Lebanese American University

Legislation of Cyber Law and Digital Forensic in Lebanon

By

Maher Salim Shehab

A thesis
Submitted in partial fulfillment of the requirements for the degree of Masters of Business Administration

Adnan Kassar School of Business
September 2018
THESIS APPROVAL FORM

Student Name: Maher Shehab  ID.: 201002595

Thesis Title: Legislation of Cyber law and Digital Forensics in Lebanon

Program: Master's in Business Administration (M.B.A)

Department:

School: School of Business

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

in the major of

Thesis Advisor's Name: Abbas Tarchini  Signature  DATE: 24/September/2018

Committee Member's Name: Buzent Baljian  Signature  DATE: 24/September/2018

Committee Member's Name: Khodor Falah  Signature  DATE: 24/September/2018
THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants the Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic formats and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name: Maher Shehab

Signet: [Redacted]

Date: 24/September/2018
PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU’s Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name:  Maher Shehab

Signature:  [redacted]

Date:  24/September/2018
Acknowledgment

Success is the result of perfection, hard work, learning from failure, loyalty, and persistence. Thank you god for giving me all the necessary characteristics to be a successful person. Thank you for giving me the strength to move forward and to achieve my goals and dreams.

A special thanks to my advisor Dr. Abbas Tarhini who motivated me and supported me along the way. You believed in me and in my skills since day one, and you were a key person to the success of this research.

I would also like to thank Dr. Puzant Balozian for guiding me throughout the whole research. Your positive words, constructive feedback, and your time were very valuable to me.

Thank you Dr. Khodr Fakih for agreeing to be on my committee. Your presence in my defense was very vital and preliminary to me.

I am very lucky to be surrounded by people whom I can call family. A special thanks to my dad who taught me never to give up on my dreams, and to do whatever it takes to succeed. Thank you mom for motivating me to grow bigger every day, and to seek new challenges and new dreams. I couldn’t have made it without your continuous support and motivation. I want to thank my older brother Dr. Saadeddine Shehab for his advice and assistance on my research from thousands of miles away. I would also like to thank my sister and my best friend Ms. Noha Shehab for being there for me all the time. You are a gift to my heart, and a blessing to my soul.

Finally, to my dog “Scar”, you are a positive energy. Thank you for all the good vibes that you have spread since you became my best friend. You have taught me the meaning of loyalty, and how does it feel to love someone unconditionally. Cheers to many more years to come.
Legislation of Cyber Law and Digital Forensic in Lebanon

Maher Salim Shehab

Abstract

Computer related crimes are highly emerging in the crime scene as human beings are relying vastly on computers in terms of communication, information gathering, data storage and much more. Hence, many countries worldwide exert an effort to merge cyber law and digital forensics with their law enforcements as an attempt to achieve justice and perceive a holistic view before making a judgement. This topic however has been set as a draft in the Lebanese parliament for years waiting to be voted for by the Lebanese government to be applied. Hence, no current cyber law or digital forensic procedure is in practice. This work studies the current procedures applied by the Lebanese government and how it affects the relationship between the courts, the I.S.F, and cybercrime cases. Moreover, it sheds light on the importance of legislating cyber law and digital forensic procedures within the Lebanese law enforcement to protect people, organizations, and the economy. With this approach, it would be more effective for the Lebanese government to analyze criminal cases and cover all evidence that can be admissible in courts, which makes it easier to tie a suspect to a criminal case.

KEYWORDS: Cyber Law, Cyber Security, Cyber Crime, Digital Forensics, Investigations
# Table of Contents

INTRODUCTION ........................................................................................................................................... 1  
1.1 Research Goals: ........................................................................................................................................ 4  
1.2 Research Objectives .................................................................................................................................. 5  
1.3 Research Questions: ................................................................................................................................... 5  

LITERATURE REVIEW .................................................................................................................................... 8  
2.1 Cybercrime, Cyber Law, and Digital Forensic ...................................................................................... 8  
2.1.1 Cybercrime ........................................................................................................................................... 8  
2.1.2 Cyber law and Digital Forensics with respect to Law Enforcement ................................................. 11  
2.1.3 Digital Evidence from Devices to the Court ...................................................................................... 13  
2.1.4 Lebanese Law Enforcement ............................................................................................................... 16  
2.1.5 Digital Forensic Readiness ............................................................................................................... 18  
2.2 The Occurrence of Digital Crime and Its Impact on Lebanese Society ............................................. 19  
2.3 Cybercrime Combat through Laws ........................................................................................................ 23  
2.4 Judges’ Perception to cyber-crimes and cyber laws: Cyber law, Knowledge, and Evidence ............. 27  

METHODOLOGY ............................................................................................................................................ 31  
3.1 Research Design ....................................................................................................................................... 31  
3.2 Method ..................................................................................................................................................... 33  
3.2.1 Participants ......................................................................................................................................... 33  
3.3 Data Collection Procedures .................................................................................................................... 37  
3.4 Instruments for Data Collection ............................................................................................................. 38  
3.4.1 Interview with I.S.F ............................................................................................................................ 38  
3.4.2 Interviews with Lebanese Judges ......................................................................................................... 39  
3.4.3 Questionnaire ....................................................................................................................................... 39  
3.5 Data Analysis .......................................................................................................................................... 40  
3.5.1 Analyzing the interview responses .................................................................................................... 40  
3.5.2 Analyzing the Questionnaire ............................................................................................................. 41  

RESULTS ......................................................................................................................................................... 42  
4.1Current Implemented Cybercrime and Digital Forensic Investigation .............................................. 42  
4.1.1 Cybercrime and Intellectual Property Office in the I.S.F. ................................................................. 43
4.1.2 Reasons for Cybercrime Office to Start Investigations ................................. 44
4.1.3 I.S.F Capabilities and Trainings ......................................................................... 44
4.1.4 Tools used in cybercrime and digital forensic investigations.............................. 45
4.1.5 Communication with people, and awareness campaigns .................................. 46
4.2 Lebanese Judges’ perception to cybercrime and its effect on current cases ........ 46
    4.2.1 Incapability of confirmation of digital evidence through cybercrime cases ... 48
    4.2.2 Recommendations that will help courts and judges overcome difficulties faced through cybercrime cases ................................................. 49
    4.2.3 Reasons leading to the gap between judges and I.S.F members while performing a cybercrime investigation.............................................................. 50
    4.2.4 Importance of implementing cyber law and digital forensic procedure ........ 51
    4.2.5 Absence of cyber laws and digital forensic procedures in Lebanon .......... 53
    4.2.6 The number of cybercrime cases in Lebanon within the past 5 years ......... 53
    4.2.7 The reasons behind the increase in cybercrime in Lebanon ......................... 54
    4.2.8 Efforts to assist judges in understanding and confirming digital evidence submitted for a cybercrime case ................................................................. 55
    4.2.9 Reasons to deny digital evidence from I.S.F ................................................. 56
    4.2.10 Reasons to start a cybercrime investigation by the I.S.F .............................. 57
    4.2.11 Reasons for the absence of cyber law and digital forensic procedures in Lebanon ........................................................................................................... 57
    4.2.12 Judges’ and I.S.F efforts to overcome the difficulties faced due to the absence of cyber law and digital forensic procedures in Lebanon ..................... 58
    4.2.13 Organizations as a target for cybercrime and cyber-attacks ........................ 59
    4.2.14 Drafts waiting to be voted upon in the Lebanese parliament ..................... 60
    4.2.15 Effect of the absence of cyber laws and digital forensic procedures on the current Lebanese cybercrime cases ......................................................... 61
4.3 The Impact of the absence of Cyber Laws on Organizations and Economy ........ 62
    4.3.1 E-Banking services in Banks ...................................................................... 63
    4.3.2 The occurrence of Cybercrime through the Banking sector ........................ 64
    4.3.3 How is the Absence of Cyber Laws Motivating Attackers ....................... 66
    4.3.4 How is the Absence of Cyber Laws affecting the cybersecurity performance of banks? ........................................................................................................ 67
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1: Cybercrime and Intellectual Property Office</td>
<td>42</td>
</tr>
<tr>
<td>Table 2: Reasons for Cybercrime Office to Start Investigations</td>
<td>43</td>
</tr>
<tr>
<td>Table 3: Reasons for Cybercrime Office to Start Investigations</td>
<td>43</td>
</tr>
<tr>
<td>Table 4: Reasons for Cybercrime Office to Start Investigations</td>
<td>44</td>
</tr>
<tr>
<td>Table 5: Communication with people, and awareness campaigns</td>
<td>45</td>
</tr>
<tr>
<td>Table 6: Incapability of confirmation of digital evidence</td>
<td>47</td>
</tr>
<tr>
<td>Table 7: Recommendations that will help courts and judges overcome cybercrime difficulties</td>
<td>48</td>
</tr>
<tr>
<td>Table 8: Reasons leading to the gap between judges and I.S.F.</td>
<td>49</td>
</tr>
<tr>
<td>Table 9: Importance of implementing cyber law and digital forensic procedure</td>
<td>50</td>
</tr>
<tr>
<td>Table 10: Absence of cyber laws and digital forensic procedures</td>
<td>51</td>
</tr>
<tr>
<td>Table 11: Number of cybercrimes in the past 5 years</td>
<td>52</td>
</tr>
<tr>
<td>Table 12: Reasons behind the increase in cybercrime</td>
<td>53</td>
</tr>
<tr>
<td>Table 13: Efforts to assist judges in understanding and confirming digital evidence</td>
<td>54</td>
</tr>
<tr>
<td>Table 14: Reasons to deny digital evidence from I.S.F</td>
<td>55</td>
</tr>
<tr>
<td>Table 15: Reasons to start a cybercrime investigation</td>
<td>56</td>
</tr>
</tbody>
</table>
Table 16: Reasons for the absence of cyber law and digital forensic procedures …………..56

Table 17: Judges’ efforts to overcome the difficulties faced due to the absence of cyber law and digital forensic procedures..................................................................................................................57

Table 18: Organizations and incidents being target for cybercrime........................................58

Table 19: Drafts awaiting to be voted upon in Lebanese parliament…………………………59

Table 20: Effect of the absence of cyber laws and digital forensic procedures on current cases…60
LIST OF FIGURES

Figure 1: Cyber Attackers Groups
Figure 2: Generic computer forensics investigation model
Figure 3: Saudi Arabia Anti Cyber Crime Law
Figure 4: The current implemented flow for cybercrime and digital forensic investigations
Figure 5: The reason behind the gap between I.S.F and the courts, and its effect on current cybercrime cases
Figure 6: Graphical representation of the use of online services
Figure 7: Detailed representation of the use of online services
Figure 8: Respondents’ Bank – Breaches
Figure 9: Other Bank - Breaches
Figure 10: Detailed representation of the respondents’ bank breaches
Figure 11: Detailed representation of the other bank breaches
Figure 12: Motivation of Attackers to perform Cybercrime due to Absence of Law
Figure 13: Detailed representation of Motivation of Attackers to perform Cybercrime due to Absence of Law
Figure 14: The effect that the absence of cyber laws has left on cybersecurity performance in banks
Figure 15: Significant path for quantitative analysis
CHAPTER I

INTRODUCTION

From year 2000 up until this day, the world has made a massive jump in terms of technology, shifting to a digital world. However, with every new technology come new vulnerabilities and new ways to break through the system. According to PwC, cybercrime ranks number two after asset misappropriation reported frauds across industries (PwC, 2018, p.8). This number highlights a problem that needs to be controlled before it is too late. People are being tricked into giving their personal information and their financial information through the digital world which is resulting in huge financial losses and is exposing personally identifiable information. According to BBC, a company has lost around two hundred thirty thousand euro after they got tricked to reveal their financial information (Cybercrime and Fraud, 2017). The latter number when compared to other numbers is considered a minimal amount as a result of cyber-crime.

It was detected that through year 2011, the annual cost of identity thefts alone (which is using someone else’s personality to commit a fraudulent action) was an estimate of $37 billion dollars (National Crime Prevention Council, 2012). Today, these numbers are increasing substantially. In 2016, the British insurance company Lloyd’s estimated that cyber-attacks cost businesses as much as $400 billion dollars annually, which includes direct damage plus post-attack disruption to the normal course of business (Steve Morgan, Forbes magazine). This number is expected to reach two trillion dollars by the year 2019. These numbers represent the total damage incurred from all types of cyber security attacks collected from cases worldwide. The case is similar when it comes
to Lebanon, for the country has lost around $12 million dollars in year 2015 due to
cybercrime (Cybercrime in Lebanon, 2016).

Some people abuse tools that are meant to do good to commit crimes and break
the law to get what they want. For example, when Alfred Nobel created dynamite, his
main purpose was to collect gold by blasting rocks in mines. However, people started
using dynamite to kill and make weapons of mass destructions to protect their lands and
attack other countries.

As the world emerges to a digital one, all financial transactions, buying & selling
goods, offering services and much more is done using the World Wide Web. This new
technology has created a new terminology which is the “Cybercrime”. Cybercrime is the
use of computers and other technological devices in order to commit a crime such as
fraud, identity theft, hacking, phishing, or just as a mean of communication planning for a
crime. However, as all crimes have traces behind them (fingerprints, phone calls…),
cybercrimes also have lots of traces and evidence that can tie a suspect to a crime and can
be admissible in courts if extracted and analysed using the right procedures. Every
technological device is usually assigned an IP address which serves as the “identity card”
of the device assigned with a set of actions done through it as proof or signature of the
completed action.

The uncovering and examination of evidence located on all electronics with
digital storage, including computers, cell phones, and networks are referred to digital
forensics (Garfinkel, Simon, 2013). It helps investigators find missing links related to
crimes, recover deleted information and data, and tie up a suspect with evidence that can
be admissible in courts. Digital forensics can cover computer forensics (data and evidence related to computer devices), mobile device forensics, network forensics, database forensics, and finally forensics analysis. Just like regular investigations and forensics, digital forensics require allocated resources and professionals in order not to taint any data and make sure that all data collected is admissible in courts.

The first condition for a digital evidence to be admissible in courts is to have a cybersecurity law and a digital forensic procedure in agreement with the government. First world countries are already aware of the importance of legislating cybersecurity and digital forensics into their law enforcements and have already started implementing the needed digital forensics tools and the allocated resources to make sure that no evidence or data is left out without judgement.

