured disk-wiping time if instructed by the C&C server. It is also configured to send a report verifying that a disk has been wiped to the C&C server (Symantec 2016).

4.2.1 Wave 2:

Wave 2 was another wave of Shamoon2, similar to the first wave with different payload used to target a second organization in Saudi Arabia. This attack tool was configured to wipe systems twelve days later, on November 29, 2016. This attack wave potentially materially impacted one of the primary countermeasures employed against wiper attacks: Virtual Desktop Interface snapshots. The payload used in this attack was very similar to the November 17, 2016 payload, but exhibited slightly different behaviors and contained hardcoded account credentials specific to the newly

targeted organization. The hardcoded account credentials met Windows password complexity requirements, which suggests that the threat actors obtained the credentials through a previous, separate attack, similar to the November 17, 2016 attack (Falcone 2017).

4.2.2 Wave 3

A third wave was set to wipe systems using the Disttrack malware on January 23, 2017. This wave of Shamoon2 attacks is similar to the other two waves in terms of the attack vectors, payloads and actions taken. This wave implies that Shamoon2 attacks are an ongoing situation and that additional waves of attack are possible in the future (Budd 2017).

NCSC has noticed many organization in the kingdom were infected with destructive attacks using Shamoon2 malware. Accordingly, as NCSC still believes other waves may come if the proper countermeasures are not implemented, warned all organization in the kingdom from Shamoon attack and advise to take appropriate precautions. NCSC described how Shamoon2 works:

1- Gathering (scan) information about the organization using multiple sources.

2- Gaining access to the network in one of the two ways: brute force or phishing emails. Repeating these steps until gaining domain admin credentials.

3- Lateral movement and access to the critical servers (domain controllers or exchange server).

4- Use PSexec.exe to distribute Shamoon2 malware 32-bit ntermgr32.exe and a batch script ntertmgr.bat in the local \SystemRoot\Windows\System32\ folder of all reachable systems in the network

5- Scan and Manual access to the backup servers to delete the backup (if available)

6- Use PSexec.exe to run the batch script and execute Shamoon2 malware and destruct the systems. (NCSC n.d.)

4.3 Stone Drill

Kaspersky Lab discovered a wiper malware which appears to be targeting organizations in Saudi Arabia.

> We're calling this new wiper **StoneDrill**. StoneDrill has several "style" similarities to Shamoon, with multiple interesting factors and techniques to allow for the better evasion of detection.

Samples of the StoneDrill malware were uploaded multiple times to multi-scanner antivirus engines systems from Saudi Arabia between 27 and 30 November 2016.

StoneDrill makes heavy use of evasion techniques to avoid sandbox execution, and anti-emulation techniques in the malware, which prevents the automated analysis by emulators or sandboxes. StoneDrill does not use drivers during deployment (unlike Shamoon) but relies on memory injection of the wiping module into the victim's preferred browser (Kaspersky 2017).

4.4 APT

On 20 November 2017, The NCSC detected a new Advanced Persistent Threat (APT) campaign targeting Saudi Arabia. The observed malicious activities used by the threat actor, was a PowerShell based malware connects to multiple known-bad domains. The malicious PowerShell utilizes HTTP tunneling to communicate with the command and control domains. The HTTP requests and responses contains data exfiltrated from infected machines or commands to be executed by the threat actor. (NCSC n.d.)

NCSC revealed two techniques that have been observed in the delivery and installation stages:

- **Injecting Microsoft Office Documents**

Most of the samples observed were Microsoft Office files containing a macro or a linked object that was delivered through spear phishing emails. Additionally, the malicious documents are sometimes compressed in a password protected .rar file to avoid mail protection mechanisms. The password is usually included in the email body. (NCSC n.d.)

• Accessing compromised Websites

Some samples were delivered using the watering hole or similar techniques such as cross site scripting. The infection was observed through a compromised "legitimate website" where the users were redirected to a malicious website and asked to download a malicious executable. The malicious file would infect the machine with the same VBS and PowerShell scripts. (NCSC n.d.)

4.5 Cyber of Emotion

On 15 August 2015, Al-Riyadh newspaper reported a Saudi group hacked more than 24 government sites within two hours, after government officials ignored messages about a possible attack. On Twitter, the hackers said their team had already warned the administrators of the websites that the sites were not properly secured and that they should do something about it. (Al-Riyadh 2015)

Cyber-Emotion stated via its Twitter account, "After the government websites ignored our messages about a possible attack, our group today announces targeting of poorly secured governmental sites and will inform you about the penetration results." (Al-Riyadh 2015)

The group confirmed via a Hashtag on Twitter (#From_us_rather_from_enemy) that the penetration would not harm the data, but only block access until the appropriate measures are taken. The group said, "We do not want to insult this site nor do any harm, but if it hacked by an

enemy, your private information would have been compromised and published. We are here to let you know that we want to protect government sites before they fall into a very big trap by enemies." (Al-Riyadh 2015)

All visitors to the websites were directed to a page that showed that following

Figure 2: The redirected page by the hackers (Al-Riyadh 2015)

The hackers published all the sites that they managed to penetrate through their account. All the websites appeared to be working properly a few hours after the hacks, which showed that the hackers intention was to reveal how vulnerable those websites (Al-Riyadh 2015). In 2014, the same group hacked the Ministry of Justice's Twitter account and questioned the Ministry over what it said were costs of 168m Saudi riyals ($45m) for developing a website (Aljazeera 2015).

The hacker wrote, mocking the Ministry of Justice about the $45 million, “the 45 million for developing the Ministry’s website, you will be asked about them on the Day of Judgment, this can be used to treat a patient or help a person in need.” The group stated, “We appreciate the efforts of the ministry when it developed its services and facilitate them, but where did 45 million go?” The group stated in another tweet, “Today we break the protection by an amount of 10 riyals Internet cafe subscription.” (Al-Riyadh 2014)

4.6 TRITON

On December 2017, security firm FireEye reported an incident at a critical infrastructure organization where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes.

> We assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations. This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack (FireEye 2017).

FireEye and Schneider declined to identify the victim, industry or location of the attack. However, Cyber security company Dragos said the hackers targeted an organization in the Middle East, while a second firm, CyberX, said it believe the victim was in Saudi Arabia.

