Impact of Cybercrime in Saudi Arabia

Abstract

The use of the internet is increasing drastically, and as a result, the threat is also increasing drastically. Cybercrime across the globe has become a major phenomenon with difficulty in its prevention and reduction, together with the increasing vulnerability of the different kinds of internet users. Saudi Arabia has become the number one target of cybercrime in the Middle East (Elnaim, 2013). This points to the risky nature of Saudi cyberspace with end-users at the receiving end of most of these crimes. This research aims at understanding the various means through which cybercrime affects end-users in Saudi Arabia. Moreover, the aim also includes providing valuable recommendations to minimise the exposure and effect to the different types of cyber crimes.

From the primary research conducted in this research, it is clear that people that use the internet in Saudi Arabia are not aware of the types of cybercrime that they can get exposed to and what impact it will cause personally, and financially. Also, it is possible to say that the Saudi Arabian government is taking steps to reduce the impact as well as reduce the exposure to cybercrime. However, the results from the steps are low because the end-users of the Internet in Saudi Arabia are not following the security precautions. The most common type of cybercrime in Saudi Arabia identified from the secondary and primary research are an online commission of intellectual property crimes, child pornography and sex trafficking, online theft, hacking, and types of malicious codes.

(Word count 252).

Table of Contents

List of tables

List of Figures

Chapter 1: Introduction

Cybercrime worldwide has become a significant phenomenon with difficulty in its prevention and reduction, together with the increasing vulnerability of the various internet users. Saudi Arabia is now the major target of cybercrime in the Middle East (Elnaim, 2013). This indicates the vulnerability of the cyberspace of Saudi Arabia and the end-users are the main victims of such crimes.

It is difficult to have a single definition of cybercrime across the globe (El-Guindy, 2013). This has made it necessary to select a definition that suits the context of this paper. The preferred definition used by this report was provided by Halder and Jaishankar (2011). Cybercrime was presented as any offence committed against individuals or against people based on a motive that is criminal to harm the reputation, physical and mental wellbeing of the victim intentionally with the use of modern telecommunication, especially the internet and mobile phones. This definition provides an end-user focus with the harmful impact highly emphasised. Cybercrime is an offence against the availability, confidentiality and integrity of computer data and systems (Algarni, 2012).

The internet has become the bedrock for businesses globally with the advancement in the commercialisation of world wide web. The advancement in web technology has made businesses across the globe to explore its opportunities as well as its effects. The high rate of internet breach in the Gulf region is evidence of the revolution of business transactions and the economy of its nations (Salazar & Low, 2011). Despite the appreciable increase in internet-based commercial transactions, the corresponding rise in online fraud and other crimes cannot be understated. Deloitte (2011) stated that millions of money had been lost to unlawful practices.

1.1. Research aim and Objectives

Aim

This research aims at understanding the various means through which cybercrime affect end-users in Saudi Arabia and provide a recommendation to minimise the cybercrime threat.

Objectives

Objective 1: To perform secondary research to identify what are the types of cybercrimes, the impact of cybercrime in Saudi Arabia, Laws and policies that govern the people in Saudi Arabia.

Objective 2: To perform primary research which includes interview and survey to study the people’s opinion regarding cybercrime and its impact.

Objective 3: To perform primary research to identify the steps the people in Saudi Arabia take in order to minimise or avoid the cybercrime threat.

Objective 4: To provide valuable recommendations to people in Saudi Arabia in order to minimise the impact of cybercrime as well as to reduce the exposure to cybercrime.

1.2. Research questions

The mapping of research questions with the project objectives is provided in table 1.

Table 1: Mapping of Research questions with the project objectives

Objectives	**Research questions**
To perform secondary research to identify the types of cybercrimes and their impacts in Saudi Arabia. Furthermore, to identify the laws and policies that govern the people in Saudi Arabia.	1. What are the types of Cybercrime available? 2. What are the laws that govern the cybercrime issues in Saudi Arabia? 3. What are the identified impacts of cybercrime in literature?
To perform primary research which includes interview and survey to study the people's opinion regarding cybercrime and its impact.	4. What kind of impacts does the Saudi Arabian end-users experience? 5. What is the opinion of cybercrime on internet users in Saudi Arabia?
To perform primary research to identify the steps the people in Saudi Arabia take in order to minimise or avoid the cybercrime threat.	6. What is the level of cybercrime perpetration regarding technology and targets in Saudi Arabia? 7. What is the level of vulnerability of end-users to cybercrime in Saudi Arabia?
To provide valuable recommendations to people in Saudi Arabia in order to minimise the impact of cybercrime as well as to reduce the exposure to cybercrime.	8. What are the recommendations to minimise the exposure to cybercrime? 9. What are the recommendations to minimise the impact of cybercrime?