Lebanon is a Middle Eastern country which has not legislated or integrated a cybersecurity law and digital forensic procedure with its law enforcements. Although the policy to implement a cybersecurity law and digital forensic was drafted and modified several times to keep up with the new trends of technology (last draft submitted to the Lebanese parliament was in 2011) , however, the policy never made it to voting in the Lebanese Parliament due to lack of awareness of its importance. Although Lebanon does not fully rely on technology and has not yet entered the digital world, the country is taking baby steps towards a digital world. Lebanese banks have already implemented and integrated online banking to their systems. E-Commerce companies (such as Makhsoom, Gosawa, and Ihoz) are becoming a trend for Lebanese people as they are buying and selling goods over the internet.
The purpose of this study is to shed light on the importance of legislating cybersecurity and digital forensic procedures to the Lebanese Law Enforcements. Moreover, the purpose of this study explores the current implemented framework for dealing with cybercrime, and studies the effect of the absence of cyber laws on the relationship between the courts and the I.S.F and the current cybercrime cases. Using a qualitative and a quantitative method approach, this paper will examine the effectiveness of solving cybercrime cases within the absence of a cybersecurity law and digital forensics procedure. Specifically, this paper will examine the importance of integrating cyber security laws and digital forensic investigation with the Lebanese Law Enforcements, and will discuss how digital evidence can be a vital missed out information in courts.

1.1 Research Goals:

This research aims to look at the Lebanese cybercrimes and digital forensics from three different perspectives and angles: I.S.F role and framework in combating cybercrimes and following digital forensic procedures, Lebanese judges’ perception of cybercrimes and how they are dealing with digital evidence, and the impact of cybercrimes and attacks on the Lebanese society, its organizations, companies, and the economy. As the Lebanese government is currently functioning with no cyber law, the goal of this research is to study the readiness of implementing a cyber law and a digital forensic procedure for cyber investigation in Lebanon, and to check the current status of the Lebanese government and Lebanese organizations regarding the addressed topic. The law should be able to protect Lebanese people, Lebanese organizations, and the Lebanese
government from cyber security attacks, and should clearly state the procedures to be
taken while performing a digital forensics investigation.

1.2 Research Objectives

The objectives of this research paper are to:

1. Clearly identify, understand, and discuss the current framework and methodology that
   is being applied by the Lebanese government when dealing with cybercrime and
digital forensics investigations (taking into consideration the absence of cyber law).

2. Understand the gap between cyber security investigators (I.S.F) and the gap between
   judges and courts, and identify how the absence of cybercriminal laws is affecting
   judges’ decisions about certain cases.

3. Discuss the impact of the absence of cyber law on the Lebanese society, economy,
   and organizations/companies, and deduce the importance of integrating a cyber-law
   and deduce the effects that resulted from the absence of cyber laws.

1.3 Research Questions:

1. What is the current framework applied by the Lebanese Internal Forces of
   Security (I.S.F), and what procedures, standardization, and trainings are being
   taken into consideration when performing a cyber security investigation?

It is vital to understand how countries practice cyber security laws and digital forensics
investigations, and what frameworks are followed in order to tie a suspect to a specific
criminal case. As Lebanon still lacks the integration of a cybercrime law through its law
enforcement, it is very important to understand how the I.S.F is performing their
investigations and how is it able to arrest suspects who performed cybercrimes or violated cyber laws.

This question seeks to explore the current framework applied by the Lebanese Internal Forces of Security in an attempt to understand the logistics of the work within this field. It also seeks to identify gaps within the current framework to come up with a modified framework that fits Lebanese people and their needs in the digital world.

2. What flaws in the current implemented laws are the reasons behind the gap between judges in courts the Internal Security Forces, and what is the latter’s impact on the cybercrime cases addressed in courts?

As a result of the absence of cyber security and digital forensics law, the gap between judges and the courts, in comparison with the Internal Forces of Security is increasing daily and is considered to be huge. Within the I.S.F of Lebanon, the cybercrime and IP Bureau office are registered and functioning under the law; however, as the Lebanese law is missing a cybercrime and digital forensics section, there is a huge gap in knowledge and information about cybercrime and digital forensics investigations between judges in courts and the specialized forces of the office. This gap is a result of the absence of cybercrime and digital forensics law, and a result of many flaws in the current implemented law.

The aim of this question is to identify the reasons behind the flaws in the current implemented framework, and to study its effects on current cybercrime cases. As this question is discussed and explored throughout this paper, it will provide a foundation and a base for the upcoming question.
3. How does the absence of laws, such as cyber security and digital forensics, impact the Lebanese economy, organizations, and people? What is the importance and significance of adding cyber laws to the existing system?

The factors and results identified in this question will build a solid ground for the importance of integrating cyber security and digital forensics through the law. It will also identify how the economy, Lebanese government, and Lebanese people are being affected by the absence of cyber laws and digital forensic investigations.
CHAPTER II

LITERATURE REVIEW

Due to the lack of theory and research regarding the topic “Legislation of Cyber Law and Digital Forensic in Lebanon”, the research review will focus on literature from different perspectives.

The literature on implementing a cybersecurity law and digital forensics procedures will shed light on the framework or procedures to be undertaken in order to keep digital evidence clean and admissible to the court. The literature will discuss mainly the five basic rules for digital evidence to be admissible to the courts (admissible, authentic, complete, reliable, and believable) along with the framework of the investigation (Pre-Process, Acquisition, Analysis, Presentation, Post-Process).

2.1 Cybercrime, Cyber Law, and Digital Forensic

2.1.1 Cybercrime

Cybercrime is the act of performing a criminal activity using computer networks and computer devices (laptops, computers, mobile phones…) (Kävrestad, J., 2017). Cybercrime activities are similar to conventional activities. They vary from identity theft, phishing attacks (fake links used to steal passwords), unauthorized access to sensitive information (credit card numbers, personal information) etc… (Pocock, L., 2017).

Due to the availability of script kiddie tools which are existing computer scripts available online for all people that are used to commit cybercrimes (Arbaugh, Fithen, &
McHugh, 2000), cybercrimes are no more tied to specific people. All human beings are now able to perform cyberattacks through these scripts whether adults or children. In addition, people who perform cyberattacks may have different motives to do so. Attackers vary from being organized attackers and hackers to being amateurs (Han, Chen, and Dongre, 2014).

Organized attackers are a group of people who hack computer systems and perform cyberattacks in order to make a political statement or fight governments (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014). These types of attackers usually are a combination of terrorists, hacktivists, or criminal actors. Hackers on the other hand are usually individuals who perform cyber-attacks for several reasons, three of which can be: They have the knowledge to do so, they accept it as a challenge, or they
want to perform a malicious activity (Voiskounsk & Smyslova, 2003). Finally, amateurs are the less skilled hackers who use available scripts in order to hack into computer systems as a mean of exploration and having fun (Andress & Winterfield, 2013).

In cybercrime, computers can be used as a tool to perform a certain kind of a crime, or as a target for a crime. Both methods involve computers and human beings for the crime to take place (Dashora, 2011). However, through cybercrime, computers play the major role in a criminal activity (Moore, 2014), while in a conventional one, human beings are the major factor (Wilson and Herrnstein, 1998). When humans use computer devices to perform a criminal activity, computers are the tool or the mean that makes the crime possible. For example, collecting digital information about a victim using computers in order to plan a crime is a common way of using computer systems in crime acts (Moore, 2014). However, computers being the target in a crime act are classified to be more dangerous. Many computer systems contain sensitive and confidential information that would lead to huge losses in case it got leaked (Lawton, 2008). For example, On November 29, 2014, U.S Giant target states that up to 70 million customers had payment card and personal data stolen from the company's databases. The attackers decided to perform this attack on one of the busiest days for retail shops known as the “black Friday”. Seventy million credit card numbers, names, and email addresses were stolen on that day, which affected the reputation of the company. Customers sued the company since it did not notify them as the attack was reported.(Target Data Theft, 2014) It is worth mentioning that cyberattacks and cybercrimes are increasing and are more successful nowadays due to the lack of security awareness and security counter-preventive systems (Kankanhalli,Teo,Tan & Wei, 2003)
Countries are starting to be aware of the power that computer devices hold and thus have started implementing laws to protect people from cyberattacks (As-Saber, Srivastava, & Hossain, 2006). Human beings are becoming more dependent on computers; hence recording and sharing all of their personal information on computer systems (Schwartz, 2004). Many philosophers and war experts have confirmed that World War 3 will be a cyberwar. John McAfee argues that the world might be prepared for a traditional warfare, but the next one will not be a traditional one; it will be a cyberwarfare were weapons and technologies will be used against us (Burke, 2015). Thus, it remains very essential for countries to implement digital forensics with their law enforcement in order to protect people.

There is a type of cyber-attack that has not yet been discussed and that would be the computer being as smart as humans in making decisions by itself. Computers nowadays are being developed with high artificial intelligence abilities. Many computer systems are also being developed as self-learning systems. Thus computers have the ability to make decisions without the consent or approval of a human being (Velik, 2013). The fact that computers have the ability to make decisions independently is considered a crime act that needs to be taken into consideration. Hence, the question that remains: Who will be held responsible of criminal acts when a computer system acts without a human’s approval?

2.1.2 Cyber law and Digital Forensics with respect to Law Enforcement

As criminal activities are increasing, cyber law and Digital Forensics need to be legislated (Ayofe & Irwin, 2010). The fact that all activities are done with the assistance of computers and the internet cannot be disregarded. Internet acts as a two edged sword
(Rao T.S et.al, 2018); it is a powerful tool that all corporations, individuals, and groups of people use to connect to the world, it can also be a tool to perform criminal activities (whether cybercrimes or conventional crimes). This fact sheds light on the importance of implementing laws in order to limit crimes and collect information through devices used to perform these crimes and submit them to the courts as admissible evidence.

Computers and smart devices have led to the creation of another world different from the one we live in. It led to the creation of a new digital world where people can chat, make friends, date, buy, sell, and do any operational work from behind their screens (Selwyn, 2012). However, this world needs to be conducted and monitored or else it will be chaotic and never to be controlled again. First world countries are already aware of the digital world and of the importance of controlling people’s activities on it. The digital world has no limits, and hence needs to a law to avoid chaos and control how people use it (Lessig, 1995).

Cyber law and digital forensic investigations act as the tools and guidelines on how to use the digital world (Lessig, 1995). With cyber law, people would be aware of what is considered to be an acceptable behaviour, and what is considered to be a prohibited or dangerous behaviour. It would also specify the penalty or punishment that people will receive in case they mistreat one another through their devices, or in case they shift from the guidelines of its usage (Lessig, 1999). Without a cyber law, everything is considered as an acceptable act as there will be no guidelines to people on how to use and live in this world. In addition, cyber laws do not cover the crime and the punishment only, it is a legal system that defines the cyber world and its components and acts as a major component in learning about the digital world and how it functions; hence
increasing the knowledge and the vision about the digital world (Bhargav & Edwin, 2017).

Digital forensic completes cyber laws. It is a digital investigation that helps the “police” catch whoever misuses the digital world. Just as a normal investigation requires a clearly specific procedure to be followed, digital investigations also need to be clear and need to be followed step by step in order to keep the digital evidence admissible in courts and to prevent this valuable evidence from being tainted (Carrier & Spafford, 2004).

2.1.3 Digital Evidence from Devices to the Court

Evidence is what actually ties a suspect to a crime. It is what turns a hypothetical claim into a tangible one. And in order for an evidence to be admissible in courts, evidence should be: Admissible, authentic, complete, reliable, and believable (Oluwasegun, David, Esther, Victor, 2014. P.35-38). Digital evidence should be admissible to courts as the procedure to collect this evidence should follow certain rules and laws to be set by the government to make sure that the evidence is authentic, complete, reliable and believable. Hence, it is the obligation of the government to draft a procedure and integrate it with the law to make sure that digital evidence is admissible and not tainted. In addition to admissibility to the courts, digital evidence should be authentic. Pointing out that digital evidence should be complete and objective (tell the whole story and not just a small part of it), the evidence collected from a crime scene should be related to the crime scene, and proves that a suspect can be tied to an incident.
Finally, digital evidence should be reliable and believable to the Jury. The court should not have any questions on how the evidence was collected. Knowing that judges do not have a technological (technical) background, digital evidence investigations should be well documented and should be reader friendly.

In digital forensics, a process model is the methodology used to conduct an investigation; a framework with a number of phases to guide an investigation (Du, Le-Khac, Scanlon. 2017). In order to assist governments in implementing cybersecurity laws along with digital forensic procedures, computer forensics process models have been formulated and published to ensure that digital evidence follows the five basic rules discussed above. One of the framework proposed discusses the digital forensics investigations through five procedures (Pre-process, Acquisition & preservation, Analysis, Presentation, and Post-Process) (Oluwasegun, David, Esther, Victor, 2014. P.35-38)
The first procedure through the digital forensics investigations should be the Pre-Process. This procedure is mostly related to all the paperwork and permissions done before the investigations starts. For example, as a police officer requires a search warrant to investigate a suspect’s house in search of a tangible asset, computers tend to be the same. The investigator must first have an approved search warrant from the government stating that he has the full privilege to investigate a suspect’s device or computer. After the investigator gets the approval to search a suspect’s device, the investigation process begins at the Acquisition & preservation procedure. This procedure is related to the tasks related to identifying, collecting, and transporting, storing and preserving captured data. This procedure also requires governments to draft procedures on how these tasks should be performed to ensure that digital evidence is complete and not tainted. After the digital data is extracted, it is the job of the investigator to analyse this data and connect the missing dots in order to tie a suspect to the crime being investigated. Once the analysis is
done, digital evidence is presented to the court with a full documentation explaining the acquisition and preservation procedure, and the analysis phase. As a final step, through the post-process, the courts return the devices and digital data that was extracted and seized to the rightful owner. This process acts as the closing process of the investigation journey.

2.1.4 Lebanese Law Enforcement

Due to lack of research on this topic, the following section will cover Lebanese law enforcement in terms of the code of criminal procedure that was published in 2001 (Act No. 359) which was distributed by Legal Publication Agency under the supervision of Mr. Houssam Chamseddine. Note that by year 2001, the cybercrime and intellectual property division was not even defined through I.S.F.

As stated under article 29, 31, and 47 in the code of criminal procedure, the investigator has the authority (granted by the public prosecution) to seize and collect all evidence from a crime scene that is related to the crime and could be of a reliable information to the case and for the trial. The articles also state that evidence collected by the investigator should be preserved and all necessary security measures should be taken in order to conserve the collected evidence. Thus, through articles 29 and 31, it is stated that the investigator has full authority to seize any weapon and other items used in the commission of the offence as well as any items that may assist in establishing the facts, and questioning the suspect about the seized items (Chamseddine, 2001). But is this law enough to cover digital evidence? Is a digital device now considered a weapon, and does the public prosecutor have the rights to seize a digital device that is suspected to be used in the crime? Moreover, article 34 of the law states that the investigator should take all
necessary actions and inspections in search for any admissible evidence that can be filed for the case in courts. Although the mentioned articles in the code of criminal procedure state that investigators have the right to seize and inspect any evidence that may lead to useful information for a criminal case, the question remains: Does this law apply to digital devices, and will digital evidence be admissible in courts? Are there any procedures that should be followed by investigators to extract reliable information from computer devices and systems?

As the aim of this paper is to study the importance of integrating digital forensics with the Lebanese law enforcement, the law does not clearly state that digital information would be admissible in courts. Hence, during the investigation of a certain crime (whether cybercrime or a conventional one), the judge has the right to refuse any digital information (even if it were useful) as it is not stated by the Lebanese law.