Security experts at CyberX who investigated the incident pointed out that Triton was likely developed to target an organization in Saudi Arabia, CyberX vice president Phil Neray said his firm found evidence that the malware was deployed in Saudi Arabia (Finkle 2017)

4.6.1 Summary of the incident

The attacker gained remote access to Safety Instrumented System (SIS) engineering workstation and deployed the TRITON attack framework to reprogram the SIS controllers. During the incident, some SIS controllers entered a failed safe state, which automatically shut down the industrial process and prompted the asset owner to initiate an investigation. (FireEye 2017)

> We assess with moderate confidence that the attacker inadvertently shutdown operations while developing the ability to cause physical damage

The TRITON attack tool was built with a number of features, including the ability to read and write programs, read and write individual functions and query the state of the SIS controller. However, only some of these capabilities were leveraged, the attacker did not leverage all of TRITON's extensive reconnaissance capabilities. (FireEye 2017)

4.6.2 Tactics and technics

The TRITON malware contained the capability to communicate with Triconex SIS controllers (e.g. send specific commands such as *halt* or read its memory content) and remotely reprogram them with an attacker-defined payload. The TRITON sample Mandiant analyzed added an attacker-provided program to the execution table of the Triconex controller. This sample left legitimate programs in place, expecting the controller to continue operating without a fault or exception. If the controller failed, TRITON would attempt to return it to a running state. If the controller did not recover within a defined time window, this sample would overwrite the malicious program with invalid data to cover its tracks. (FireEye 2017)

TRITON was deployed on an SIS engineering workstation running the Microsoft Windows operating system. The malware was named to masquerade as the legitimate Triconex Trilog application. This application is used for reviewing logs and is a part of the TriStation application suite. The malware was delivered as a Py2EXE compiled python script dependent on a zip file containing standard Python libraries, open source libraries, as well as the attacker-developed Triconex attack framework for interacting with the Triconex controllers. Along with the executable, two binary files, inject.bin (malicious function code) and imain.bin (malicious control logic), were deployed as the controller's payload. These file names were hard coded in the Py2EXE compiled python script. (FireEye 2017)

4.7 Summary

From the above attacks incidents, the attackers have something in common which is targeting organizations in various critical and economic sectors in Saudi Arabia. The targets fall into two types: one is Industrial Control Systems at large and strategically important companies, where the attackers aimed at halting operations, stealing data, planting viruses, or aims for mass destruction of systems inside the targeted organizations. These attacks have the ability to destroy data and render infected systems unusable. The second one is high-profile government targets, where the attackers aimed at disrupting and damaging government computers. Another factor that appears to be common is the method or technique used to gain access and spread to other systems on the network, which is by using stolen credentials successfully gathered via phishing campaigns or by an insider.

CHAPTER FIVE

5. Cybercrime and Cybercrime Law

5.1 Concept of cybercrime

The United States Department of Justice defines computer crime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution" (Kim 2012). The United Kingdom defines Cybercrimes in two categories. One is crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity). The other one is, traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (CPS n.d.). The Saudi Anti-Cyber Crime Law defines it, "Any action which involves the use of computers or computer networks, in violation of the provision of this Law" (CITC 2007)

Generally, there are three major categories of cybercrimes, which are:

- **Crimes Against People.** While these crimes occur online, they affect the lives of actual people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online related libel or slander (Upcounsel n.d.).Moreover, attacks against Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) systems, which are high-level process supervisory management that control a process or operation like oil and gas pipelines, power

generation, electric power transmission, water treatment, etc. Changes or alteration of these systems can result in injury and loss of life.

- **Crimes Against Property.** Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and Intellectual Property Rights (IPR) violations (Upcounsel n.d.).
- **Crimes Against Government.** When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software (Upcounsel n.d.).

5.2 Concept of cybercrime law

Cyber law is any law that applies to the internet and internet-related technologies. Cyber law is one of the newest areas of the legal system. This is because internet technology develops at such a rapid pace. Cyber law provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet (Upcounsel n.d.).

5.3 Current Legislations to Combat Cybercrime in the Kingdom of Saudi Arabia (KSA)

5.3.1 The body of law of KSA "Shari'ah"

Shari'ah law is the official basis of criminal justice in Saudi Arabia. Shari'ah is considered as a divine law as it is based on God's words. Shari'ah, consists of Qura'an and Sunnah. The Qura'an is the words of God (Allah) that were revealed in stages during the lifetime of prophet Mohammad under various circumstances through the Angel Gabriel. Sunnah means the prophet Mohammad's sayings, actions, and the actions done with his approval. The Qura'an and Sunnah, are considered the fundamental sources of legality, which are unanimously accepted by Muslim scholars. However, there are secondary sources, which can be used when new circumstances occur that were not identified in the past. (Algarni 2010)

These secondary sources come under the title of Al-Ijtihad, which means the striving of a legitimate scholar to reach a religious judgement This includes mainly consensus (Ijma'a) and analogy (Qiyas). Consensus (Ijma'a), which means the unanimous agreement of religious scholars on a legal judgement at any time after the death of the Prophet. Ijma'a is used by Muslims to resolve situations that has not been declared in the Qura'an or Sunnah. However, the general consensus decision can be accepted as long as it does not contradict the provisions of the Qura'an and Sunnah. (Algarni 2010)

Shari‟ah law is holistic or eclectic in its approach to guiding individuals on most daily matters. Shari‟ah law controls, rules and regulates all public and private behaviors. The rationale of Islamic law is to protect the five important indispensables in Islam: Religion, Life, Intellect, Offspring and Property. Any deviation from or attack on these aspects constitutes crime.

Prohibited acts under Shari'ah are punishable by specific penalties set out in the Holy Qura'an or the Sunnah. However, as mentioned earlier, where the Holy Qura'an and the Sunnah are silent in that regard, judges may use their discretion to determine the appropriate penalty. Such penalties may include imprisonment, monetary compensation and/or deprivation of certain rights. In determining the severity of a penalty, a judge will take into consideration the damage suffered by a victim and whether such damage is actual or consequential. In general, however, only actual proven damages are awarded by Saudi Arabian adjudicatory bodies. (Al-Fawzan n.d.)

Shari'ah principles protect each individual's right to privacy and prohibit any offensives against the five important indispensables mentioned earlier. Under Shari'ah principles, disclosure of secrets is prohibited except the cases where the owner of the relevant secret agrees to such disclosure or if the public interest requires so. The Holy Qura'an and the *Sunnah* do not stipulate a penalty for disclosure of secrets; however, as explained above, such disclosure may be punishable by a penalty that a judge, in his discretion, deems appropriate and equitable. (Al-Fawzan n.d.)

5.3.2 Laws under Communications and Information Technology Commission (CITC)

5.3.2.1 Background

Communications and Information Technology Commission was established under the name of (Saudi Communications Commission) The name was changed after the Commission was entrusted with new tasks related to information technology to become "Communications and Information Technology Commission" on July 2003.

The vision statement of the Commission is to "Advance the communications and information technology sector through regulation to achieve a highly competitive environment for the provision of superior services to end-users and an attractive ecosystem for investors."

The Commission enjoys the juridical and financial independence to achieve its objectives stipulated in the Telecommunications Act, its Bylaws and the Ordinance of the Communications and Information Technology Commission. (CITC n.d.)

The Government of the Custodian of the Two Holy Mosques has understood the importance of keeping pace with the huge developments in the field of telecommunications on international level which leads to regulatory changes in the competitive and investment environment of this sector, and how these developments create fundamental changes in the infrastructure and regulation of the telecommunications sector in the Kingdom. (CITC n.d.)

In the light of this attention by the Government, Telecommunications Act and the Ordinance of the Saudi Communications Commission were approved and issued on 2001.

These legislations aim to face the challenges of the coming stage in the field of telecommunications, and creating a competitive environment based on equity and transparency emerging from it provision of high quality universal telecommunications services at affordable prices, activating the role of the private sector and motivating its investments in that field.

Due to the importance of the role of the Information Technology and its adherence with the successive developments in the telecommunications world, the Commission was entrusted with new tasks related to information technology (CITC n.d.).