The research question and the justification for the selection of the specific questions are provided in Appendix C.

1.3. Research Justification

Cybercrime has been researched extensively in Saudi Arabia. Three core researchers that explored this topic include Algarni (2013), Elnaim (2013) and Khan (2012). The argument from the three papers is about awareness and vulnerability of Saudis, types and sophistication of crime, and the impact on end-users. Both Algarni (2013) and Khan (2012) affirmed the financial impact as a major factor in KSA despite the notable prohibition of crime statistics publication. This emphasis stems from the financial losses that are in millions of pounds.

However, Elnaim (2013) maintained that there is increasing sophistication in this type of crime portraying variation in perpetration and outcome. The emphasis on target and impact was another area of interest with individual end-users and business (or government infrastructure) end-user forming the basis for comparative analysis. It was established that the Saudi cyberspace is highly vulnerable thereby aiding the different types of crime. This resulted in an argument that Saudi does not have the monopoly of vulnerability because other countries have more level of vulnerability.

Other researchers such as AlKahtani (2015) and Almerdas (2014) reviewed the Saudi Anti-Cybercrime law while Alanezi (2015) researched the impact that perceptions of online fraud on the countermeasures in Saudi Arabia. These researches have focused on just one aspect of cybercrime, even though there is a need to investigate the entire cybercrime industry. The focus on the end-user is vital to determine the depth of the social awareness and the effect being felt from cybercrime. This research is imperative to provide an up to date insight into the current situation of the cybercrime industry alongside with the direct interference with the end-user.

1.4. Report Structure

The complete details regarding this report structure are provided in table 2.

Table 2: Report Structure

Chapters	Content Brief
Literature Review	This chapter provides the information from the existing literature. Moreover, the information received from the existing literature are critically analysed.

Research Methodology	This chapter provides the necessary details regarding the data collected; the approached used to collect data and how the data are analysed.
Data Analysis	This chapter provides the survey and interviews analysis.
Discussion and Recommendation	This chapter provides detailed information regarding the overall discussion regarding the research conducted and provide appropriate recommendations to reduce the impact of cybercrime and the exposure to the cybercrime in Saudi Arabia.
Conclusion and Future work	This is the last chapter of the project which provides, the conclusion, future works, risk table and the Gantt chart.

Chapter 2: Literature Review

2.1. Introduction

This chapter provides the basic background information regarding the cybercrime in Saudi Arabia using the existing literature.

2.2. Cybercrime

Cybercrime is a global problem, and no country is immune. In recent years, the Middle East has witnessed rapid growth in Internet connectivity together with similar cybercriminal activities (El-Guindy, 2008). Rapid advancement in telecommunications witnessed from the end of 20th century and early 21st century have enhanced the use of the internet with corresponding cybercrime attached.

The concept of cybercrime despite being committed using a computer in most cases are being referred to as computer crime. Khan (2012) depicted cyber-related crime (such as Hacking, Software Piracy, Denial of Service Attack, Pornography and website defacement) to be a computer crime. This confusion provided the basis for the enlarged scope of this type of crime thereby making the carving of impact to be difficult. It is difficult to define cybercrime as well as its impact based on the different perspective and nature of the crimes (Yar, 2014). Redford (2011) agreed that there are various mediums of perpetuating the crime. The use of mobile phones and other devices in cybercrime reduce the validity and acceptability of the computer crime definition.

However, the use of other devices in cybercrime has formally negated the proposition of these types of crime to be strictly computer crime. Gunjan, Kumar and Avdhanam (2013) identified laptops, PDA, Watches, PDA, Desktop and even vehicles as a communication medium that can be used for cybercrime. The extensive nature of devices for cybercrime perpetration further makes the definition of the scope to be difficult. From the inception of cybercrime, cybercriminals are focused on taking advantage of the internet (Al-Sanea & Al-Daraiseh, 2015). The rise in perpetration and the multifaceted nature points to advancement on the single computer-based scope.