On the other hand, as per the Lebanese law, any evidence submitted to the court has to be well documented and should be extracted using a certain procedure stated by the law. Therefore, in order for investigators to be capable to extract digital information, they should be aware of digital forensics tools and procedures. Since the Lebanese law has not yet implemented a digital forensics procedure along with a cyber law, it is almost impossible for an investigator to extract and preserve digital information. Digital forensics investigation is not an easy task. It requires security professionals in order to recover deleted information, extract suitable information from computer systems, and track the necessary logs of actions performed on a specific system.
Since the publication of the code of criminal procedure in 2001, Lebanon was not affected by the technological revolution, and hence there was no need to implement any laws or procedures to protect people from cybercrimes. However, today Lebanon has implemented a new infrastructure that allows people to use the Internet, computer devices and systems to connect with the world. Banks are already using powerful softwares to perform transactions and make use of the online banking concept. People own high tech smart phones with high speed connections that allow them to communicate with one another using Internet connections and perform many personal transactions over the World Wide Web. Although this might sound as an improvement, relying on computer systems have its threats. People are more susceptible to cybercrime which puts them under threat as there is no law to protect them from these crimes. For example, if a Lebanese citizen’s credit card information was stolen over a fake website or through phishing link, there is no law that can protect this citizen, or even compensate for his/her loss.

2.1.5 Digital Forensic Readiness

Digital forensic readiness is the process at which organizations and governments get ready to analyze digital data extracted from computer systems to submit admissible evidence to the courts. It helps governments and organizations utilize resources and it boosts the awareness of the readiness to start an investigation (Dardick, Endicott-Popovsky, Gladyshev, Kemmerich, & Rudolph, 2014). While digital forensic readiness is a topic that can be a research by its own, the following section will only focus on the training opportunities and the knowledge needed to be acquired in order to start a digital forensic investigation.
Training opportunities play a huge role in digital forensic readiness. It gives the responsible staff the needed experience to analyze data and extract admissible evidence (Rowlingson, 2004). In order to fight cybercrimes and online frauds, it is vital to develop and maintain cybersecurity and digital forensic training programs whereby employees will get the needed experience and exposure to deal with data (Tu, Xu, Wira, Balan, & Cronin, 2012). Training opportunities help employees increase their mechanism to detect, analyze, and report cybercrime. Tu, Xu, Wira, Blan, & Cronin, also state that training opportunities also “ensure adequate analytical and technical capabilities for law enforcement, and it raises awareness among employees (2014).

2.2 The Occurrence of Digital Crime and Its Impact on Lebanese Society

As technology is advancing on daily basis, the occurrence of digital crime is increasing and is getting more sophisticated (Ionescu, L., 2011) From script kiddies attack to sophisticated attacks, organizations and governmental sites are being bombarded by huge numbers of viruses, fraudulent attacks and denial of service attacks on daily basis. Some are successful ones, some are a failure, but no one can deny the fact that there are at least hundreds of digital attacks and digital crimes performed daily.

In order to limit the scope, this work will look into smaller numbers and smaller cases. The scope is limited to include Lebanese systems and Lebanese organizations in order to study the importance of integrating a cyber-security law in Lebanon along with a digital forensics law. Due to the political tension in the region, and due to the enhancement in technology in the middle-east, Lebanon has witnessed several cyber-
attacks and cyber-crimes in the past few years. Some of these attacks had huge impacts, and some were just small attacks performed by script kiddies.

Through financial embezzlement, and identity theft, attackers have succeeded to transfer money to their accounts through 84 fraudulent transactions. Mr. Abdul Hafiz Mansour, secretary of the special investigation commission has commented that the first step to fight these types of crimes and to cease such fraudulent acts from happening, is to provide legal and legislative measures and raise the awareness among all banks and financial institutions. He added that there are draft laws pertaining to this issue that should be approved, most notably electronic signature and digital transactions. He confirms that these laws have been sitting in drawers at parliament for over 16 years. It is worth mentioning that the Lebanese financial and banking sector is considered to be one of the most important sectors in Lebanon, and it is targeted on a daily level to cyber-attacks (Halawi, 2016).

Away from the financial sector and from fraudulent attacks, Lebanon is also targeted through other attacks such as hacking and Denial of Service attacks (DOS and DDOS attacks) as a result of the political tension. One of the latest attacks occurred on November 11, 2017 where anonymous hackers have hacked the Special Investigation Commission (SIC) website under the name of the electronic Saudi Arabian hackers as they declared a cyber-war on Lebanon (Chemaly, 2017). The SIC has not yet responded to the attack, but they were able to recover their website within hours of the attack. Other attacks were also noted on governmental websites lately. It was witnessed that the Internal Security Forces (I.S.F) website got hacked. According to MTV news, which is a local Lebanese news station, on July 7, 2017 the I.S.F were being under a targeted attack
whereby anonymous hackers have changed the front-page of the I.S.F website to another page that shows the logo of the attackers under the name of “Syrian Revolution Army” (Most dangerous breach, 2017). However, the I.S.F were able to recover their website within few hours after the attack has occurred.

The Lebanese educational sector was also a target of cyber-attacks. As the educational system in Lebanon is shifting to a digitalized one, the latter has also had its chunk of cyber-crimes. On December 10, 2015, during the final exams period, the dean of students in the Lebanese American University (L.A.U) sent mass emails to students informing them that their website has been receiving a large scale of Distributed Denial of Service attack (DDOS attack), and that the website has crashed as a result of this attack. As part of L.A.U’s business continuity, the university was able to successfully publish two portals on two different servers in order to allow students to access their courses and download the material needed (Website Outrage, 2015). But again, who is responsible for this attack, or who should be accountable to such damage? This is a question that can only be answered through a cyber security law and a digital forensics investigation.

The rising number of digital attacks and cyber-crimes may be affecting organizations, businesses, and governmental sites directly, but there is a deeper and a bigger impact from these attacks on the Lebanese society. Cybercrimes in Lebanon have been divided into three categories in this paper: (a) attacks against financial institutions, (b) attacks against governmental sites, and (c) attacks on educational institutions. Each targeted attack has a big impact on society in a way.
Lately and for the first time in Lebanese history, Lebanese immigrants received an SMS informing them to register their names on a governmental website to be able to vote abroad in the next elections (Grace, 2017). The registration process required that Lebanese immigrants should include their names, ID numbers, phone numbers, email address, the address of residence, parents name, uploads of Lebanese ID’s and so on (Kantara, 2018). Lebanese people were excited to the idea as it was the first time in history that immigrants are given the rights to vote from their resident country. So after they started registering, people started receiving campaigns on social media and their emails from candidates to market their ideas and convince the immigrants to vote for them. The latter however raises a question of how candidates got their hands on the immigrants private information. Immigrants living in resident countries have laws against sharing private contact information, and sending (spamming) unsolicited emails, messages and text messages to people within their jurisdiction ((Kantara, 2018)). This leaves Lebanese people wondering whether or not the voting system or even the registration system is a credible one with the absence of a cyber-security law. Would Lebanese people trust to disclose their personal information on a governmental server especially within the absence of an unauthorized access law or distributing private information law? One of the articles that was published lately accuses the Lebanese government of being the source of a huge cyber-attack in 22 different countries. In spring 2017, and while security researchers at the “Lookout” cybersecurity firm were investigating a cyber-attack that took place in Kazakhstan (phishing and malware campaign), they came across a twin or a similar attack under the name of “Dark Caracal” originating from Lebanon which have turned out to be one of the most prolific hacking
campaigns ever documented. On January 2018, “Lookout” and another security firm under the name of the “Electronic Frontier Foundation” have released a fifty one page report that proves and claims that the source of the attack originated from a building in Lebanon, Beirut, and the building belongs to the Lebanon’s General Security (Marsa, 2018). Whether the Lebanese government was verdict to this accusation, or whether it was falsely accused, the question remains whether or not there should be a cyber law that protects everyone’s rights?

Although Lebanon is beginning to advance technologically, the question remains: Would all these technologies be effective and beneficiary in the absence of a cyber security law and digital forensics investigation? Moreover, is it important to implement a cyber security law and a digital forensics investigation procedure, or is it enough to keep the normal procedures as they are?

2.3 Cybercrime Combat through Laws

As discussed in section 2.2, the occurrence of digital crime and its impact on Lebanese society is under no shade from cyber-attacks. Every day, organizations, banks, educational institutions, or governmental websites are under the risk of being attacked by hacktivist groups (El Amine, 2017). This section will answer the remaining questions from previous discussions which are “how do countries worldwide combat such attacks?” and “how is Lebanon capable of fighting these attacks with the absence of a cybersecurity law and digital forensic investigations?”
First world countries have already established international laws and procedures in order to protect their citizens from the digital world. Let’s take a look at how first world countries are combating cybercrimes and compare them to the ones occurring in Lebanon. The following section will discuss different laws from the European continent, from the American continent, and finally from the Asian (Middle Eastern in particular) continent.

The General Data Protection Regulation well known as GDPR, is one of the recent most talked about international European laws (Haug, 2018). Goddard (2017) highlights the six general data protection regulations of GDPR and categorizes them into “fairness and lawfulness; purpose limitation; data minimisation; accuracy limitation; and integrity and confidentiality” (p.703). The law is not only limited to the European countries, but is extended to reach out to all organizations and institutions that deal with European citizens’ data that ranges from the most critical information such as card data, to the simplest collected information such as internet cookies (Frank & Wagner, 2018). It forces all entities to process European data in a secure manner, and ensures that European citizens are aware of any data breach that might affect their personal information. It also provides the European citizens with the “right to be forgotten” which ensures that data that is not needed anymore does not reside on the digital world unless it is needed for legal obligation (Kunz 2018). Hence, the importance of this regulation and the aim is to protect all European citizens’ data that resides on each and every server around the world (Smouter, 2018).

On the other hand, after the famous 9/11 attack in the United States of America, the states has declared the USA Patriot Act of 2001 which is a law that was signed by
president Bush to intercept and obstruct anti-terrorism (Laundering, 2001). The act has given information security officers the right to intercept and track communications from emails to telecommunication conversations (Doyle, 2002). Another famous cyber law that was approved by the congress of the U.S is the Computer Fraud and Abuse Act of 1986. In an attempt to fight computer related crimes and to limit the number of computer frauds and computer abuses, the act includes every computer in the United States, and millions of computers from other countries (Kerr, 2009). The law has been modified several times from the date of publication, as the congress has seen how important it is to cover all types of new cyber-attacks and cyber-crimes (Skibell, 2003).

The Kingdom of Saudi Arabia has already drafted and implemented a cyber security law to protect its citizens from any cyber-attacks. The law aims to enhance information security, protect rights pertaining to the legitimate use of computers and information networks, protect public interest, morals and common values, and protect the national economy (Elnaim, 2013). Elnaim (2013), also mentions that “The new Arab Cybercrime Agreement (no. 126 of 2012) was approved in Saudi Arabia. This agreement will mainly address the rise in electronic crime which embraces such crimes as credit card frauds, internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system interference, illegal access and interception and so on. It aims as well at encouraging cooperation between Arab countries in combating cybercrimes. The Agreement stipulates also on the importance of enforcing the Copyrights Law.”
On the other hand, although Lebanon is missing a cyber law, the Cybercrime and Intellectual Property Office within the I.S.F are fulfilling their tasks by arresting attackers who are performing simple cases. But how are they doing so? Under which cyber-laws do they have the right to arrest suspects and sentence them?

As the Lebanese cyber-law draft has been placed in a drawer for the parliaments to vote upon for several (Halawi, 2016), the Lebanese government has decided to protect the cyber world through mapping the normal convictional crime law to the cyber world (El-Chaer, 2013). There is no special procedure for cybercrimes. For example, the punishment for piracy and the use of torrents applies to the law of protection of literary and artistic property (El-Chaer, 2013). The Lebanese law through article 86 discusses the protection of literary and artistic property. Through article 86, the law states, “People
who abuse any copyrights in order to make revenues shall be punished by sentencing to prison from three months to three years and shall pay a fine that ranges from five million Lebanese Lira to fifty million” (Onaysse, 2013).

Few other laws related to communication were also put in place to protect people’s private communications from attacks or infringements. The Lebanese law through article 17 targets telecommunications services sector in the Lebanese Territories and includes the rules for its transfer, or the transfer of its administration, in full or in part, to the private sector (El Chaer, 2013).

The question that remains from the literature in this section is: What flaws in the current implemented laws are the reasons behind this gap, and what is its impact on the current cybercrime cases that are being handled in courts?

2.4 Judges’ Perception to cyber-crimes and cyber laws: Cyber law, Knowledge, and Evidence

From judges’ point of view, cybercrimes are similar to a regular convictional crime that includes a criminal case, a victim, a suspect, lawyers, and evidence. Based on all the latter inputs, in addition to judges’ knowledge and understanding of the topic of the case and based on the laws defined by a particular country or state, a judge can make up his/her mind and rule out on a cyber-crime case (Nawafleh et.al, 2016). Hence in order rule out a case, two important factors are pre-requisites: laws, and knowledge of the topic.
Through one of his interventions within the “First Regional Conference on Combating Cybercrime”, Dr. El-Chaer has argued that there is neither a crime nor a punishment without a law. It is a necessity to adapt a cyber-law that can criminalize any assault on information systems or usage of information systems in Lebanon and in the Arab world (El-Chaer, 2013). Dr. Elchaer adds through his intervention that most prosecutions that resulted from cybercrimes are being handled in comparison to the normal conventional Lebanese laws that were published and approved in 1943 (such as stealing, fraudulence, cheating, any many other typical crimes).

The following section will discuss several cybercrimes that have occurred in Lebanon, ways Lebanese judges dealt with these cases, and the effect the cyber law absence had on the judge’s decision.

Within the crimes against public morals and morality, a Lebanese guy was accused of publishing child pornography related materials on the internet. After digital evidence was submitted, the judge has accused the suspect of publishing child pornography materials, and has assigned a punishment for his actions according to articles 531, 532, and 533 of the Lebanese Law. However, the court of criminal appeal declined the judge’s ruling on the case, and punished the suspect according to article 533 of the Lebanese law since articles 531, and 532 do not define the internet as a tool for attack (El-Chaer, 2013). The absence of a cyber law in this case changed the punishment sentence on the suspect.

In another example, and under the category of fraud crime, a Lebanese person was accused of hacking into business owners’ email accounts where he sent emails to their relatives asking them for money. Moreover, after digital evidence was submitted to
the court, the judge assigned to this case declared that the suspect should be punished according to articles 655 and 636 of the Lebanese law. Later, the suspect was exempted from the punishment according to article 636 of the Lebanese law, as this article does not define an email account as something that can be stolen since it is not of financial value. Therefore, and through this example, the suspect was exempted from a deserved punishment due to the lack of cyber law that clearly defines cyber-crime and its punishment.