5.3.2.2 CITC Roles and Responsibilities

- Granting licenses to provide telecommunications and information technology services
- Managing tariffs of telecommunication and information technology services
- Protection of users' rights
- Supervision and management of the National Numbering Plan
- Setting service quality standards
- Preparation of policies, regulatory frameworks and studies of ICT sector in the Kingdom of Saudi Arabia
- Interconnection
- Managing frequency spectrum
- Administration of the domain name space of Saudi Arabia (.SA).
- Increasing the information security awareness level in the Kingdom of Saudi Arabia
- approving of communication and information technology devices
- Enabling Users to keep their mobile phone numbers when transferring between mobile service providers
- Supervision of the National Committee for Information Society
- Content Filtering Service
- CITC Initiatives to develop information technology sector
- Radiofrequency Electromagnetic Fields

The Communications and Information Technology Commission (CTIC), is responsible for the implementation of the laws, including issuing licenses to authentication services providers (ASPs); verifying compliance by ASPs; and guaranteeing continuity of services and suspending or canceling licenses. The Ministry of Interior (MoI) and Ministry of Communications and Information Technology (MCIT) are jointly responsible for issuing general policies and developing plans and programs for electronic transactions and signatures. (CITC n.d.)

Internet use is persistently monitored by the CITC, which employs filtering on online content and social media posts considered "harmful," "illegal," "anti-Islamic," or "offensive," and consistently blocks websites related to pornography, gambling, drugs, extremist ideology, as well as pages belonging to human rights or political organizations. (CITC n.d.)

CITC requires mobile network operators to register sub- scribers' real names, identity numbers, and now even their fingerprints in order to "limit the negative effects and violations in the use of communication services." (CITC n.d.)

5.3.2.3 CITC Legislations

5.3.2.3.1 Anti-Cyber Crime Law

The Anti-Cybercrime Act is the Kingdom's first set of laws designed to combat the growing threat of IT crimes. Prior to the introduction of this legislation, judgement in computer crime cases presented before the General Courts, which are ruled by Islamic law, was left, as already explained, to the judge's discretion. (CITC 2007)

The Act comprises sixteen articles. Article one is set of definitions used throughout the articles of this law. The second article list the objectives of this law, which are: "1) Enhancement of information security; 2) Protection of rights pertaining to the legitimate use of computers and information networks; 3) protect of public interest, morals, and communal values; and 4) protection of National Economy". Articles three through seven identify the cybercrimes and their imposed punishments as follow:

Cybercrime	Punishment
Article 3 includes: Spying, Unlawful access, Invasion of privacy, and defamation	A maximum of one year of jail and a fine up to 500,000 Riyals ($ 130,000) or either
Article 4 includes: using Internet for fraudulent transactions	A maximum of three years of jail and a fine up to 2,000,000 Riyals ($ 530,000) or either
Article 5 includes: Denial of Service, Unlawful access to computers or networks with intention to delete, destroy, breakdown, leak or alter private data	A maximum of four years of jail and a fine up to 3,000,000 Riyals ($ 800,000) or either
Article 6 includes: Impinging on public order, religious values, public morals and privacy	A maximum of five years of jail and a fine up to 3,000,000 Riyals ($ 800,000) or either

Human Trafficking, Pornography, Gambling, and narcotic and psychotropic drugs, through information networks or computers	
Article 7 includes: terrorist related cybercrimes and jeopardizing security of the country or its national economy	A maximum of ten years of jail and a fine up to 5,000,000 Riyals ($ 1,300,000) or either

Article 8:

The imprisonment and the fine may not be less than half the maximum if the crime was coupled with one of the following:

1. The crime is perpetrated through organized crime.
2. The offender holds a public office and the crime perpetrated relates to this office, or if he perpetrates the crime using his power or influence.
3. The luring and exploiting of minors and the like.
4. The offender has been previously convicted of similar crimes within or outside the Kingdom.

Article 9:

Any person who incites, assists or collaborates with others to commit any of the crimes stipulated in this law shall be subject to a punishment not exceeding the maximum punishment designated for such crimes, if the crime is committed as a result of said incitement, assistance or collaboration, and he shall be subject to a punishment not exceeding half the maximum punishment designated, if the intended crime is not committed.

Article 10:

Any person who attempts to commit any of the crimes stipulated in this Law shall be subject to a punishment not exceeding half the maximum punishment designated for said crimes.

Article 11:

The competent court may exempt may an offender from such punishments if he informs the competent authority of the crime prior to its discovery and prior to the infliction of damage. If the culprit informs the competent authority after the occurrence of the crime, the exemption from punishment shall be granted if the information he provides eventually leads to the arrest of other culprits and the seizure of the means used in the perpetration of the crime.

Article 12:

Application of this law shall not prejudice the provisions of relevant laws, especially those pertaining to intellectual property rights, nor relevant international agreements to which the Kingdom is party.

Article 13:

Without prejudice to the rights of bona fide persons, equipment software, and means used in perpetrating any of the crimes stipulated in this Law or the proceeds generated therefrom may be confiscated. In addition. The web site or the venue where the service is provided may be shut down permanently or temporarily if it is the source for perpetuating the crime and the crime is committed with the owner's knowledge.

Article 14:

The Communications and Information Technology Commission, pursuant to its powers, shall provide the assistance and technical support to competent security agencies during the investigation stages of such crimes and during trial.

Article 15:

The Bureau of Investigation and Public Prosecution shall carry out the investigation and prosecution of crimes stipulated in this Law.

5.3.2.3.2 Electronic Transaction Act

The 2007 Electronic Transaction Act regulates e-commerce and establishes a legal regime for electronic transactions and digital signatures in Saudi Arabia. This Act consolidates the use of electronic transactions in the public and private sectors, at local and international levels, and advocates their use in commerce, medicine, education, e-government, e-payment systems, and other applications. In addition, the law seeks to protect digital records, and limit and prevent potential abuse, fraud, and embezzlement. It recognizes the equal validity of transactions carried out online and those carried out in a physical space and regards the legal equivalence of electronic signatures and written signatures. (CITC 2010)

This Act consists of 31 articles distributed between ten chapters, Chapter nine represents the offences defined in Article 23 and their consequences penalties defined in Article 24.

Article 23:

1- Engaging in the activities of a certification service provider without a license from CITC
2- A certificate holder's use of information concerning the applicant, for purposes other than certification without the applicant's consent in a written or electronic form
3- A certificate holder's disclosure of information accessed by virtue of his work without the certificate holder's consent in a written or electronic form, or as provided for by law.
4- A certificate service provider's submission of false or misleading information to the commission or misuse of certification services
5- Creating, publishing or using digital certificates or digital signature for fraudulent or any other unlawful purposes
6- Forging electronic records, digital signatures or digital certificates or using them with knowledge of forgery

7- Willfully providing false information to a certification service provider, or false digital signature information to any party relying on such signature under this Law
8- Accessing, copying, restructuring or taking over another person's digital signature system without valid authorization
9- Stealing the identity of another person or falsely claiming to represent him in applying for, accepting or requesting the suspension or revocation of a digital certificate
10- Publishing a forged, false, revoked or suspended digital certificate or knowingly placing such certificate at the disposal of another person

Article 24:

Any person who commits one of the above offenses shall be subject to a fine not exceeding five million Riyals ($ 1,300,000), imprisonment for a period not exceeding five years, or both penalties.