The cyberspace influences every aspect of our daily lives thereby making the prominence of the global reliance on information technology (IT). De Hengst and Warnier (2013) stated that IT is now a critical infrastructure with the communication over the platform becoming more susceptible to breach or attacks. Cybersecurity is now a core security and economic challenge for individuals, governments and private businesses. The global expansion of online businesses and e-commerce has further extended the scope and coverage of these crimes (Redford, 2011). Securing both the data and the service infrastructure in e-commerce is a major challenge.

Cybercrime is often driven by personal gains, irrespective of the inappropriateness of the motive. This type of crime results in the breaching of the norm, civil or criminal order of the internet society for malicious purpose or financial gain (Redford, 2011). The inappropriate gain further fuels the subjectivity claim because it remains difficult to have a generic depiction of what might be regarded as malicious or inappropriate on the internet.

2.2. Types of Cybercrime

In recent times, the simplicity and availability of tools for hacking, together with increasingly dangerous and targeted nature of the crimes, further elaborate the increasing typology (Hassan et al., 2012). Cybercrime can be perceived as to be in different forms thereby making the classification to be difficult. Hassan, Lass and Makinde (2012) classify the crime using the criteria of computer and network to outline the different types of the crime. From the organised crime perspective, Wall (2015) classified the crimes in a way that is different from others. Anderson et al. (2011) in research discovered about 14 types of cybercrime. Holt and Bossler (2014) further provided a classification that emphasises on broad typology. With the focus on the target of the crimes, several authors provided classifications for the cybercrime which are provided in table 3.

Table 3: classifications for the cybercrime from different literature

Author	Classification
Hassan et al. (2012)	• Cyber Terrorism • Cyberterrorism, identity theft • spam • Cyber Stalking • Drug Trafficking • Malware • Password Sniffing • Logic Bombs
Wall (2015)	• Carding and ID theft Operations • Botnet operations

	• Cybercrime Hubs • Spammer Operations • Malware Development and Distribution Specialists • Auction fraud - • Hackers/hacktivist • Scammers
Anderson et al. (2011)	• Online payment card fraud • Online Banking Fraud • In-person payment card fraud • Fake Anti-virus • Infringing pharmaceuticals • Copyright-infringing software • Copyright-infringing music and video • ‘Stranded traveller’ scams • ‘Fake escrow’ scams • Advanced Fee Fraud • PABX Fraud • Industrial cyber-espionage and extortion • Fiscal Fraud • Other Commercial Fraud
Holt and Bossler (2014)	• Cyber-trespass • Cyber-deception/theft • Cyberporn and obscenity • Cyber violence.
Neufield (2012)	• Crime against Persons • Crime against Property • Crime against Society

The existence of numerous classifications that are influenced by perspective and professional perspective continue to make it difficult to agree on a concise typology of the crimes. From the various classification, twelve itemised cybercrimes can be derived. These crimes have different names but imply similar meanings.