Moving on to the second pre-requisite for a judge to rule out on a cyber-crime, the judges’ knowledge of the topic (which in our case is cybercrime and digital attacks) is essential. Judges should be aware of the types of cybercrime and the tools or ways attackers use to hide evidence. While the civil judge is limited with certain types of proofing and evidence, the criminal judge, on the other hand, has complete freedom to accept or reject an evidence based on his assumptions, his vision of the case, and his vision of the digital evidence submitted to him (Nawafleh, Y., Nawafleh ,A., Nawafleh S., 2016). Thus, judges’ knowledge about the topic plays a big role in the judgment call on a cybercrime case. And since Lebanon has no cyber law yet, judges’ might have heard of cybercrimes, or might be aware of few cyber-attacks, but they are definitely not knowledgeable in that field. Therefore, knowing that prosecutors and judges do not have background in information technology, a reasonable trial result cannot be assured (Chang, 2012). This lack of knowledge about cybercrime and digital attacks, is what creates a gap between Lebanese courts and judges and the I.S.F.

In any cybercrime, the I.S.F through its Cybercrime and Intellectual Property Bureau which have professionals and experts in the digital forensic and cyber-attacks
field can actually cooperate well with judges if they were knowledgeable about Information Technology and its crimes. But it would take a lot of time to explain digital evidence and teach a judge about a cybercrime in case the judge had no knowledge about the topic; which will lead most of the time to a bad judgment or a false positive (Chang, 2012).

The literature continues by recommending a couple of solutions in order to cover the gap between the judges and the I.S.F, and to decrease the lack of knowledge within the courts. The solutions are concluded by implementing a cyber law first that would define cyber world. Second, sentences the penalty fines have to be put in practice if the cyber world was misused. Moreover, more seminars, conferences, and training sessions are to be implemented for judges. Fine tuning the relationship between information technology and between the law (judges in particular) whether by implementing a cyber law or by offering training opportunities raises the efficiency of solving cybercrimes, and raises the level of competence judges have in the use of information technology.
CHAPTER III

METHODOLOGY

Cybersecurity law is no different than any other law that is implemented or applied by a country. It conducts people and their behaviours in the digital world, and protects people’s digital assets, information, and businesses from cybercrimes. Digital forensics is the science of recovering and analysing computer related data in order to submit them as admissible evidence to the court in order to support or defend a crime. As the mentioned are the basis of the cyber world, and since their absence would result in chaos, it is vital to study the data collected from a qualitative and a quantitative perspective. A mixed method design helps the researcher analyse data profoundly and thoroughly since the study is exploratory and there is lack of previous research to support the current study. This chapter represents the research methodology implemented to carry out the current study.

3.1 Research Design

Quantitative research methodology is the mathematical and statistical analysis of the data collected by distributing surveys, polls, or questionnaire. The purpose of this methodology is to collect information from entities and external resources to better understand if the research defies its purpose or not. On the other hand, a qualitative research methodology is the analysis of data that is collected through interviews. It is a
very important methodology as the researcher will be able to better understand the reasons, motivations, and opinions towards a research or a subject.

This research uses a mixed method approach, a combination of both quantitative and qualitative research methodologies. The research for the topic “Legislation of Cyber Law and Digital Forensic in Lebanon” will require to both quantify the problem that is being discussed, collect information, opinions, discuss real life situations with the appropriate personnel to better understand the issue, and clarify how cybercrimes are being handled with the absence of a cyber law and a digital forensic procedure for cyber investigations.

Surveys and questionnaires about cyber laws and digital forensic procedures were distributed to a selected sample of employees in Lebanese banks (which represent the financial sector and the major factor in the Lebanese economy) to identify the level of awareness among Lebanese employees in organizations. In addition to measuring the level of cybercrimes in banks, it was necessary to verify whether or not the Lebanese society was aware of the consequences of a cybercrime. Surveys and questionnaires also served the purpose of identifying whether or not Lebanese people are aware of the “digital forensic” terminology and its importance to carry out cyber investigations.

On the other hand, interviews were also communicated with upper management within Lebanese judges to identify if there is a gap between the Lebanese courts and the I.S.F and to clarify how cyber-crimes are ruled out within the absence of a cyber-security law. Interviews with I.S.F members were also conducted to better understand how the I.S.F is currently functioning and carrying cyber-crimes and digital forensic investigations.
3.2 Method

3.2.1 Participants

In order to move forward with this research, the researcher had to interview one person from the Cybercrime and Intellectual Property Bureau in the I.S.F. The researcher did not have the opportunity to specify the sampling of the interviews. The researcher has requested to interview the head of Cyber Crime and Intellectual Property Bureau. The I.S.F assigned one participant from the higher management positions to participate in this research rather than accepting the original request. As per the Lebanese law, the researcher had first to submit a signed copy from the researcher’s university stating that the information collected through this interview will only be used for scientific research, and will not be disclosed to public media. After the letter was submitted and approved by the Public Relations Division, the researcher was informed that an interview with one personnel from the Cybercrime and Intellectual Property Bureau can be conducted, and was given the name, contact number, and the email of the interviewee to schedule a meeting. The researcher then was able to contact the interviewee and schedule an interview for forty five minutes with the I.S.F.

The interview questions that were asked to the I.S.F revolved around identifying the procedures applied by I.S.F to conduct a digital forensic investigation, relationship with the Lebanese judges in handling cybercrimes, I.S.F involvement in cyber security awareness and cybercrimes occurring in Lebanese organizations, and the availability of training opportunities for the Lebanese I.S.F (see appendix A)
In addition to the above interview conducted, five judges were contacted in the area of Beirut to discuss and better understand how cyber-crimes were being ruled out, laws that victims were condemned under, and reasons behind the gap between the Lebanese judges and the Lebanese Internal Security Forces. Random sampling was not necessary for this part of the research as these five judges are the only judges in Lebanon who are working in close cooperation with the I.S.F regarding cyber-crimes and digital forensic investigations. The researcher selected this sample because it best fits the purpose of this study, and because the number of judges who are assigned to this topic is limited.

As per the normal Lebanese procedure, the researcher had to contact the Ministry of Justice to get their approval to conduct interviews with five of their judges. A letter approved by the researcher’s university was handed to the Ministry of justice (M.O.J) for their approval. Once the M.O.J approved the request, the researcher contacted the nominated judges to check if they are willing to participate in the research and to schedule a twenty minute interview with each judge accordingly. The researcher had to wait for weeks to get the approval to conduct these interviews, and to actually find an available time slot with the judges.

The interview questions that targeted the five Lebanese judges revolved around identifying the reason behind the gaps between the Lebanese judges and courts, and between the Lebanese I.S.F, identifying the procedures taken by the Lebanese judges to confirm admissibility of digital evidence, the number of cybercrime cases assigned to the Lebanese courts, and identifying the basis for a judge to grant permission to conduct a digital forensic investigation (see appendix B).
To better serve the purpose of this study, questionnaires and surveys were also conducted and distributed to participants in an attempt to quantify the answers collected from the interview questions. A sample of 96 participants was selected by the researcher to better serve the purpose of this study. Questionnaires were sent and collected from the top four Lebanese local banks. The researcher has chosen to send the questionnaires specifically to Lebanese banks as the Central Bank of Lebanon obliges each Lebanese registered bank to have a cyber-security division running under its name to handle cyber-attacks and to protect the bank from any cybercrime. Questionnaires were sent and collected to the Information Security division of each of the selected bank (as they are the personnel most knowledgeable about the subject of this research), in addition to randomly selected divisions (retail support, small or medium enterprise banking, branch network and liabilities…).

The researcher had to contact the Human Resources division of each of the selected banks for their approval. Once the questionnaires were approved, the human resource division then distributed the link of the questionnaire that was provided by the researcher. The participants were given the right to accept or reject participating in this study. Once all approvals were received, the researcher had the right to distribute the link and collect the needed information. The questionnaire distributed to the five local Lebanese banks revolved around identifying if any digital services and digital transactions took place in the selected banks, and if the employees are aware of cyber security and of any cybercrime that took place in the selected bank or any other local Lebanese bank (see appendix C).
The below tables summarize the interviewee numbers along with their positions/divisions, and the interview duration.

**Interview conducted with I.S.F (Cyber Crime and Intellectual Property Bureau Section)**

<table>
<thead>
<tr>
<th>Interviewee number</th>
<th>Interviewee Position</th>
<th>Interview Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Lieutenant</td>
<td>First Lieutenant in the Cybercrime and Intellectual Property Bureau</td>
<td>Forty-Five minutes</td>
</tr>
</tbody>
</table>

**Interview conducted with Lebanese Judges**

<table>
<thead>
<tr>
<th>Interviewee Name</th>
<th>Interviewee Position</th>
<th>Interview Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Judge 1</td>
<td>First Investigating Judge</td>
<td>Twenty minutes</td>
</tr>
<tr>
<td>Judge 2</td>
<td>Admin Judge on the Information Centre in I.S.F</td>
<td>Twenty minutes</td>
</tr>
<tr>
<td>Judge 3</td>
<td>Deputy General of Appeals</td>
<td>Twenty minutes</td>
</tr>
<tr>
<td>Judge 4</td>
<td>Lebanese Judge</td>
<td>Twenty minutes</td>
</tr>
<tr>
<td>Judge 5</td>
<td>Lebanese Judge</td>
<td>Twenty minutes</td>
</tr>
</tbody>
</table>
3.3 Data Collection Procedures

After receiving approval from the public relations division in the I.S.F, the researcher visited the Cybercrime and Intellectual Property Bureau offices. A copy of the interview questions was sent to the interviewee to be checked and approved. Moreover, the copy gave the interviewee enough time to prepare any document that might come in handy. The interviewee was given the freedom not to participate in this research. Before the interview started, the researcher explained the purpose of the research and the reason behind the interview, and assured the interviewee that all personal information will remain confidential, and that interview answers will only be used for scientific purposes and will not be distributed to public media. At the end of the interview, the researcher gave the interviewee a copy of the interview answers for proof reading and was granted approval to use the answers in his research.

After the interview with I.S.F was conducted, the researcher received approval from the Ministry of Justice in order to conduct interviews with five Lebanese judges. The ministry also requested a copy of the interview questions ahead of time for approval. Once all approvals were received, the researcher visited each judge in his office on different days, and interviews were conducted. Judges had the freedom to participate in this research. The same procedure that was applied to conduct an interview with the I.S.F was applied for the Lebanese judges, as both entities run under the Lebanese governmental law.

After collecting all interview questions from the I.S.F and the Lebanese judges, the researcher was able to get approvals from four local Lebanese banks to distribute the
questionnaire link and collect the data from their information security division and from any randomly selected division.

3.4 Instruments for Data Collection

3.4.1 Interview with I.S.F

The interview was composed of twelve open/ended interview questions each with approximately four to five sub questions about the interviewee’s perception of cyber laws and digital forensic investigations and the current implemented infrastructure that is used by the I.S.F in order to perform cyber security investigations. The interview questions were developed specifically for this research by the researcher. Before the interview questions were sent to the I.S.F, they were reviewed and modified by two professors that hold a PhD in information systems and are specialized in information security. In addition to exploring the current implemented framework for combating cybercrime, the interview has shown some evidence on the importance of legislating a cyber security law and a digital forensic procedure in Lebanon.

While conducting the interview, the interviewee was asked for more clarifications on few points. Clarifications on few questions were also added to the interview to better understand the complex procedure applied by the Lebanese internal security forces while performing a cyber security investigation.

The conducted interviews took forty to forty-five minutes. The interview was held face to face in the First Lieutenant’s office. The interview was phone recorded after the approval of the interviewee. Recordings were zipped and compressed securely (password protected), and were stored on the researchers personal computer for reference.
3.4.2 Interviews with Lebanese Judges

Interviews with Lebanese judges consisted of five open/ended questions each with approximately two or three sub questions about the interviewee’s perception of the reasons behind the gap between I.S.F and Lebanese judges (if any), and about identifying the procedures taken by Lebanese judges regarding cybercrime cases. This instrument have confirmed the gap between the I.S.F and the Lebanese judges and have shed light the importance of the legislation of a cyber security law along with a digital forensic procedure.

Each conducted interview took 15 to 20 minutes. Interviews were also phone recorded after the approval of the judges. Recordings were stored on the researcher’s personal computer for later references (password protected).

3.4.3 Questionnaire

After conducting the interviews with both I.S.F and the Lebanese judges, the researcher started working on the quantitative questionnaires, then handed the questionnaire link to the Lebanese banks in order to be filled within a time frame of one week. Banks were given the option to select either the English or the Arabic language by preference to fill out the questionnaires and surveys. All banks selected the English language to fill out the questionnaire and surveys especially that all their employees were familiar with the English terminologies of cybercrimes.

The questionnaire was divided to five parts: personal information (gender, age, profession level, and level of knowledge about cybercrime and about cyber security in the banking sector), E-Banking services that are used, the occurrence of cybercrime through
the banking sector, mapping between absence of cyber laws and the motivation to target the banking sector, and finally the relationship between absence of cyber laws along with the security performance of the bank. The questionnaire was taken and modified from a previously prepared questionnaire (Wada, 2011).

3.5 Data Analysis

3.5.1 Analyzing the interview responses

After the researcher has conducted five interviews with senior Lebanese judges, and with a senior personnel from the I.S.F, all six interviews were transcribed. Then, the researcher analysed the interview responses using open-coding which is known for highlighting the headings and the categories of all transcribed data (Burnard, 1991). Open-coding was conducted by reading the transcribed interviews and highlighting headings, titles, terminologies, statements, and major concepts. All transcribed interviews were also shared with two other researchers who are professionals about the subject, and the same exercise was done in an attempt to validate the accuracy of the open-coding method. The results were then compared by all three researchers.

Once the above exercise was done, the researcher counted the frequency and repetition of similar concepts identified within each question of all six interviews conducted. Since only one interview was conducted with a senior level personnel in the I.S.F (intellectual property and cyber bureau office), frequency of answers was only limited to one opinion as the interview questions were exploratory and highlighted how the I.S.F dealt with cybercrimes. The occurrence of similar concepts and statements
through all interview questions allowed the researcher to answer the first two questions in this paper.

3.5.2 Analyzing the Questionnaire.

After the responses to the questionnaires were collected through survey monkey, the information was extracted and was imported to smartPLS for analysis. SmartPLS is a structural equation modeling software that deals and creates relations between responses to come up with model that better explains the relation between different questions in surveys and questionnaires (Monecke & Leisch, 2012).