5.3.2.3.3 Telecom Act Bylaw

This law regulates Searching and seizing, investigations, and data privacy. it contains 15 chapters and 97 articles. The chapters in this law are: Telecommunications Licenses, Access to property, Competition between service providers, Interconnection, Disputes between Service Providers, Tariffs, Relations Between Service Providers and Users, Universal Access and Universal Service policies, Numbering, Telecommunications Equipment, and Protection and Prevention against intrusion. The articles related to this research are mentioned below (CITC 2002):

Article 5 Provision of Data and Information to the Commission

5.1 The Commission may, ask Service Provider or any other person to provide it with any data or information which the Commission deems necessary for the application of any of its regulations within the period determined by the Commission, in any form or manner deemed by the Commission, this include for example providing electronic systems or

terminal devices in sites specified by the Commission to enable obtaining that data or information

5.2 The person who is required to submit data or information to the Commission in accordance with paragraph 5.1, shall provide the Commission with it, and ensure its accuracy and validity

5.3 Taking into consideration the confidentiality of the information, the Commission may inform the public of any information submitted to it

Article 6 Disconnection

6.1 Where the Governor believes that there is a risk of imminent harm to a telecommunications network or a person, or where a frequency is used contrary to a Commission statute, decision or license, and after giving reasonable notice to the persons affected, the Governor may order a service provider to disconnect any of its telecommunications facilities from any other telecommunications facilities, if the Governor considers such disconnection necessary to prevent a violation of a Commission statute or any license or decision made pursuant to this Bylaw.

6.2 Subject to paragraph 6.1 of this Article, the Governor may require a disconnection to be made at or within such time, and subject to such conditions, if any, regarding compensation or otherwise, as the Governor determines to be just and expedient.

Article 7 Searching and Seizing

1.7 The Governor or his appointee may appoint or assign any person to carry out the inspection work, and enter any location or site that is listed with the licensee to ensure that the regulations and decisions of the Commission are implemented and not violated

2.7 In the event that it is necessary to inspect any location or site that is not referred to in paragraph 7.1, in order to ensure the application of the regulations of the Commission, this shall be done after coordination with the competent authorities if the command or order requires it.

3.7 The Inspector shall be enabled to perform his duties immediately upon presentation of the inspection card or letter issued by the Authority, and shall not be prevented or hindered while conducting inspections, and in case of prevention or disability; the inspector shall document in a record to take the necessary action.

Article 8 Investigation

8.1 The Governor may appoint any person as an inquiry officer to inquire into and report to the Commission on any matter pending before the Commission or within the Commission's jurisdiction under a Commission statute.

8.2 For the purposes of an inquiry, an inquiry officer shall have the powers of an inspector under Article 7 of this Bylaw.

8.3 All persons shall cooperate fully with inquiry officers during investigation

8.4 The Authority may use the competent security authority to be able to carry out the investigation tasks provided for under this Article

8.5 The Authority may call those who believe that they are relevant to the investigation in the manner that the Authority deems fit. In the event that the reported person is not present, the Commission shall take the appropriate action

8.6 The investigation shall be in written and through which the accused shall be confronted with the offense attributed to him and informed that he is in the process of an official investigation. The investigations can be done directly or through e-mail, or through any means deemed appropriate by the Authority, at any time or place determined by the Commission

8.7 Subject to the provisions of the preceding paragraph, the investigation shall be in a record including the following:

(A) Location and time of investigation

(B) Name and information of the Investigator

(C) The name and information of the person under investigation

(D) To confront the person under investigation with the alleged offense and the evidence against him and to allow him to respond to the facts and evidence attributed to him

8.8 The Investigator may start his investigations as to where the previous investigations have ended, if any

8.9 If the person under investigation abstains to give his testimony or sign on it, then this shall be noted in the record

8.10 If the results of the investigation lead to the confirmation of the violation of those attributed to it, the Commission shall sue it before the Commission for the Examination of Violations of the Telecommunications Regulations

Article 56 Confidentiality of User Information

56.1 A service provider shall not disclose information other than the user's name, address and listed telephone number to anyone without the user's written consent or unless disclosure is required or permitted by the Commission or by law to another legally authorized public authority.

56.2 A service provider's liability for disclosure of user information contrary to this Article shall be determined in accordance with Chapter 13 of this Bylaw.

56.3 Upon request, users are permitted to inspect any service provider's records regarding their service. Users shall have the right to require that any user information contained in their records that they can demonstrate is incorrect, be corrected or removed.

56.4 All user-specific information, and in particular billing-related information, shall be retained by a service provider only for billing purposes and retained only for so long as it is required by the laws of the Kingdom.

56.5 Nothing in this Bylaw shall be interpreted to prohibit or infringe upon the rights of concerned government agencies to exercise their rights to access otherwise confidential information relating to a user. Such access shall be made in accordance with the laws of the Kingdom.

Article 57 Confidentiality of User Communications

57.1 Service providers shall take all reasonable steps to ensure the confidentiality of user communications in accordance with Article Nine of the Act.

57.2 Service providers shall not alter or modify a user communication.

57.3 For the purposes of tracing and locating a source of harassing, offensive or illegal calls;

a) A user may request that the Commission authorize a service provider to monitor calls to the user's telephone;
b) The Commission or other duly authorized authority in the Kingdom may direct a service provider to monitor calls to and from a user's telephone and the service provider shall comply with any such direction;
c) The service provider shall provide the Commission the information resulting from its monitoring of the user's telephone, including the telephone numbers that are the source of the harassing, offensive, or illegal calls and the dates of occurrence of such calls and their frequency; and
d) The Commission may undertake any appropriate action to protect the public from harassing, offensive or illegal calls in accordance with the Commission statutes, and if necessary refer the matter to the appropriate authorities for further action

Article 58: Protection of Personal Information

58.1 A service provider shall be responsible for user information and user communications in its custody or control and in that of its agents.

58.2 A service provider shall operate its telecommunications facilities and telecommunications network with due regard for the privacy of its users. Except as permitted or required by law, or with the consent of the person to whom the personal information relates, a service provider shall not collect, use, maintain or disclose user information or user communications for any purpose.

58.3 The purposes for which user information is collected by a service provider shall be identified at or before collection, and a service provider shall not, subject to this Article, collect, use, maintain or disclose user information for undisclosed purposes.

58.4 Service providers shall ensure that users' information is accurate, complete and up to date for the purposes for which it is to be used and that user information and user communications are protected by security safeguards that are appropriate to their sensitivity.

5.3.3 Current Laws to combat Intellectual Property

5.3.3.1 Copyright Law

The Copyright Law contains of 7 chapters and 28 articles, Article 1 covers matters related to general definitions. Protected works including original works and derivative works are covered in Chapter One, Articles 2-4. Ownership of copyright works including single or collective works and works of folklore comes under Chapter Two, Articles 5-7. Rights protected including moral rights and economic rights in Chapter Three, Articles 8-14, lawful uses of copyright works in Chapter Four, Articles 15-17, and Scope and duration of copyright protection in Chapter Five, Articles 18-20. Copyright infringement and penalties are addressed in Chapter Six, Articles 21-15, and general provisions on the implementing regulations and validity of the Law, and the repealed Copyright Law 1989 in Chapter Seven, Articles 26-28 (Royal Decree 2003).

5.3.3.2 Trademarks Law

The Trademarks law ("the Law") contains 10 Parts and 58 Articles: Part I (Articles 1-2) on General Provisions, Part II (Articles 3-19) on Procedures and Publicizing of Trademarks, Part III (Articles 20-22) on the Effect of Trademark Registration, Part IV (Articles 23-28) on the Renewal and Cancellation of Trademark, Part V (Articles 29-32) on the Transfer of Ownership, Pledge and Attachment of the Trademark, Part VI (Articles 33-37) on the Licenses for Trademark Use, Part VII (Articles 38-40) on the Jointly-Owned Trademarks, Part VIII (Articles 41-42) on Fees, Part IX (articles 43-54) on Crimes and Punishments and Part X (Articles 55-58) on Concluding Provisions (Royal Decree 2002).

5.3.3.3 Penal Law on Dissemination and Disclosure of Classified Information and Documents

This law defines classified documents and information, the articles related to this research are mentioned below (Royal Decree 2011):

Article 5

Without prejudice to any harsher punishment prescribed by law, the following acts shall be punished by imprisonment for a period not exceeding twenty years or a fine not exceeding one million riyals or by both:

1. Disseminating or disclosing classified information or documents.
2. Entering or attempting to enter a place without authorization, with the intent of obtaining classified information or documents.
3. Obtaining classified information or documents by illicit means.
4. Possessing or becoming privy – by virtue of office – to official classified information or documents, and disclosing, communicating or disseminating the same without a lawfully justified cause.
5. Willfully destroying or misusing classified documents, knowing that such classified documents relate to the State's security or public interest, with the intent of undermining the State's military, political, diplomatic, economic or social status.
6. Failing to maintain confidentiality of Information or Documents.

5.4 Using Shari'ah laws as a reference to cybercrime laws

In some cases, the laws are either too general or not clear regarding a specific cybercrime. The judge will use the relevant Shari'ah laws. For example, stealing money using computer as a tool, the financial laws of Shari'ah will apply hand by hand with the Anti-Cybercrime law to tackle the crime and prosecute the criminal.

5.5 Current Countermeasures to combat Cybercrime

5.5.1 CITC Information Security Policies and Procedures Guide

This guide has been developed by the Computer Emergency Response Team – Saudi Arabia (CERT-SA), in the Communications and Information Technology Commission – (CITC), to further its statutory responsibilities under the Council of Ministers Act, that assigns CITC / CERT-SA authority to develop and promulgate information security policies and guidelines, including minimum requirements, that shall assist Government agencies in Saudi Arabia in managing their information security risks. (CITC 2011)

This document presents an overview of the information security policies and procedure development framework developed for Government Agencies in Saudi Arabia. The target audience of this Framework is the Government Agencies in Saudi Arabia. However, the framework can also be used by other public and private sector organizations in Saudi Arabia and Abroad. (CITC 2011)

The approach used in developing the Information Security Policies and Procedures Structure has considered input from

- ISO/IEC 27001
- CoBiT

- Saudi Laws
- Input from government agencies
- US- Federal Information Processing Standards FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems
- US-National Institute of Standards & Technology NIST PUB 80053--Recommended Security Controls for Federal IS
- Germany- Federal Office for Information Security (BSI) Baseline Protection Manual. (CITC 2011)

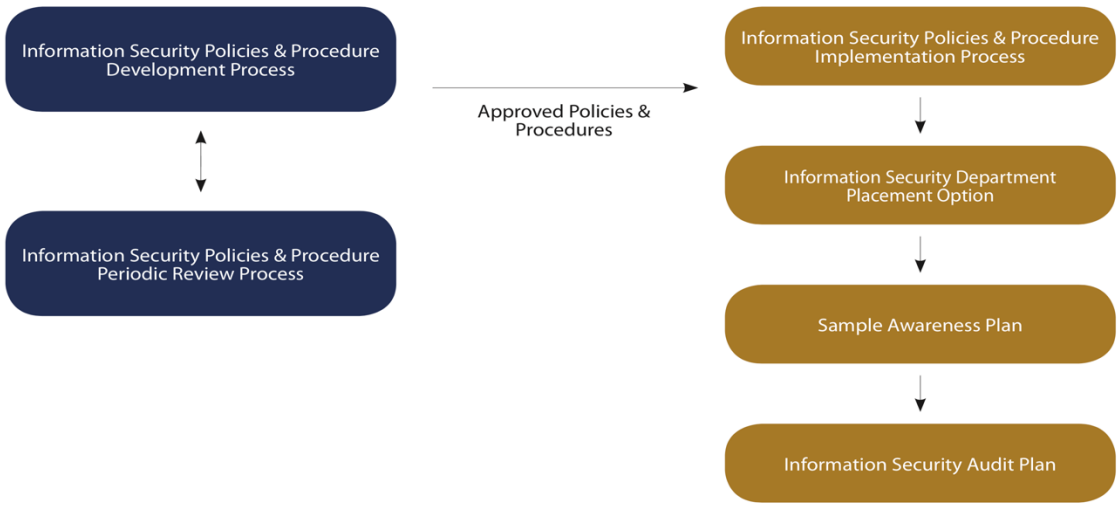

Figure 3: CITC Frame work (CITC 2011)