Once the data was imported and validated on the software, the researcher constructed different logical models and validated their alphas until the best model came to life. The model presented in the following section.
CHAPTER IV

RESULTS

The results in this chapter are divided into three parts. The first and second part of the results are based on the data collected from interviews conducted with the Lebanese judges and the I.S.F regarding cyber-crime and the way it is being dealt with in Lebanon within the absence of a cyber law and digital forensic procedures. The I.S.F is exerting an effort to track cyber-crime and the judges are doing the same to rule out on cyber-crime cases. That stated, the below tables define the current procedures undertaken by the I.S.F to investigate cybercrimes and highlight the flaws in the current implemented system. Moreover, the tables present the effect of the absence of cyber laws and digital forensic procedures on the current cybercrime cases. The third part of the results represents data that was collected from Lebanese banks in order to measure the level of impact of the absence of cyber law and digital forensic procedures and to highlight the significance of adding these laws to the existing system. Results highlight the frequency of the occurrence of cybercrime on the Lebanese financial sector and the importance of integrating cyber laws and digital forensic procedures to the existing system.

4.1 Current Implemented Cybercrime and Digital Forensic Investigation

For the purpose of this exploratory research about cybercrime and digital forensic investigations within the absence of cyber laws, the researcher conducted an interview with a senior member in the Cybercrime and Intellectual Property Bureau office in the I.S.F. The interview was semi-structured and lasted for 45 minutes. The interview was composed of thirteen questions, where each question had a maximum of two or three sub
questions related to the topic of the question. The I.S.F member’s response to the interview questions was analyzed using the open-coding strategy which was described in the methodology chapter.

The model below is a suggested model that highlights the current implemented path for a cybercrime and a digital forensic investigation which can be used for future research.

Fig 4: The current implemented flow for cybercrime and digital forensic investigations

4.1.1 Cybercrime and Intellectual Property Office in the I.S.F.

The analysis of the interview with the I.S.F member showed four different points. The points mentioned are recorded in along with the frequencies.

Table 1

<table>
<thead>
<tr>
<th>有效 / 无效</th>
<th>频率</th>
</tr>
</thead>
<tbody>
<tr>
<td>受法律保护</td>
<td>1</td>
</tr>
<tr>
<td>自2006年功能有效</td>
<td>1</td>
</tr>
</tbody>
</table>
The I.S.F member responded to many of the questions asked and stated that the I.S.F can’t start their investigation unless:

- Cybercrime and Intellectual property bureau are not allowed to take any action before getting judge’s approval.
- Someone, maybe the victim, or the victim’s family has reported the crime.

4.1.3 I.S.F Capabilities and Trainings. The analysis of the interview I.S.F member showed two different points. The points mentioned are recorded in the below table along with their frequencies and their percentages.
Table 3

*Reasons for Cybercrime Office to Start Investigations*

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular training</td>
<td>1</td>
</tr>
<tr>
<td>Attending courses</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2</strong></td>
</tr>
</tbody>
</table>

N= 1 I.S.F member

The researcher has explicitly asked “Does the I.S.F send employees to professional trainings on regular basis”, and the response for this question was the following:

- The people who work in our digital forensics labs are being trained regularly and are assigned to attend courses related to digital forensics.
- Employees are being registered in cybersecurity and digital forensic classes to empower their knowledge.

4.1.4 **Tools used in cybercrime and digital forensic investigations.** The analysis of the interview of the I.S.F member showed two different points. The points mentioned are recorded in the below table along with their frequencies and their percentages.

Table 4

*Reasons for Cybercrime Office to Start Investigations*

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Source</td>
<td>1</td>
</tr>
<tr>
<td>Licensed software</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2</strong></td>
</tr>
</tbody>
</table>

N= 1 I.S.F member

The I.S.F member has stated that “I.S.F uses digital forensics tools through their digital forensics investigations. Both private licensed and public open source tools are being used depending on the functionality and the criticality of the case”.

45
4.1.5 Communication with people, and awareness campaigns. The analysis of the I.S.F member showed two different points. The points mentioned are recorded in the below table along with their frequencies and their percentages.

Table 5

Communication with people, and awareness campaigns.

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication through Public Relation division</td>
<td>1</td>
</tr>
<tr>
<td>Approval from PR division</td>
<td>1</td>
</tr>
<tr>
<td>Regular awareness sessions</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>3</strong></td>
</tr>
</tbody>
</table>

N= 1 I.S.F member

The I.S.F member has responded to awareness campaigns and to communication with people through the below statements:

- We contact the Public Relations Division, and inform them that we need to spread the news regarding a particular crime or security event, and once they approve it, then we have the rights to go to the media and spread the news. Otherwise, we have no authority to use the media as a channel to spread the news.
- We are performing regular awareness sessions through universities, schools, and through media (LBC, MTV, and other Lebanese media) and social media (twitter, facebook….)

4.2 Lebanese Judges’ perception to cybercrime and its effect on current cases

In order to understand what flaws in the current implemented laws are responsible for the gap between the I.S.F and the Lebanese judges, the researcher performed five interviews with senior Lebanese judges. The interviews were semi-structured and lasted on an average of 20 minutes per interview. The interview was composed of six questions;
each question had a maximum of two or three sub question related to the topic. The judges’ responses to the interview questions were then analyzed using the open-coding strategy which is described in the methods chapter.

The model shown in Figure 5 shows the flow of the data collected and highlighted the effect resulting from the absence of cyber laws and digital forensic procedures and its effect on the economy and organizations. The model represents eight hypotheses: No education, lack of awareness for people, lack of awareness for politicians, political conflicts, lack of knowledge, absence of cyber laws, loss/missing digital evidence, misjudgment on cases, and acceptance of all digital evidence regardless of its admissibility. These hypotheses will be later discussed in the discussion chapter.
Fig 5: The reason behind the gap between I.S.F and the courts, and its effect on current cybercrime cases

4.2.1 Incapability of confirmation of digital evidence through cybercrime cases. The analysis of the judges’ statements showed five different responses that are related to the judges’ incapability of confirming that digital evidence is not tainted and is admissible to the courts. The responses are shown in the Table 6 along with their frequencies and their percentages.
Table 6

Incapability of confirmation of digital evidence

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can’t confirm admissibility of digital evidence</td>
<td>4</td>
<td>36.36</td>
</tr>
<tr>
<td>Judges’ call to confirm admissibility of digital evidence</td>
<td>3</td>
<td>27.27</td>
</tr>
<tr>
<td>Absence of cyber law or digital forensic procedures</td>
<td>2</td>
<td>18.18</td>
</tr>
<tr>
<td>Suspects negate digital evidence</td>
<td>1</td>
<td>9.09</td>
</tr>
<tr>
<td>Any evidence submitted by I.S.F is admissible</td>
<td>1</td>
<td>9.09</td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges & 1 I.S.F member

Judges’ provided their perspective to the incapability of confirmation of digital evidences in different ways. One judge, for example stated that “As long as there is no cyber law or digital forensic procedure, we can’t confirm if the evidence is admissible or not”, while another judge has stated that “Suspects sometimes might negate these evidences and we can’t confirm if this is true or not as evidence did not follow certain procedures to be collected”. The I.S.F member on the other hand stated that “It all depends on the judge assigned to the case. He has the right to accept or reject certain evidence”.

4.2.2 Recommendations that will help courts and judges overcome difficulties faced through cybercrime cases. The analysis of the judges’ responses to the interview questions highlighted three different recommendations to overcome difficulties that are faced while ruling out on a cybercrime case. While all judges have agreed that the implementation of cyber laws and digital forensic procedures is one way to overcome difficulties, three judges also highlighted that increasing the number of training opportunities related to the subject for Lebanese judges would also be a good
recommendation. The recommendations are stated in Table 7 with their corresponding frequencies and percentages.

Table 7

Recommendations that will help courts judges, and I.S.F to overcome cybercrime difficulties

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The implementation of cyber law and digital forensics</td>
<td>6</td>
<td>60</td>
</tr>
<tr>
<td>Increasing the number of training opportunities</td>
<td>3</td>
<td>30</td>
</tr>
<tr>
<td>Prioritize voting on cyber law in Lebanese Parliament</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>10</td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

N=5 judges & 1 I.S.F member

Judges provided different recommendations to overcome the difficulties faced in the courts while ruling out on cybercrime cases. A senior judge in the Lebanese courts stated:

Implement a cyber-law that defines all cyber-attacks and how to deal with them. Another judge stated: I believe that the best solution on this case is to conduct more training sessions and more awareness sessions about cybercrime and how to deal with it.

I.S.F member commented: once the law is set and once digital forensics is enforced through the law, we will have specialized judges.

4.2.3 Reasons leading to the gap between judges and I.S.F members while performing a cybercrime investigation. The analysis of judges’ responses highlighted different reasons that lead to the gap between judges and I.S.F. Three stated that the lack of knowledge about cybercrime plays a major role. Three out of five judges also stated that the absence of cyber law or digital forensic procedures is a major reason behind the gap.

The results are stated in Table 3 below along with their frequencies and percentages.
Table 8

*Reasons leading to the gap between judges and I.S.F*

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of knowledge about cybercrime</td>
<td>4</td>
<td>30.76</td>
</tr>
<tr>
<td>Absence of cyber law or digital forensic procedures</td>
<td>3</td>
<td>23.07</td>
</tr>
<tr>
<td>Lack of technical skills</td>
<td>3</td>
<td>23.07</td>
</tr>
<tr>
<td>Subject not given as core requirement in universities</td>
<td>1</td>
<td>7.69</td>
</tr>
<tr>
<td>Lack of training opportunities</td>
<td>1</td>
<td>8.33</td>
</tr>
<tr>
<td>Not aware about the importance of the subject</td>
<td>1</td>
<td>8.33</td>
</tr>
</tbody>
</table>

Total 13 100

N=5 judges & 1 I.S.F member

The participants were asked: “What are the reasons behind the gap between the Lebanese judges and the I.S.F?”, the judges’ responses to this question included statement as:

“The main reason behind this gap is that in Lebanon we did not yet implement a cyber law that can protect people’s right and hence the interests to create cybercrime training opportunities is not enough”

“Lebanese lawyers and judges do no study this material as a core requirement through their educational cycle”

“The judges in court they do not yet have the knowledge to reject a digital forensics evidence (perhaps because there was a step missing) as there is nothing in the law that forces us to follow any standards”

4.2.4 *Importance of implementing cyber law and digital forensic procedure.* The analysis of the judges responses to the importance of implementing a cyber law and digital forensic procedures in Lebanon showed that all judges agreed that it would help increase their knowledge and skills about the subject. Four judges highlighted that there would be an increase in training opportunities, and four judges agreed that it would give them a good definition of what is considered to be a cybercrime and what punishment should be associated with the crime. Table 9 represents the importance of implementing a cyber law and digital forensic procedures, along with their frequency and percentages.
Table 9

Importance of implementing cyber law and digital forensic procedure

Effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase of knowledge and skills to judges about the subject</td>
<td>5</td>
<td>16.12</td>
</tr>
<tr>
<td>Increase training opportunities</td>
<td>4</td>
<td>12.90</td>
</tr>
<tr>
<td>Definition and confirmation of digital evidence</td>
<td>4</td>
<td>12.90</td>
</tr>
<tr>
<td>Limitation of the number of cybercrime cases</td>
<td>4</td>
<td>12.90</td>
</tr>
<tr>
<td>Definition of cybercrime and its punishments</td>
<td>4</td>
<td>12.90</td>
</tr>
<tr>
<td>Obligation to teach cyber law as a core course</td>
<td>3</td>
<td>9.67</td>
</tr>
<tr>
<td>Increase in awareness</td>
<td>2</td>
<td>6.45</td>
</tr>
<tr>
<td>Evolution of digital world in the country</td>
<td>1</td>
<td>3.22</td>
</tr>
<tr>
<td>Courts will be interested to create a cybercrime division</td>
<td>1</td>
<td>3.22</td>
</tr>
<tr>
<td>Covers digital aspect in normal convictional crime</td>
<td>1</td>
<td>3.22</td>
</tr>
<tr>
<td>Protection of people and their assets</td>
<td>1</td>
<td>3.22</td>
</tr>
<tr>
<td>Known responsibilities and specific frameworks to follow</td>
<td>1</td>
<td>3.22</td>
</tr>
<tr>
<td>Total</td>
<td>31</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges & 1 I.S.F member

The judges’ and I.S.F responses included statements such as:

- “If a cyber law is implemented in Lebanon, then we will be obliged to teach this law through our educational program.”
- The implementation of a cyber law would define what is a crime and who is considered to be a suspect in a digital crime”
- Our responsibilities will be more defined and we will start working under a specific framework with specific duties rather than working based on experience.

Four judges believe that once a cyber law and digital forensic procedures are implemented, the number of cybercrime cases in Lebanon will be limited, and the training opportunities offered by the courts will increase. Three judges agreed that it will be an obligation to teach cyber law as a core requirement in universities. Two judges said that there would be an increase in the awareness levels for judges and for people. One judge said that it would help the Lebanese country develop and evolve in the digital world.
4.2.5 Absence of cyber laws and digital forensic procedures in Lebanon. The judges’ highlighted terminologies related to the absence of cyber laws and digital forensic procedures throughout the interview. Four judges have used the terminology “Absence of cyber law”, three judges have referred to the point that the “Current Lebanese law does not cover cybercrime”, and two judges have pointed out that “Absence of digital forensic procedures to extract evidence is effecting cybercrime cases in courts.” Table 10 summarizes the terminologies along with their frequencies and percentages.

<table>
<thead>
<tr>
<th>Absence of cyber laws and digital forensic procedures effective / ineffective</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence of cyber law</td>
<td>5</td>
<td>45.45</td>
</tr>
<tr>
<td>Current Lebanese law does not cover cybercrime</td>
<td>3</td>
<td>27.27</td>
</tr>
<tr>
<td>Absence of digital forensic procedures to extract evidence</td>
<td>3</td>
<td>27.27</td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges & 1 I.S.F member

Judges’ and I.S.F member have used the below statement throughout the whole interview:

- “As you know, Lebanon lacks the absence of a cyber law”
- “Everything related to computer crime such as ecommerce or any related online service lacks the legal aspect in Lebanon”

4.2.6 The number of cybercrime cases in Lebanon within the past 5 years. The judges’ responses to the question” Within the past 5 years, did you notice any change in the number of cybercrime cases” showed that all five judges have agreed to the fact that the numbers have definitely increased in Lebanon. No other responses were highlighted in this question. Table 6 represents the common answer given by the judges regarding this question.
Table 11

*Number of cybercrime within the past 5 years*

**Effective / Ineffective**

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase in the number of cybercrime</td>
<td>5</td>
<td>100</td>
</tr>
<tr>
<td>Total</td>
<td>5</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges

One judge said that “The numbers definitely have doubled or even tripled within the past five years”, while another judge has agreed but with a different statement such as “There is an increase in cybercrime within the past 5 years. Usually I.S.F does these kinds of statistics, but I can assure you that the number has increased”

4.2.7 The reasons behind the increase in cybercrime in Lebanon. The analysis of judges’ responses to the reasons behind the increase in cybercrime in Lebanon showed five different reasons. Four judges have stated that people in our days are relying vastly on technology which could be a main reason behind the increase in cybercrime. Four judges have highlighted that people in Lebanon are easily disclosing personal information as they lack awareness about cyber security and about cybercrime. The reasons behind the increase in the numbers of cybercrime in Lebanon are represented in Table 12 along with their frequencies and percentages.