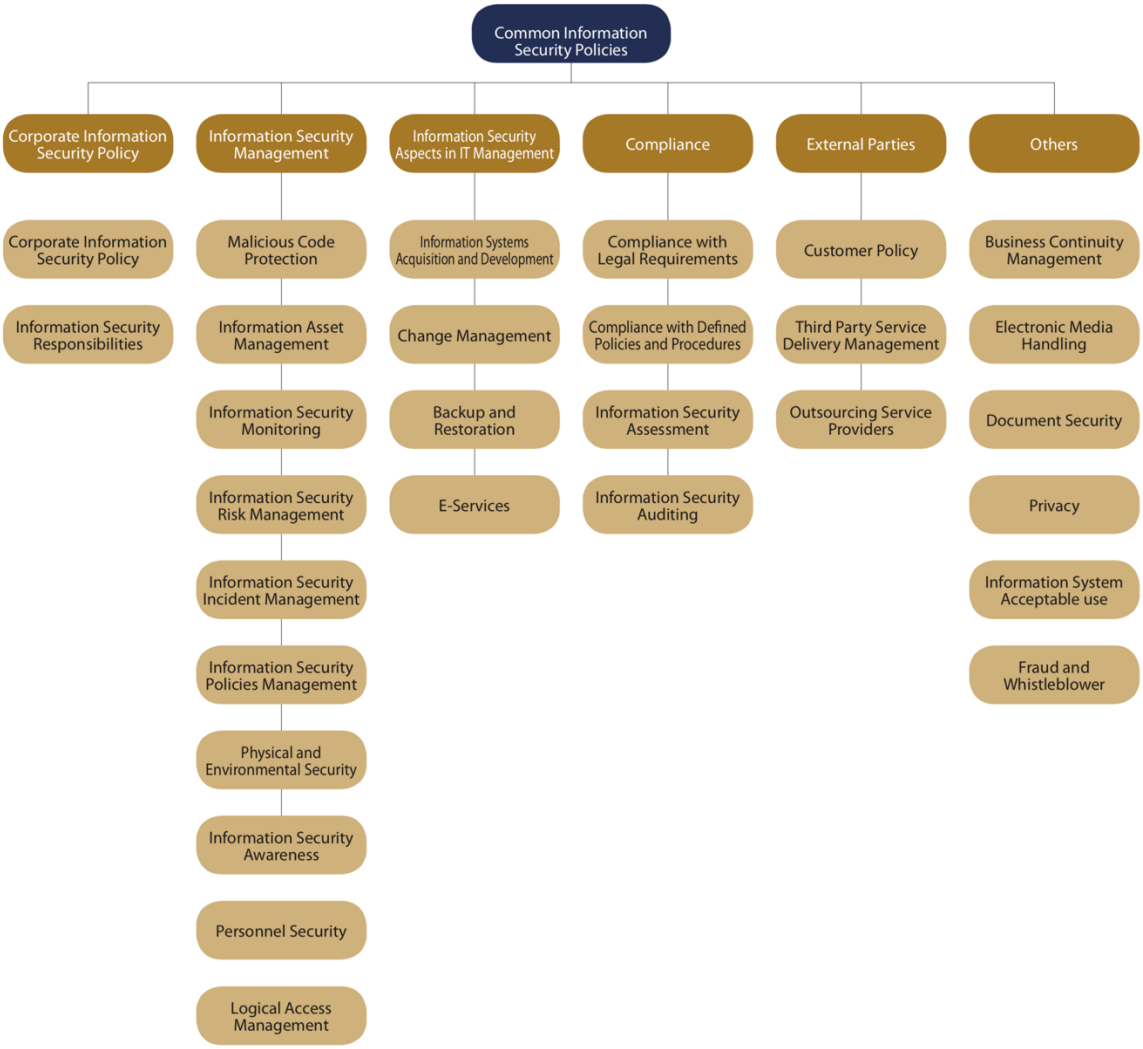

Figure 4 Common Policies (CITC 2011)

5.5.2 National Cyber Security Center (NCSC)

5.5.2.1 NCSC Background

As part of the Ministry of Interior, the National Cyber Security Center (NCSC) is at the forefront of the Kingdom's national cyber security defense initiative. NCSC develops and leads the national strategic direction for cyber security in collaboration with our primary Critical National Infrastructure, (CNI) partners, government ministries and agencies, and other key partners. With a focus on cyber security in the Kingdom, NCSC performs its national role by identifying cyber security threats, providing guidance to protect critical assets, promoting information sharing of cyber threats, and coordinating efforts to effectively respond and recover from national cyber incidents. The NCSC's Unified Cyber Platform acts as the central security stage enabling the Kingdom's networks to be analyzed to discover cyber threats and to provide real time situational awareness. This enables NCSC and our partner organizations to defend against cyber incidents, coordinate responses to incidents, and make informed decisions regarding the protection of critical systems (NCSC n.d.).

5.5.2.2 NCSC operational Framework

Figure 5: NCSC Framework (NCSC n.d.)

5.5.2.3 NCSC Basic Cyber Security Controls

In alignment with this national priority, the National Cyber Security Center's (NCSC) has developed the Basic Cyber Security Controls (BCSC) to assist Entities operating in the Kingdom in improving their cyber security readiness.

The BCSC Controls are composed of 15 Control Statements that are supported by 135 Control Standards. (NCSC n.d.)

The main goal of the Basic Cyber Security Controls is to provide actionable guidance to Entities operating in the Kingdom on how to establish basic *cyber security* hygiene and protect themselves against common cyber threats. (NCSC n.d.)

The Basic Cyber Security Controls were designed to be applicable to any Entity, and all Entities operating in Saudi Arabia are encouraged to adopt and implement these Controls. (NCSC n.d.)

Appendix A is essential for Entities to be able to interpret the Controls correctly; the definitions are considered part of the Controls.

Appendix B provides a wealth of information to Entities on how to best implement every Control Standard, including per-Control references to some popular international standards and best practices.

Appendix C provides 40 action items which Entities are advised to implement for Controls for which the Fundamental Control Standards are not yet established.

The Control Self-Assessment (CSA) Tool is a spreadsheet-based tool that is provided to assist Entities in implementing the recommended 6-step process

5.5.3 Cyber resilience in financial market infrastructure

With the increased dependencies on technology including mobile & web platforms for business operations, there is a significant increase in the cyber security threats. Further with the ever changing threat landscape in the region, Saudi Arabian Monetary Authority (SAMA) understands the criticality of cyber security risks and its impact on business operation. SAMA conducted a comprehensive cyber security assessment for banks to assess the effectiveness of cyber security controls and maturity. This assessment includes readiness of business resilience plans in case of incidents. The assessment allowed SAMA to have an up- to-date national (banking) risk assessment of cyber- security risk. In addition, analysis have been performed to

identify key common issues, key common strengths and recommendations were shared with the required entities (SAMA 2017).

- Cyber Security Strategy for Banking
- Cyber Security Framework and Governance
- Business Continuity Framework

5.5.4 Arab Convention on Combating Information Technology Offences

Saudi Arabia is a signatory of the Arab Convention on Combating Information Technology Offenses. This international legal framework among the League of Arab States was enacted in 2010 with the aim of enhancing cooperation between the Arab countries "to combat information technology offences threatening their security, interests, and the safety of their communities," and enabling parties to "adopt a common criminal policy aimed at protecting the Arab society again information technology offences." Saudi Arabia is one of the 18 member states to sign the Arab Convention, but is the only country that has not yet ratified it. Moreover, the convention is quite vague in its definitions and provisions to combat cybercrime and, despite its wide acceptance, it has not been formally activated. In fact, there is no reference to its provisions in any of the Arab nations' cybercrime laws, and coordination between the 18 state parties remains ineffective. (Hakmeh 2017)

5.5.5 National Cyber Security Authority

Saudi Gazette, the official newspaper of Saudi Arabia, said King Salman issued a decree on 31, October 2017 to set up the National Cyber Security Authority. Minister of State and Member of the Cabinet Dr. Musaed Al-Aiban has been appointed as chairman of the board of directors of the authority. The authority will be directly linked to the monarch, the Saudi Press Agency

reported. Members of the board include head of the Presidency of State Security, chairman of the General Intelligence, deputy minister of interior, and assistant minister of defense. Al-Aiban thanked the King and Crown Prince Muhammad Bin Salman, deputy premier and minister of defense, for establishing the authority as the Kingdom's competent body with all those related with cyber security with an objective of enhancing the State's cyber security so as to protect its vital interests, national security and sensitive infrastructure. Al-Aiban said the authority will begin its regulatory and operational tasks in the area of cyber security by enhancing the protection of networks, IT systems, operating systems, hardware and software components, services and data, taking into account the increasingly vital importance of cyber security in the lives of the public. He disclosed that the authority also aims to establish a national industry in the field of cyber security. Al-Aiban stressed that the authority will give top priority to attract and hire qualified national cadres, build partnerships with public and private entities, and stimulate innovation and investment in cyber security to contribute to achieving a technological renaissance that serves the future of the Kingdom's national economy. (Saudi Gazette 2017)

5.5.6 Digital Evidence

Digital evidence is now accepted in Saudi courts as a trusted source of evidence, this decision activated on 2017. High Court as declared that Digital Forensic Evidence is enough to prosecute as a major evidence. (Supreme Court 2017)

5.5.7 The National Center for Information Security

The Center aims to raise the level of awareness of dangers related to the use of electronic transactions as well as the level of confidence in information security and digital safety resulting from collaboration with members and partners of the Center, which has provided training and education on the subject

5.5.8 Agreement with USA

Saudi Arabia increased its cooperation with the United States through a Security Cooperation Agreement aimed at improving training for special operations and counter-terrorism forces, integrating air and missile defense systems, strengthening cyber defenses, and bolstering maritime security. (Melissa Hathaway 2017)

CHAPTER SIX

Conclusion and Recommendation

6.1 Conclusion

Saudi Arabia was ranked within the top vulnerable countries to fall victim to cybercrimes. Cybercrime is on the rise across Saudi Arabia. The Internet has presented a new challenge to humanity in facilitating crimes. As a result of the cyberattacks Saudi Arabia endured in recent years, cyber security and cyber defense have taken on heightened urgency in Saudi Arabia. Protecting against cyber threats is an ongoing management challenge for organizations in the country. Daily lives rely more and more on digital information; hence lives are more susceptible to attacks. This research is conducted based on the critical analysis on how Saudi Arabian legal system is successful to combat cybercrime, evaluate their legal systems to deal with the growing threats of computer-related crimes. In which it has been found that the laws are good to a limited extent, because they do not reflect the best level required to face all sort of cybercrimes. There are Laws to handle various harmful activities that occur in cyberspace. However, these laws do not tackle the crimes in all their detail. This research aimed to highlight the existing laws to combat cybercrime, where a misconception that "Anti-Cybercrime law" is the only law in Saudi Arabia that is considered relevant, however the analysis showed that there are more laws that relate to cybercrime. Most of the people know about cybercrime but very less is aware of the associated legislation to combat these crimes. Saudi Arabia plays a crucial role in maintaining security and stability in the region due to its economic, political, and cultural importance, as well as its strategic location.

6.2 Recommendation

6.2.1 Publicly Published Reports and Cases

The lack of publicly published documentation about different attacks and cases can affect the society in many ways. One, it can lessen the awareness of the significant impact of the incident. Being aware of the technical analysis of an attack can be used as lesson learned by other companies or organization, hence reduce the chance of repeating the incident on different targets. Another one, is publishing cases will increase the awareness of the existing laws and how they are handling cybercrimes. A clear regulation about publicly publishing incident reports and cases is a good step toward better, more secure digital environment

6.2.2 Awareness of the existing laws among the Saudi Society

Being aware of the existing laws will help reduce the rate of cybercrime. Moreover, attentiveness of laws will lead to clear understanding of rights and privileges, hence, considering reporting cybercrimes will increase.

6.2.3 Continues update of Existing Laws

Updating the existing laws to reflect new cybercrimes with their related specific details and different scenarios.

6.2.4 Establishment of Subordinate laws

Creating sub laws that address similar or related cybercrimes together with all their related regulation under one document instead of having different set of laws that contain provisions addressing certain aspects of a single cybercrime.

6.2.5 Compliance with Cybersecurity Best Practices and Standards

Apply penalties for not being compliance with security best practices and standard in the Saudi organizations. This can be done by conducting audits.

6.2.6 Establishment of Forensic Labs

Forensics investigation is a very important science in the information security field. With the increasing rate of attacks in our world, Computer Forensic investigation is very highly needed to prove and establish strong evidences that incriminate a person in a digital crime.

Digital forensics laboratories are needed to facilitate professionals' investigations to capture and classify digital evidence.

6.2.7 Establishment of Cybersecurity Programs at schools, Universities and Business

A significant number of internet users in the Kingdome are under 18, some are unaware of the term cybersecurity and the importance of using security measures. On the other hand, some were noticeable to have great hacking skills without any awareness of the ethical ways nor any knowledge about cybersecurity principles. This shows a need to spread cybersecurity awareness among this age group.

A recent study had been conducted on Saudi Arabian Universities' students showed that 50% are familiar with the term phishing attack, however most of them are in computer science department, while 50% are not familiar with the term itself. 62% have no idea on how to protect themselves against phishing attacks. 78% are not aware of the difference between http and https protocols. 72% are not familiar with the term "social engineering". 82% do not check the URL when opening new website (Elamin 2017). To help enhance this, Cybersecurity fundamentals course can be considered as part of the core courses during preparation year. Moreover, setting up a

Cybersecurity Major in the major universities across the country will help in preparing students to become cybersecurity professionals.

All enterprises despite their size and industry, are a potential target of cybercrime. Hence adopting a cybersecurity program for their employees is a good step to keep up with this trend.

References

Symantec. 2012. *Symantec Official Blog.* August 16. https://www.symantec.com/connect/blogs/shamoon-attacks.

Al-Fawzan, Noor. n.d. "Data Protection in the Kingdom of Saudi Arabia: A Primer."

Algarni, Abdullah Faze. 2010. "Is a Shari'ah-based Law Compatible with Cybercrime? An Inquiry into the Saudi Regulations on Internet Fraud." *Inspire Journal.* https://inspirejournal.files.wordpress.com/2011/11/algarni52.pdf.

Aljazeera. 2015. *Saudi websites hacked by well-intentioned group.* August 15. https://www.aljazeera.com/news/2015/08/saudi-websites-hacked-intentioned-group-150815194012877.html.

Almerdas, Suhail. 2014. "The Criminalisation of Identity Theft under the Saudi Anti-Cybercrime Law 2007." *JICLT.* http://www.jiclt.com/index.php/jiclt/article/viewFile/203/200.

Alriyadh. 2014. *Breakthrough the Ministry of Justice official account in Twitter.* October 14. http://www.alriyadh.com/984899.

Amro, Sulaiman Al. 2017. "Cybercrime in Saudi Arabia: fact or fiction?" *IJCSI International.* http://www.ijcsi.org/papers/IJCSI-14-2-36-42.pdf.

Aramco. 2012. *Facebook.* August 15. https://www.facebook.com/Saramcopage/posts/474783089213183.

Bronk, Christopher. 2013. "The Cyber Attack on Saudi Aramco." *Survival: Gobal Politics and Strategy* 81-96.

Budd, Christopher. 2017. *Threat Brief: Shamoon 2 Wave 3 Attacks.* January 30. https://researchcenter.paloaltonetworks.com/2017/01/unit42-threat-brief-shamoon-2-wave-3-attacks/.

CITC. n.d. *CITC Roles and Responsibilities.* Accessed January 17, 2018. http://www.citc.gov.sa/en/AboutUs/AreasOfwork/Pages/default.aspx.