Table 12

*Reasons for the increase in cybercrime*  

**Effective / Ineffective**

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>People are relying on technology</td>
<td>4</td>
<td>30.7</td>
</tr>
<tr>
<td>Ease of disclosing personal information</td>
<td>4</td>
<td>30.7</td>
</tr>
</tbody>
</table>
Lack of awareness 3 23
Absence of Cyber laws 1 7.6
Information as a target for attacks 1 7.6
Total 13 100

N=5 judges

The participants were asked “What do you think is the reason behind this change?” the judges’ responses to this question included statements as:

“I believe that the main reason behind this change is that the Lebanese people are relying more on the internet and are disclosing their personal information easily without taking into consideration to cybercrime”

“I think as we rely more on technology, our personal data will be target to more attacks”

4.2.8 Efforts to assist judges in understanding and confirming digital evidence submitted for a cybercrime case. Throughout the interview questions, judges have highlighted several times that there are some external efforts that are being used as an input to let the judges understand and confirm digital evidence. Three judges have mentioned that they are hiring digital forensic specialists in order to assist them with cybercrime cases. The efforts required to assist the judges in confirming and understanding digital evidence are highlighted in Table 13.

Table 13

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiring digital forensic specialists</td>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>Assistance from technical people</td>
<td>1</td>
<td>20</td>
</tr>
</tbody>
</table>
General statements from judges included:

- I have requested the assistance of a technical person to understand the evidence several times on many of my cases.
- If I have any concerns or questions, I would either ask them or assign external professional analyst to give me a report about a digital evidence.

4.2.9 Reasons to deny digital evidence from I.S.F. The analysis of judges’ responses to the question “What are three reasons to deny a cyber security request from I.S.F?” have shown that there is no criteria to deny any digital evidence. All five judges have agreed that judges take into consideration all digital evidence that is submitted to the courts. The reasons are stated in Table 14 along with their frequencies and percentage.

Table 14

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No special criteria to deny any digital evidence</td>
<td>5</td>
<td>71.4</td>
</tr>
<tr>
<td>Judge has the right to ask for clarifications</td>
<td>1</td>
<td>14.2</td>
</tr>
<tr>
<td>Absence of standards to deny digital evidence</td>
<td>1</td>
<td>14.2</td>
</tr>
<tr>
<td>Total</td>
<td>7</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges

One judge stated that “There are no reasons to deny any cyber security requests or evidence from the I.S.F. There are no clear procedures or frameworks that we as judges need to follow in order to accept or deny any digital evidence or cybercrime” while
another judge stated that “The judge has the right to ask for clarifications and for technical assistance. If he was not convinced by the evidence, then he has the right to deny the cyber security evidence”

4.2.10 Reasons to start a cybercrime investigation by the I.S.F. The analysis of the judges’ responses have showed that the I.S.F will not start an investigation unless an incident is reported. All five judges have agreed that a victim needs to report an incident before the I.S.F takes action or an investigation is initiated. Table 15 summarizes the reasons to start a cybercrime investigation in Lebanon.

Table 15

Reasons to start a cybercrime investigation

<table>
<thead>
<tr>
<th>effective / ineffective</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim reported an incident</td>
<td>5</td>
<td>55.5</td>
</tr>
<tr>
<td>No actions unless cybercrime is reported</td>
<td>4</td>
<td>44.4</td>
</tr>
<tr>
<td>Total</td>
<td>9</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges

Judges responses included statements such as:

- I.S.F does not start their investigations unless a crime was reported
- The main reason behind the investigations is the occurrence of a cybercrime. And if the victim did not report the crime, then the I.S.F will not take any action.

4.2.11 Reasons for the absence of cyber law and digital forensic procedures in Lebanon.

The analysis of judges’ responses to the question “Why do you think Lebanon does not have a cybersecurity law yet?” showed five different responses. Three judges believe that
this is not a priority yet to the Lebanese politicians, while three judges believed that
Lebanese people and politicians are now aware of cybercrime impact on society. Two
judges believe that the main reason is due to political issues and conflicts. Table 16
highlights all five responses along with their frequencies and percentages.

Table 16

*Reasons for the absence of cyber law and digital forensic procedures*

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not a priority to politicians</td>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>Drafts conflicts</td>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>Not aware of cybercrime impact on society</td>
<td>2</td>
<td>16.6</td>
</tr>
<tr>
<td>Lack of awareness for people and politicians</td>
<td>2</td>
<td>16.6</td>
</tr>
<tr>
<td>Political issues</td>
<td>2</td>
<td>16.6</td>
</tr>
<tr>
<td>Total</td>
<td>12</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges

One judge stated that “The Lebanese parliament is not being very productive about this
issue. When two Lebanese political parties are drafting a cyber law, the politicians are
fighting over the validity of these cyber laws and over which law should be chosen, and
hence this is leading to the dismissal of the voting or the implementation of a cyber law”,
while another judge stated that “One other reason which I believe is delaying the
implementation of a cyber security law is that it is not considered as a priority yet.”

4.2.12 Judges’ and I.S.F efforts to overcome the difficulties faced due to the absence of
cyber law and digital forensic procedures in Lebanon. The analysis of judges’
responses has showed that the judges are putting personal efforts to define cybercrime
and to determine the deserved punishment for cybercrime cases. All five judges have
agreed that they are improvising by mapping the current penal law to cybercrime cases.
Three judges stated that there are few negligible laws that apply to few cybercrime cases that are occurring in Lebanon. The different efforts performed by Lebanese judges are represented in Table 17.

Table 17

*Judges’ and I.S.F efforts to overcome the difficulties faced due to the absence of cyber law and digital forensic procedures*

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improvising while mapping current law to cybercrime</td>
<td>6</td>
<td>50</td>
</tr>
<tr>
<td>Few current laws might refer to cybercrime</td>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>Additional tangible evidence is required</td>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>12</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges & 1 I.S.F member

Judges’ & I.S.F member responses included statements such as:

- Judges are improvising where they are mapping the cybercrime to the normal convictional crime. To what consent will this be doable I can’t really tell.
- I think the courts are performing what is said to be adaptation to the current law.
- We have few laws that might be related to cybercrime in one way or another such as the intellectual property law or the phone tap communication law.

### 4.2.13 Organizations as a target for cybercrime and cyber-attacks

The judges’ responses have shown that Lebanese organizations such as the financial sector, educational sector, and human crimes are targeted using cybercrime. The different people and organizations affected are highlighted in the below table.
Table 18

*Organizations and incidents being target for cybercrime*

*effective / ineffective*

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lebanese financial sector</td>
<td>3</td>
<td>50</td>
</tr>
<tr>
<td>Lebanese educational sector</td>
<td>2</td>
<td>33.3</td>
</tr>
<tr>
<td>Murder</td>
<td>1</td>
<td>16.6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>6</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

N=5 judges

Three judges have mentioned that the Lebanese financial sector is being a target for cybercrime where one judge has stated that “We have heard a lot of cybercrime cases targeting the Lebanese financial sector and especially the Lebanese banks”, while another judge has highlighted that “The Central Bank of Lebanon has even published a report that states the increase in cybercrime on the Lebanese bank”.

4.2.14 Drafts waiting to be voted upon in the Lebanese parliament. Through the analysis of judges’ responses, they highlighted that there are several drafts in the Lebanese parliament that actually defines a cyber law, and a digital forensic procedures. Three judges have mentioned that the drafts include digital forensic procedures, while two judges stated that the cyber law includes and tackles e-commerce, privacy issues, and cybercrime. Two judges have also stated that the drafts have been submitted to the Lebanese parliament since 2005. Table 19 states the highlights referring to the drafts waiting to be voted upon in the Lebanese Parliament.
Table 19

Drafts waiting to be voted upon in Lebanese parliament

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes digital forensic procedure</td>
<td>3</td>
<td>37.50</td>
</tr>
<tr>
<td>Drafts since 2005</td>
<td>3</td>
<td>37.50</td>
</tr>
<tr>
<td>Includes e-commerce, privacy issues, cybercrime</td>
<td>2</td>
<td>25.00</td>
</tr>
<tr>
<td>Total</td>
<td>8</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges & 1 I.S.F member

Judges’ responses included statements as:

- I even myself have joined tens of committees to write and draft these laws
- This law was drafted several times over several years and it is still not legislated.

4.2.15 Effect of the absence of cyber laws and digital forensic procedures on the current Lebanese cybercrime cases. The analysis of judges’ responses exposed seven different topics on how the absence of cyber laws and digital forensic procedures are actually affecting the Lebanese cybercrime cases. Four judges stated that they are enable to map each and every cybercrime to the current implemented laws. Three judges stated that no fair judgment can be made with the absence of a cyber law. Two judges stated that the absence of a cyber-law is actually motivating attackers to perform cyber-attacks as there is nothing that can legally bind them to a criminal case. The different effects are represented in Table 20 along with their frequencies and percentages.
Table 20

*Effect of the absence of cyber laws and digital forensic procedures on current cases*

effective / ineffective

<table>
<thead>
<tr>
<th>Reasons</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inability to map cybercrime cases to current laws</td>
<td>4</td>
<td>17.3</td>
</tr>
<tr>
<td>Loss of vital digital evidence</td>
<td>4</td>
<td>17.3</td>
</tr>
<tr>
<td>Digital evidence missed out</td>
<td>4</td>
<td>17.3</td>
</tr>
<tr>
<td>Can’t confirm admissibility of digital evidence</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>No fair judgements</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>Inefficient interpretation of digital evidence</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>Increases motivation for attackers</td>
<td>2</td>
<td>8.6</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
<td>100</td>
</tr>
</tbody>
</table>

N=5 judges

Judges’ responses included statements such as:

- At one case that we heard about as judges (we can’t confirm), a drug dealer was arrested in the Lebanese airport for carrying drugs on the spot, and there were no technicians yet. The team at the airport tried to log in to the suspect’s phone several times to look for evidence, which lead to wiping his phone for several wrong password attempts at the end.
- Some are not getting fair judgements as mapping digital crime to our regular law may not cover the whole crime.
- I believe that there are many digital evidence that is left out on many cases.

4.3 The Impact of the absence of Cyber Laws on Organizations and Economy

In an attempt to interpret the impact of the absence of cyber laws on organizations, and on the economy, the researcher has distributed a questionnaire to four different big banks in Lebanon, and responses were collected immediately as the distribution was done using an online link (Surveymonkey). The researcher was able to collect responses from 96 participants. The questionnaire consisted of five different topics that were defined in the methods chapter.
4.3.1 E-Banking services in Banks.

The analysis of the use of the E-Banking services used in banks across Lebanon was quantified through seven different categories: Online transfers, online bill pay, online deposit accounts, wire transfers, online banking demo, ATM cash withdrawals, and credit card services. The below figures show the graphical representation of the data collected along with the weighted average of each option (ranges from 1 which is strongly disagree, to 7 which is strongly agree).

Fig 6: Graphical representation of the use of online services

The data collected above for this question shows that the ATM cash/withdrawals is the most used online service in Lebanon with a weighted average of 6.14/7 while the lowest online service used is the online deposit accounts with a weighted average of 4.91/7.
4.3.2 The occurrence of Cybercrime through the Banking sector

The analysis of the occurrence of Cybercrime through the Banking sector was quantified through seven different categories and was measured on the respondent bank, and on other banks: Online banking related crime, identity theft (phishing), ATM fraud, online money laundering, email scam, and unauthorized withdrawals. The below figures show the graphic representation of the data collected along with the weighted average of each option (ranges from 1 which is strongly disagree to 7 which is strongly agree).
The data collected from the above for this question shows a slight increase between the respondents’ bank breaches from the breaches occurring in other banks that the respondent does not work in. The highest cybercrimes that are occurring in banks as per the data collection is the email scam with a weighted average of 4.76/7 and the online money laundering with a weighted average of 5.56/7.

<table>
<thead>
<tr>
<th>Crime</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>SOMETHING DISAGREE</th>
<th>NEUTRAL</th>
<th>SOMETHING AGREE</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
<th>TOTAL</th>
<th>WEIGHTED AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online banking related crime</td>
<td>2.29%</td>
<td>14.58%</td>
<td>3.13%</td>
<td>4.37%</td>
<td>17.71%</td>
<td>15</td>
<td>30.21%</td>
<td>11.46%</td>
<td>4.58</td>
</tr>
<tr>
<td>Identity theft (Phishing)</td>
<td>6.25%</td>
<td>12.50%</td>
<td>4.37%</td>
<td>19.79%</td>
<td>14.58%</td>
<td>14</td>
<td>25.00%</td>
<td>17.71%</td>
<td>4.70</td>
</tr>
<tr>
<td>ATM fraud</td>
<td>7.29%</td>
<td>8.33%</td>
<td>7.29%</td>
<td>28.13%</td>
<td>15.63%</td>
<td>15</td>
<td>21.88%</td>
<td>11.46%</td>
<td>4.48</td>
</tr>
<tr>
<td>Online money laundering</td>
<td>5.51%</td>
<td>14.58%</td>
<td>2.33%</td>
<td>29.77%</td>
<td>12.50%</td>
<td>12</td>
<td>21.88%</td>
<td>12.54%</td>
<td>4.49</td>
</tr>
<tr>
<td>Email scam</td>
<td>6.25%</td>
<td>7.29%</td>
<td>5.21%</td>
<td>23.99%</td>
<td>17.71%</td>
<td>17</td>
<td>21.88%</td>
<td>17.71%</td>
<td>4.76</td>
</tr>
<tr>
<td>Unauthorized withdrawals from customer's account</td>
<td>7.29%</td>
<td>14.58%</td>
<td>3.13%</td>
<td>27.05%</td>
<td>14.58%</td>
<td>16.67%</td>
<td>14.58%</td>
<td>4.35</td>
<td></td>
</tr>
</tbody>
</table>

Fig 8: Respondents’ Bank - Breaches

Fig 9: Other Bank - Breaches

Fig 10: Detailed representation of the respondents’ bank breaches
4.3.3 How is the Absence of Cyber Laws Motivating Attackers:

The analysis of how the absence of cyber laws is motivating attackers to perform cybercrime on the banking sector was quantified into four categories: the absence of cyber laws is motivating the attackers to perform identity theft crimes, ATM frauds, email scams, and unauthorized withdrawals. The below figures show the graphic representation of the data collected along with the weighted average of each option (ranges from 1 which is strongly disagree, to 7 which is strongly agree).
The data collected from the respondents show that the absence of cyber laws is motivating attackers to perform mostly Email scam attacks with a weighted average of 5.8/7, along with identity theft 5.77/7, and ATM frauds and unauthorized withdrawals 5.71/7

Fig 13: Detailed representation of Motivation of Attackers to perform Cybercrime due to Absence of Law

4.3.4 How is the Absence of Cyber Laws affecting the cybersecurity performance of banks?

The analysis of how the absence of cyber laws is affecting the cybersecurity performance of the banks was quantified to three categories: banks being demotivated to perform cybersecurity trainings, disregarding reporting cybercrime to I.S.F, and confusion on how to deal with insider attacks. The below figures show the graphic representation of the data collected along with the weighted average of each option (ranges from 1 which is strongly disagree, to 7 which is strongly agree).
Fig 14: The effect that the absence of cyber laws has left on cybersecurity performance in banks

The data collected shows that the absence of cybersecurity laws is a main reason for banks to disregard reporting cybercrime cases to I.S.F with a weighted average of 5.04/7, in addition to it demotivating banks to perform cybersecurity trainings with an average of 4.49/7. Moreover, it has confused banks on how to deal with insider attacks with an average of 4.94/7.