—. 2016. "Annual Report." http://www.citc.gov.sa/en/mediacenter/annualreport/Documents/PR_REP_012Eng.pdf.

—. 2007. "Anti-Cyber Crime Law." *CITC.* http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx.

—. n.d. *Background.* Accessed January 14, 2018. http://www.citc.gov.sa/en/AboutUs/Pages/History.aspx.

—. 2009. "COMPUTER AND INTERNET USAGE IN THE KINGDOM OF SAUDI ARABIA." *citc.* http://www.citc.gov.sa/en/reportsandstudies/studies/Documents/IT%20009%20E%20-%20Computer%20and%20Internet%20Usage%20in%20KSA%202007-2009.pdf.

—. 2010. "Electronic Transactions Law." *CITC.* http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx.

—. 2011. *Information Security Policies and Procedures Development Framework for Government Agencies.* http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx.

—. 2002. "Telecom Act Bylaws." http://www.citc.gov.sa/en/RulesandSystems/bylaws/Documents/LA_005_%20E_Telecom%20Act%20Bylaws.pdf.

CPS. n.d. *Cybercrime - prosecution guidance.* Accessed January 2018. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

Elamin, Bushra. 2017. "The Current State of Phishing Attacks against Saudi Arabia University Students." *International Journal of Computer Applications Technology and Research* 42-50.

Elnaim, Bushra. 2013. "Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future." January. https://www.researchgate.net/profile/Bushra_Elamin/publication/309040131_Cyber_Crime_in_Kingdom_of_Saudi_Arabia_The_Threat_Today_and_the_Expected_Future/links/57ff2f9508ae6b2da3c89b36/Cyber-Crime-in-Kingdom-of-Saudi-Arabia-The-Threat-Today-and-the-Expecte.

Falcone, Robert. 2017. January 9. https://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/.

—. 2017. *Shamoon 2: Delivering Disttrack.* March 27. https://researchcenter.paloaltonetworks.com/2017/03/unit42-shamoon-2-delivering-disttrack/.

Finkle, Jim. 2017. *Hackers halt plant operations in landmark attack.* December 15. https://www.itnews.com.au/news/hackers-halt-plant-operations-in-landmark-attack-479886?eid=3&edate=20171215&utm_source=20171215_PM&utm_medium=newsletter&utm_campaign=daily_newsletter.

FireEye. 2017. *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.* December 14. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

Hakmeh, Joyce. 2017. "Cybercrime and the Digital Economy in the GCC Countries." *Chatham House.* June 30. https://reader.chathamhouse.org/cybercrime-and-digital-economy-gcc-countries#.

Kaspersky. 2017. *FROM SHAMOON TO STONEDRILL Wipers attacking Saudi organizations and beyond.* March 7. https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf.

Kim, Chris. 2012. "Computer Crimes." *American Criminal Law Review Volume:49* 443-488. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=262047.

Melissa Hathaway, Francesca Spidalieri. 2017. "KINGDOM OF SAUDI ARABIA CYBER READINESS AT A GLANCE." *potomacinstitute.* September. http://www.potomacinstitute.org/images/CRI/CRI2_0_SaudiArabiaPofile.pdf.

Ministry of foreign affairs. n.d. *About Saudi Arabia.* Accessed January 11, 2018. http://www.mofa.gov.sa/sites/mofaen/aboutKingDom/Pages/KingdomGeography46466.aspx.

NCSC. n.d. *Alerts.* Accessed December 22, 2017. https://www.moi.gov.sa/wps/portal/ncsc/home/Alerts/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziDQ1dLDyM3A18_M29XQwcnQKD3UyN3Y0dfQ30w8EKDDxNTDwMTYy8_YMMDAwcjcM8PIwtnA0N3I30o_BIWxjC9OMAjgbE6cfjwCj8xgen5gHNiMJrDcgXhMwpyA0NjajwTAcAkBgHyw!!/dz/d5/L2dBISEvZ0FBIS9n.

—. n.d. *Guidance.* Accessed October 13, 2017. https://www.moi.gov.sa/wps/portal/ncsc/home/Guidelines/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziDQ1dLDyM3A18LJyc3AwcvSycvYK8DI0NnAz0w8EKDDxNTDwMTYy8_YMMDAwcjcM8PIwtnA0N3I30o_BIWxjC9OMAjgbE6cfjwCj8xgen5gHNiMJrDcgXhMwpyA0NjajwTAcAtDb4lg!!/dz/d5/L2dBISEvZ0FB.

—. n.d. "Profile: Introducing the National Cyber Security Center." Accessed February 11, 2017. https://www.moi.gov.sa/wps/wcm/connect/ncsc/36d36576-8020-4991-ae97-73ae8e6952f9/NCSC+Profile-English.pdf?MOD=AJPERES&CVID=lF-3M8a&CVID=lF-3M8a&CVID=lF-3M8a&CVID=lF-3M8a&CVID=lF-3M8a&CVID=lFyx0Ux&CVID=lFyx0Ux&CVID=lFyx0Ux&CVID=lFyx0Ux&CVID=lFyx0Ux.

—. 2017. *Threats and Risk Report.* https://www.moi.gov.sa/wps/portal/ncsc/home/Reports/!ut/p/z1/jY9NC4JAEIZ_SwevzeiaSbetYDWFsMhsL6HhV5hruvr706RbRnOb4Xle3gEOAfAy7PI0lLkow6LfL9y4qurWtDSGrrleUvQQfZvaDvEcA85vAG1dt1Rdc_YHRKTEtyxiblRkBPg__g9g8HFiKPY-H5GpBtoHmM7YAU8LEY3v0jIiZgq8jpO4jut5W_fnTMqqWS.

Riyadh. 2015. *Saudi hacker" penetrates 24 government sites within two hours.* August 15. http://www.alriyadh.com/1073358.

Royal Decree. 2003. *Copyright Law.* http://www.wipo.int/wipolex/en/details.jsp?id=3593.

—. 2011. *Penal Law on Dissemination and Disclosure of Classified Information and Documents.* April 12. http://www.wipo.int/wipolex/en/text.jsp?file_id=330797.

—. 2002. *THE LAW OF TRADEMARKS* . http://www.wipo.int/wipolex/en/text.jsp?file_id=129518.

SAMA. 2017. "Cyber Security Framework." *Saudi Arabian Monetary Authority.* May.

Samani, Raj. 2017. *Shamoon Returns, Bigger and Badder.* April 25. https://securingtomorrow.mcafee.com/business/shamoon-returns-bigger-badder/.

2017. "SAUDI ARABIA and the VISIT OF PRESIDENT TRUMP." https://www.saudiembassy.net/sites/default/files/WhitePaper_TrumpVisit_June2017.pdf.

Saudi Gazette. 2017. *King orders setting up of National Cyber Security Authority.* October. http://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority.

Supreme Court . 2017. "Decree number 34 ."

Symantec. 2016. *Shamoon: Back from the dead and destructive as ever.* November 30. https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever.

Upcounsel. n.d. *Cyber Law: Everything You Need to Know.* Accessed January 15, 2018. https://www.upcounsel.com/cyber-law.

USC. n.d. *Research Guides.* Accessed February 14, 2017. http://libguides.usc.edu/writingguide/researchdesigns.