4.3.5 Significance path of the Questionnaire

Looking at the above analysis, and using the above data, the researcher has used smartPLS (SEM software) described in the previous section to come up with the following significant model.

Fig 15: Significant path for quantitative analysis
The above model introduces three hypotheses that will be discussed in the discussion chapter:

- Due to the absence of cyber law, banks are acting poorly regarding cybersecurity, and thus, this is motivating criminals in their endeavor.
- Due to the absence of cyber law and banks poor performance, motivated attackers are increasing the breaches in banks.
- Increased breaches in banks are impacting the poor performance of the economy.


CHAPTER V

DISCUSSION AND CONCLUSION

5.1 Discussion

The purpose of this study was to explore the current implemented anti-cybercrime procedure in Lebanon within the absence of cyber laws and digital forensic procedures, and identify the gap and the reasons behind it. This study also aims to explore how the absence of cyber laws is affecting the cyber-crime cases in Lebanon and how it is affecting Lebanese organizations and the economy.

To achieve this purpose, a total of six interviews were conducted with the Lebanese Internal Security Forces and Lebanese judges. In addition, a questionnaire was distributed to four Lebanese banks where the sampling reached out to all cybersecurity divisions in the banks, and few other retail divisions. Hence, a total of 96 questionnaire responses, and six interview responses were collected for the purpose of this study. Using results from the collected and analyzed data, the three research questions will be answered and discussed in this chapter. Limitations, conclusions, and implications are also presented in this chapter.

5.2 The Current Implemented Framework by I.S.F to Combat Cybercrime

The responses to the interview questions with the I.S.F member and with the Lebanese judges revealed the current implemented framework along with the trainings,
capabilities, policies, and procedures undertaken by the I.S.F to carry on a cybercrime and digital forensic investigations. Thus, the below sections will highlight the current implemented framework in Lebanon.

**5.2.1 Reasons to start a cybercrime investigation.** Taking the fact that there is no cyber law in Lebanon into consideration, the results of this study indicated that there are two reasons for the I.S.F to start a cybercrime and digital forensic investigation. One reason is a victim reporting a cybercrime case to the I.S.F or to the Lebanese courts (100%). The other reason is a memo from the Lebanese courts that is issued by a Lebanese judge (16%). It is noteworthy to point out that 80% of the judges interviewed have also stated that no action can be taken if a case was not reported.

The two hypotheses look similar to the suggested worldwide frameworks where the first step of cybercrime and digital forensic investigations is the “pre-process”. The pre-process phase suggests that the first thing an investigator needs to perform is to identify a cybercrime, get all the paperwork done, and get all the approvals needed to start a cybercrime investigation (Oluwasegun, David, Esther, Victor, 2014). However, there are few questions that need to be answered in order to implement a successful pre-process phase. These questions are: What is defined as a cybercrime? On what basis should a certain action be classified as a crime? Do cyber laws define what is an acceptable act and what is prohibited one? (Lessig, 1999). Moreover, without cyber laws, will there be no mean to identify if an act is considered a crime that requires a cybercrime investigation? (Lessig, 1995).

**5.2.2 Cybercrime and Intellectual Property Office Investigation.** Assuming that a certain action was considered as a cybercrime, and all the paperwork and approvals were
issued, it is now the responsibility of the Cybercrime and Intellectual Property Office to start an investigation. Based on the interview with the I.S.F member, the Cybercrime and Intellectual Property office is registered and protected by law since 2006, and is divided into two teams: investigators and digital forensics Lab team. This allows the transition to the second phase of the discussed international framework which is the “Acquisition & Preservation” phase. According to Oluwasegun, David, Esther, and Victor, this phase requires identifying, collecting, transporting, storing, and preserving captured data and should be done through certain procedures that are drafted, published, and enforced by the law for the evidence to be admissible. Also, based on the interview with the I.S.F member, the I.S.F already follows a set of standards while performing a digital forensics investigation. However, these steps and procedures are not mentioned in the law yet; hence the procedures are not enforced and are not taken into consideration by the judges to confirm the admissibility of the evidence.

5.2.3 Analysis of the collected data through cybercrime investigations. Once the data is collected, it is then ready to be analyzed. This leads to the third process of the digital forensic investigation model shown in figure 2. Oluwasegun, David, Esther, and Victor suggest that this phase is where the analysis of the data is done, and it starts when the investigator needs to connect the dots to come up with admissible evidence. However, in order for the investigators to perform the analysis, they need to acquire certain skills that are associated with digital forensic readiness (Dardick, Endicott-Popovsky, Gladyshev, Kemmerich, & Rudolph, 2014). Given that training opportunities increase the technical skills for investigators and help them in detecting and analyzing cybercrime (Tu, Xu, Wira, Balan, & Cronin, 2012), the I.S.F member has confirmed that the team in the I.S.F
is ready to analyze the data as they are sending their employees to regular training sessions. He also added that some of the employees are even being registered in cybersecurity and digital forensic courses to empower their knowledge and their experience as they are using both special licensed software and open source software. This gives the I.S.F a solid base to analyze the data from the preserved systems in order to collect evidence that can tie a suspect to a cybercrime.

5.2.4 Presenting digital evidence to the Lebanese Courts. Once all evidence is extracted and is written in a well readable documented format, the evidence is returned to the courts for the data to be presented to the judges. This starts the fourth phase in Oluwasegun et al. model which is the “presentation phase”. The presentation phase should be a simple phase were the judge receives all digital evidence from the I.S.F with a full report on how the evidence was preserved and extracted, and how the evidence is significant to the case allowing the judge to give a fair judgment. However, within the absence of cyber laws, digital forensic procedures judges become obliged to seek external assistance to better understand the digital evidence submitted. The responses collected from the judges through the interview questions revealed that 60% of judges interviewed are hiring digital forensic specialists to better understand the evidence, while 20% of the judges are seeking assistance from technical people, and the remaining 20% are going back to the I.S.F for further assistance.

5.2.5 Post-Process, awareness, and media. The final step after presenting digital evidence to the courts and making a judgement call on the cybercrime case is the Post-Process phase that the model presents. The Post-process phase is where all seized devices are returned to their owners, and where awareness about cybercrime is spread to all
people through all available channels and media. The responses collected from the I.S.F member revealed that all communications between the Cybercrime and Intellectual Property office and between people should be passed through the Public Relation division in the I.S.F. The I.S.F member has confirmed that they are already performing regular awareness sessions through universities, schools, Lebanese media (television and radio) and through different social media such as Twitter and Facebook.

5.3 Flaws in the Current Implemented Framework, Reasons Behind it, and its Effect on the Current Cybercrime Cases

Looking at the above discussion and comparing it to the international known framework for digital forensic investigations suggests that the flaws in the current implemented framework lies in the Pre-process phase where there is no cyber law to define a crime and its punishment, in the Acquisition and Preservation Phase where there is no digital forensic procedure to acquire and preserve digital evidence, and in the Presentation phase where judges are not following up on digital evidence. The responses to the interviews that were conducted with the Lebanese judges have revealed the reasons behind the three mentioned flaws, and their effect on the current cybercrime cases in the Lebanese courts.

5.3.1 The reasons behind the delay to draft and implement cyber laws and digital forensic procedures. While the absence of cyber laws and digital forensic procedures was identified as a flaw in the current Lebanese implemented framework, the responses of the judges to the interview questions have revealed that there are three reasons behind the delay of the implementation: lack of public awareness, lack of politicians’ awareness,
and political conflicts. 60% of the judges believe that politicians are not aware of the importance of the cyber world and the means needed for protection from attacks. 40% of the Judges also believe that the lack of awareness for both people and politicians is one main reason for the delay in the implementation of cyber laws and digital forensic procedures.

The judges and the I.S.F member have also noted that a draft was already submitted to the Lebanese Parliament since 2005 (60%) that included a digital forensic procedure (60%), and that included articles related to e-commerce, privacy issues, and the definition of a cybercrime (40%), but due to political conflicts regarding the drafts, these laws never came to life (60%). Mr. Abdul Hafiz Mansour (secretary of the special investigation commission) has even confirmed through one of the articles that the drafts have been on hold for over 16 years. Hence, the lack of awareness about the importance of cybercrime and its laws, and political conflicts are the reason behind the delay in the implementation of a cyber law and digital forensic procedures.

5.3.2 The reasons leading to lack of knowledge within Lebanese judges regarding cybercrime. Bhargav et al. have defined cyber law as a legal system that defines the digital world and its components, and hence increasing the knowledge about the subject is a necessity. Looking deeper into the reasons behind the lack of knowledge within Lebanese judges regarding cybercrime, reveals that the absence of cyber laws is negatively impacting their technical skills(60%), training opportunities (20%), and their awareness about the subject (20%) which then impacts their knowledge about cybercrime (80%).
The judges have also mentioned that they lack knowledge about the subject as cyber law was not given as a core requirement in universities as it is not a component of the Lebanese law (20%). 60% of the judges have agreed that if a cyber law was included through the Lebanese law enforcement, it would be obligatory to teach cyber laws in universities which in return would increase their knowledge about the subject. Hence, lack of knowledge within Lebanese judges results from the absence of cyber laws, and from the lack of education on the subject.

5.3.3 The impact resulting from the absence of cyber laws, and the lack of knowledge on current cybercrime cases. The responses collected from the judges through the interview questions have resulted in four hypotheses that explain the impact resulting from the absence of cyber laws on current cybercrime cases:

- The absence of cyber laws is leading to misjudgment on cases
- The absence of cyber laws and the lack of knowledge is leading to the loss/miss of digital evidence
- The absence of cyber laws is leading to the denial of cases in Lebanese courts.

Through one of his interventions, Dr. El-chaer has argued that there is neither a crime nor a punishment without a law, and he has given examples of how the absence of cyber laws has led to misjudgments and false accusations. He also highlighted that judges are putting personal efforts to map the current normal convictional law to cybercrime. However, the question that needs to be asked here is whether or not the normal convictional law would cover all aspects of cybercrime? 80% of judges have responded that the absence of a cyber law is leading to the inability to map all cybercrime cases to the current convictional law which is leading to misjudgments on the current cybercrime
cases. 60% of the judges have responded that mapping the current convictional law to cybercrime does not give a fair judgement at all.

Carrier and Spafford suggested that Digital forensic completes cyber laws by setting a clear procedure to be followed in order not to miss or taint any digital evidence (2004). On the other hand, Nawafleh et al. suggested that there are two pre-requisites that need to be taken into consideration before making a fair judgement that covers all digital evidence: cyber laws and knowledge of the topic (2016). 80% of the judges’ responses that were collected through the interview questions revealed that due to the absence of cyber laws and digital forensic procedures, vital digital evidence is lost. 80% of the judges also stated that some digital evidence is being also missed out in a cybercrime case which is leading sometimes to fault accusations and misjudgments.

The last hypothesis in this section stresses the absence of cyber laws which leadis to the acceptance of all digital evidence regardless of its admissibility. Oluwasegun et al. stated that digital evidence should be believable and reliable to the jury and the judges in a way that the court should not have any doubts or questions on how the evidence was collected. However, in previous discussions, the fact that judges are seeking external assistance to understand digital evidence and confirm its admissibility has been highlighted. All judges have confirmed through their responses to the interview questions that there is no special criteria to deny any digital evidence, while only 20% of the judges have stated that the judge has the right to ask for clarifications though the case is till counted as admissible evidence.
5.4 The Absence of Cyber Laws effect on The Lebanese Economy and on Organizations, and The Significance of Adding These Laws

Discussing the current implemented framework for combating cybercrime, highlighting its flaws, identifying the gap resulting from the flaws between the I.S.F and the Lebanese courts and studying its effect on the current cybercrime cases (assuming that the Lebanese banks represent a huge chunk of the Lebanese economy) was necessary and could only be done through interview questions and questionnaires that targeted the Lebanese banking sector. The collected responses open the gate to the following section which will zoom into cybercrime, and will study how the absence of cyber law is affecting the performance of the Lebanese banks, increasing the motivation of attackers, and impacting the Lebanese economy.

5.4.1 Information security performance within the absence of cyber laws. The responses collected from the questionnaire reveals that 80% of the respondents agree that the Lebanese banking sector has moved towards online banking where the banks are performing online transfers, online bill pay, online deposit, ATM cash withdrawals, and are offering credit card services. The latter puts the banking sector in the aim of cyber attackers, and hence proves that the absence of cyber laws is affecting information security negatively in banks which in turn is motivating attackers in their endeavor. Previous studies have shown that banks are under the risk of being attacked by hacktivist groups on daily basis. And as per the data collected, 72% have agreed that the absence of cyber laws is one of the main reasons for not reporting cybercrime cases in the banks to the I.S.F, while 64% agree that it is demotivating banks to perform cyber security trainings hence confusing banks on how to deal with insider attacks. The interview with
the I.S.F member has also shown that only 10% of the cybercrime cases that they deal with are related to email scams, while 90% of the cybercrime cases are not being reported.

5.4.2 Motivation of attackers, and increase in the number of breaches. Hackers are usually individuals who perform cyber-attacks because they either have the knowledge to do so, are challenged to do so, they want to perform a malicious activity such as stealing money (Voiskounsky & Smyslova, 2003), or even hack into computer systems as a mean of exploration and having fun (Andress & Winterfield, 2013). Within the absence of cyber laws, the digital world would have no limit, and would motivate attackers to have fun (Lessig, 1995). The data collected for this study has revealed that the 82% of the respondents agree that the absence of cyber laws and the banks poor performance discussed above is motivating attackers to perform identity theft and email scam attacks, while 81% have agreed that it is motivating attackers to perform ATM frauds and unauthorized withdrawals. The secretary of the special investigation in Lebanon have even confirmed that cyber attackers have succeeded to transfer money to their accounts through 84 online fraudulent transactions that were not even reported to the I.S.F.

5.4.3 The relationship between the breaches in banks and the economy. The responses collected have revealed that due to the absence of cyber laws, 79% of the respondents have agreed that the Lebanese banking sector is witnessing online money laundering, while 76% agreed on the online banking crime and identity theft. Within the rising number of breaches to the bank, and according to previous research, when the victim of a cyber-attack is a financial service firm (which in our case is the banking sector), the economic consequence can be a very serious one.
5.4.4 The Importance and significance of adding cyber laws and digital forensic procedures.

The significance of adding cyber laws and digital forensic procedures lies in hindering the highlighted gaps mentioned previously, and introducing a new kind of protection for the digital world. While digital forensic readiness stresses on knowledge and experience, introducing a cyber law would fulfil those requirements allowing our country to be ready for cybercrime investigations. And as presented in the results chapter previously, both the judges and the I.S.F agree that introducing cyber laws would increase their knowledge and improve their skills. 13% of the judges believe that introducing a cyber law would limit the number of cybercrimes while our society is already under cyber and privacy attacks.

As laws define what is prohibited and what is accepted, it is vital to implement a cyber law since as said by 13% of the judges, it would give them a definition of cybercrime and would instruct them to export, document, and present digital evidence the right way to be readable by all judges. Universities would also be obliged to offer cybercrime courses as core requirement to the law school increasing the training opportunities and the knowledge base.

5.5 Conclusion, Recommendations, Implications and Limitations

5.5.1 Conclusion

Cyber laws control and define what is right and what is wrong in the digital world. They are the means that judges refer to when ruling out on a cybercriminal case to determine who the suspect is and who is the victim, and to determine the punishment resulting from
a criminal act. Digital forensics on the other hand compliments cyber laws. It is the science that directs investigators on how to extract data without tainting, losing, or missing digital evidence in a crime scene (Lessig, 1995). The interviewed Lebanese judges and the I.S.F member were knowledgeable about the subject. They all believe that it is very important in our days to implement a cyber law and a digital forensic procedure as the whole country is evolving towards the digital world. The statements “can’t confirm admissibility of evidence” and “the absence of cyber law and digital forensic procedures” were highly used in all interviews.

The results of this study have indicated the current framework that is being applied in Lebanon to chase cybercrime cases, and have highlighted what are the current flaws that is causing a gap between the courts and the Lebanese I.S.F. In addition, this study has revealed how the absence of cyber laws and digital forensic procedures affecting the current cybercrime cases, organizations, and the economy of Lebanon.

5.5.2 Recommendations

It is recommended that more studies be done on the current implemented framework to chase cybercrime however on a bigger scale to explore further the strategies, policies, and procedures undertaken to solve a cybercrime. The recommendation would be to collect further data on the chain of cybercrime within the I.S.F Cybercrime and Intellectual property Bureau office, and to explore other divisions that deal with such cases such as the information technology division.

It is possible to fine tune the current highlighted gaps between the I.S.F and the Lebanese judges for the time being, but as Lebanon is moving towards the digital world, were the government would be evolving to an e-government, and elections would
transform into an online one, and where e-banking and e-commerce is spreading across the Lebanese people, it is mandatory to implement a cyber law and a digital forensic procedure in order to protect the Lebanese organizations, people, and economy.

In terms of knowledge, it is recommended to increase awareness sessions that would reach out all Lebanese people and organizations. Our current world relies vastly on information, and protecting information should be a priority to all people including politicians, judges, the government, and company owners. In addition, the increase of training opportunities to judges and to I.S.F member is a must as it exposes them to different scenarios that can happen in real life and increases their experience.

**5.5.3 Implications and Limitations**

In this study, we have explored the current implemented framework to chase cybercrime in the Cybercrime and Intellectual Property office; however, the researchers had a limitation where they were only approved to interview one I.S.F member from the Cybercrime and Intellectual Property office due to time constraint and to internal conflict constraints. Perhaps further studies would have the ability to look further into this subject and to collect a bigger data that would help understand the framework better.

The researchers were able also to explore the gap between the Lebanese judges and the I.S.F members through interviews with Lebanese judges; however, the researchers had a limitation where only five judges were interviewed due to the lack of judges that are knowledgeable about cybercrime and deal with it. Perhaps by the time further studies on this subject are explored, the number of judges that deals would cybercrime would have increased.
Another limitation is that the data collected from the banks was only conducted within four banks resulting in 96 responses which do not represent all the banks in Lebanon. It would definitely be better to include more banks for better representations.
References


Has the SIC in Lebanon been hacked? If so, by whom? (2017), retrieved from http://blog.tarekchemaly.com/2017/11/has-sic-in-lebanon-been-hacked-if-so-by.html


PwC.(2018). Pulling fraud out of the shadows. The biggest competitor you didn’t know you had. Global Economic Crime and Fraud Survey 2018, 8


Appendix A: Interview Questions with I.S.F

1- Is digital forensics enforced through the Lebanese Law?
   a. Is it possible to get a copy of the law?
   b. Usually a digital forensics investigation passes through four phases: Pre-Process, acquisition & preservation of evidence, analysis of evidence, presentation of evidence, and post-process. Does the I.S.F use the same framework for cyber investigations? What are the procedures and the steps that the I.S.F follow through each phase? Appreciate if you can provide me with documents related to this question.
   c. Are the judges informed about these laws? And are they aware of the importance of digital forensics and the latest cyber-attacks.
   d. To what extent is digital forensics law adopted by the judges?
   e. Is there any framework to be followed when performing a digital forensics investigation? For example, does the procedure of a digital forensics investigation differ when used internally then when used with other countries? (I would appreciate it if you can provide me with documents related to this question.)
   f. Does the I.S.F have the right to seize any digital device at any time using a search warrant?
   g. Are there any political limitations that are affecting digital forensics investigations?

2- Does the I.S.F use any digital forensics tools or software to investigate cyber-crimes?
   a. If yes, when does the I.S.F decide to use these tools? Which criminal activities require digital forensic tools, and who is responsible to decide whether or not these tools are to be used.
   b. Are the assigned personnel trained to use digital forensic tools?
   c. Does the I.S.F send employees to professional trainings on regular basis?

3- Do you think that Lebanese people are aware of cyber security and cyber-attacks?
   a. Does the I.S.F have any official surveys or statistics that can be provided? (I would appreciate it if you can provide me with documents related to this question.)
   b. How does the I.S.F make sure that the Lebanese people are always updated with the latest news and latest attacks?
   c. Are there any future plans to spread cyber security awareness?
4- Media plays a big role in spreading cyber security awareness. Is media in Lebanon putting any effort to spread security awareness? Or is it just being ignored?
   a. Why isn’t media shedding light on cyber security attacks? Are there any policies that oblige media to inform people about cyber security attacks?
   b. Other than media, who do you think is responsible to shed light on cyber-attacks and cyber security?

5- Are the Lebanese people ready to adopt a digital forensics law or a cyber security law?
   a. What is the current level of adoption of digital forensics law for the Lebanese people?
   b. What are the limitations that prevent a strong digital forensics law from being implemented?
   c. To what extent are people ready to adopt to new laws and to cyber security laws?

6- On July 7 2017, Lebanese people were aware through media that the internal security forces website (I.S.F website) was hacked. What measures did the I.S.F undertake in order to prevent such attacks from happening again?
   a. Were any digital forensics tools used in order to locate the source of the attack?
      i. Was this the first cyber security attack that targets the I.S.F? If no, why weren’t previous attacks exposed to the media?
      ii. Was the I.S.F able to locate the source of the attack and to identify the attacker?
         1. If yes, does the I.S.F have the rights by the law to arrest the attackers if discovered through digital forensics software?
         iii. Was the I.S.F able to gather any information related to the attack?
         iv. What vulnerability did the attackers use in order to exploit the system?

7- 3 days before the I.S.F website got hacked, the official Lebanese television (Tele Liban) was under attack by the same hacktivist group that attacked the I.S.F website. Do you think that the attacks were related?
   a. Knowing that Tele Liban is a governmental media channel, did the I.S.F assist Tele Liban with their experience to track the attackers and to ensure that such attacks won’t happen again?
   b. Was there any digital forensics investigations performed?
      i. If yes, what steps were taken by the I.S.F to start the investigation?
      ii. Were there any search warrants issued in order to start the digital forensics investigation?
1. If not, do you think that if a digital forensic law was enforced and was in place the I.S.F would have identified the attackers and would have prevented the attack on the Lebanese I.S.F website?

8- I am aware that the Central Bank of Lebanon forces all the local banks to have an Information Security division that specializes in protecting the bank’s digital assets and that ensures business continuity despite all kind of cyber-attacks. Are the I.S.F involved in any cyber-crime that takes place in banks?
   a. If not, do you believe that the I.S.F should be involved in such attacks?
   b. On May 15 2017, the Lebanese Central Bank thwarted a cyber-attack on its email system. Was the I.S.F aware of this attack?
      i. As the Lebanese Central Bank reports to the Lebanese government, did the I.S.F interfere with the cyber investigations?
      ii. Were any digital forensic tools used in order to identify the location, source, and the person or group behind this attack?
      iii. It is known that the Lebanese financial sector is what is keeping Lebanon to stand on its feet. Do you think that enforcing a digital forensic law would help protect Lebanon’s financial sector from cyber-attacks?
      iv. The Lebanese Central Bank (Banque Du Liban) was able to stop the cyber-attack on its email system as it was prepared for such attacks. Do you believe that other local banks (probably smaller banks) would be able to survive such attacks?

9- Lebanon has two official telecommunication companies (Touch and Alfa) to provide the Lebanese people with mobile communication and mobile data usage. Is there any coordination between these companies and the I.S.F?
   a. If yes, does the I.S.F have the rights to collect information from those companies through a criminal investigation? Hence, does the I.S.F need a search warrant or any official document to gather the needed information for a criminal investigation?
   b. In case of any criminal activity, is the I.S.F requesting from those companies to reveal recorded phone calls, text messages, or web requests?
   c. Are there any frameworks or policies implemented that enforces telecommunication companies to abide by the law and rules and to collaborate with I.S.F whenever needed?

10- The I.S.F was able to arrest Ramzi Al-Kadi after he posted several comments through social media (Facebook and Twitter) regarding the attack that happened in Istanbul and lead to the death of several Lebanese people.
a. How does the I.S.F differentiate between privacy and between criminal cyber activities?
b. How was the digital forensics investigation conducted?
c. How did the I.S.F make sure that the comments and posts were actually written by Ramzi Al-Kadi and not by any other hacker?
d. What laws did the I.S.F use in order to arrest Ramzi Al-Kadi?

11- The I.S.F was able to stop the “Number Plate” application that was available on App store and on Google Play Store. The application revealed car plate numbers with owners information to the public.
   a. How was the I.S.F able to block such an application?
   b. How was the I.S.F able to track the owner of the application?
   c. How did the owner of the application get access to all the confidential data?

12- Was a draft given to the Lebanese Parliament in order to enforce cyber-security and digital forensic
   a. If yes, was the draft voted upon to integrate digital forensics with the Lebanese law enforcement.
   b. Do you believe that the draft/law is now outdated and needs to be modified?

When did the I.S.F include a Cybercrime and Intellectual Property division through its structure?
Appendix B: Interview Questions Targeting Lebanese Judges

1- Have you ever ruled out on a case that required digital forensic investigation and digital evidence?
   a. How did you confirm that the digital evidence was admissible and was not tainted before being presented?
   b. Clarify any difficulties faced while applying/binding a cybercrime case to a Lebanese law?
   c. What suggestions would you recommend to overcome the difficulties that Lebanese judges face while working with cybercrimes and with digital forensic investigations.

2- Do you think that there is a gap of knowledge between the Internal Security Forces and the Lebanese judges in accordance to cybercrime?
   a. In case the answer was yes: what are the reasons behind this gap? And what do you think is the best solution to unify judges and I.S.F efforts to come out with a fair judgment
      i. How is this gap affecting cybercrime cases handled at courts.
   b. In case the answer was no: what recommendations would you suggest to increase coordination between I.S.F and Lebanese judges.

3- Within the past 5 years, did you notice any change in the number of cybercrime cases?
   a. What do you think is the reason behind this change(whether they increased or decreased)
   b. How do you think that the implementation of a cyber security law would limit the number of cyber-criminal cases
   c. How would the implementation of a digital forensic procedure help the Lebanese judges in understanding digital evidence, and pertaining its integrity.

4- Have you denied any cyber security related case requested from I.S.F?
   a. What are three reasons to deny a cyber security request from I.S.F?
   b. On what criteria do judges approve cyber security requests coming from I.S.F

5- Why do you think Lebanon does not have yet a cybersecurity law
Appendix C: Questionnaire Targeting Lebanese Banks

Gender: …………………

Age:………………

1) Profession Level: O Strategic Level Management O Middle Level Management O Operational

2) How would you describe your knowledge of Cyber Security and Cyber-Crimes in Banking:
   O Not at all O Somewhat O Knowledgeable O Very Knowledgeable

3) E-Banking Services On a scale of 1-7, 1 being the least and 7 being the most provided service, please indicate which E-banking services are currently provided 1

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Online inquiry and transfers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Online bill-pay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Online deposit accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Wire transfers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Online banking demo (e.g., customer assistance, personal service over the telephone, e-mail)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. ATM cash withdrawals/deposit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Credit Card Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4) Please indicate by marking in the appropriate box how much you agree or disagree with the following statements about Cyber Crime in your banking institution

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I am aware that my bank has experienced online banking related crime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. I am aware that my bank has experienced cases of identity theft (Phishing)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. I am aware that my bank has experienced cases of ATM fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. I am aware that my bank has experienced cases of money laundering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. I am aware that my bank has experienced cases of email scam related remittances.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. I am aware that my bank has experienced unauthorized</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1=Strongly Disagree; 2=Disagree; 3=Somewhat Disagree; 4=Neutral; 5=Somewhat Agree; 6=Agree; 7=Strongly Agree</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1. I am aware that other Lebanese banks has experienced online banking related crime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. I am aware that other Lebanese banks have experienced cases of identity theft (Phishing)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. I am aware that other Lebanese banks have experienced cases of ATM fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. I am aware that other Lebanese banks have experienced cases of money laundering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. I am aware that other Lebanese banks have experienced cases of email scam related remittances.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. I am aware that other Lebanese banks has experienced unauthorized withdrawals from customers account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1=Strongly Disagree; 2=Disagree; 3=Somewhat Disagree; 4=Neutral; 5=Somewhat Agree; 6=Agree; 7=Strongly Agree</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The absence of cybersecurity laws is motivating attackers to perform identity theft crimes (phishing)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. The absence of cybersecurity laws is motivating attackers to perform ATM frauds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. The absence of cybersecurity laws is motivating attackers to perform email scam related remittances</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. The absence of cybersecurity laws is motivating attackers to perform unauthorized withdrawals from customers account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1=Strongly Disagree; 2=Disagree; 3=Somewhat Disagree; 4=Neutral; 5=Somewhat Agree; 6=Agree; 7=Strongly Agree</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The absence of cybersecurity laws is not motivating banks to perform technical cybersecurity trainings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. The absence of cybersecurity laws is a main reason for not reporting cyber security cases to I.S.F and to the courts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. The absence of cybersecurity laws confuses banks on how to deal with insider attackers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>