- **Crimes of data infringement:** This type of crime is the illegal use of information or any data. Yar (2014) noted that cybercriminals often gain access to data illegally and use it for purposes that are not legally permissible. This act, irrespective of the source, often involves the distortion of the entire information thereby altering the integrity in the process. De Hengst and Warnier (2013) noted that the use of programs such as Trojans and Viruses, together with indiscriminate information sharing on social network often results in data infringement. The data is used for the purpose not intended, thereby altering its veracity.
- **Crimes against money:** These types of crime are continually focused on financial gains. It consists of every cyber-related crime that is focused on financial gains. Within the previous classifications, it is often regarded as cyber fraud, theft, or electronic. This classification provided an umbrella for every financial loss related crime in which the victims bear the financial brunt. Anderson et al. (2011) noted that advanced fee fraud in which cybercriminals are after money is a core type of cybercrime.
- **Sexual exploitation of minors:** This is widely known as online pornography or paedophilia. This kind of crime involves individuals or group of persons performing different actions online that sexually exploits minors. Sharing of sexual images of minors online is prominent online together with grooming of minors using applications and websites that operate online (Mishna et al., 2011). This type of crime often preys on these minors and in most cases, can result in cyberstalking or cyberbullying in which the minors become victims. Gilden (2011) associated sexual exploitation of minors as a major characteristic of cyberbullying that has sometimes resulted in the suicide by victims. Simpson (2015) provides another narrative to this crime by highlighting the lack of consent in the distribution of sexual images or content of minors.
- **Crimes against Intellectual Property for Digital Works:** This is a crime that is primarily focused on inappropriate access, usage, duplication and distribution of copyrighted or intellectual property. This is regarded as digital piracy in which digital intellectual property is altered or released illegally. It involves the sale and distribution of intellectual property of an organisation or an individual (Anderson et al., 2011). This property can be software, academic materials, movies or music. An example is the hacking of the Sony studio in November 2014 by the hacker group named "Guardians of Peace" (GOP).
- **Crimes against information systems:** This type of cybercrime is focused on significantly damaging the functioning of the services, infrastructure, access and usage of the cyber-enabled system. There

are numerous ways in which this attack can be conducted. However, Denial of Service (DoS) Attack is a major implementation in this crime. Yar (2014) noted that skilled computer programmers or hackers find a way to bring the network down without necessarily entering the network. This is often done by using bogus traffic to flood the access routers or server of a system. The flooding ensures that legitimate users cannot access the service. In some other crimes, software programmes are used to alter the network until it cannot work again.

- **Crimes affecting personal information:** this type of crime involve stealing, alteration or unauthorised access to personal data. Das and Nayak (2013) explained such personal information to include passwords and social security information together with the modification of such information by an unauthorised party. This negates the communication privacy principle that is important during transit where viewing and modification should not occur. Yar (2014) noted that distributed environments often enable the malicious impact of the third party to be experienced through penetration into the network or devices thereby tampering with or accessing the data during transportation over the network.
- **Crimes of bank cards and electronic money:** This type of crime is focused on manipulating the electronic payments system and the bank cards for fraudulent purposes. Anderson et al. (2011) noted this fraud to be very rampant as card information can be used without the PIN to commit fraud where the customer and the bank share the liability. These crimes might be initiated from the basic form of stealing payment cards, or through the illegal access to customer information through practices such as hacking. Das and Nayak (2013) highlighted that data theft regarding credit card information, enhances this type of crime because they provide the means for which these crimes can be conducted.
- **Misuse of computer hardware or software:** This is a crime that refers to the illegal and inappropriate use of information technology infrastructure. Higgins et al. (2012) noted that the abuse of both hardware and software could result in a crime, especially when privileged information is divulged, or other entities are endangered by such action.
- **Crimes of racism and crimes against humanity using Information:** This is any crime that promotes discrimination and anarchy on the cyberspace. One major example of this crime is cyber terrorism. Anderson et al. (2011) noted that the internet is used to adversely attack other countries in a way that fatal result is derived. For example, the recent ransomware that attacked the National Health Service (NHS) is an example of how critical infrastructure can be terrorised. Holt and Bossler (2012) noted that crime against humanity could be orchestrated on the internet. The spread of hate speech and other information that can promote racism are available on the internet.

- **Crimes against the state and public safety:** This crime is concerned with endangering national security through the endangering of the internal security of nations. For example, a case of crime is being raised against Edward Snowden for misuse of the IT infrastructure to endanger the national security of the United States of America.
- **Crimes of gambling and the promotion of narcotics using information:** The popularity of electronic commerce in the cyberspace have made it become a viable means for which narcotics abuse and gambling-related crime are conducted. Anderson et al. (2011) noted that pharmaceuticals that are fake or not standardised are being sold online thereby endangering consumers. Lavorgna (2014) established that fake pharmaceuticals have the internet as a major medium of distribution. On the other hand, underground and disguised sales of narcotics are present online. An example is the closed down Silk Road website where camouflaged sales of narcotics are being conducted (Seebruck, 2015).
- **Crimes of information encryption:** This is a crime where a service provider or an individual encrypt vital information thereby eliminating access by the authorised user. This can be derived from the encryption practice of viruses and worms when they infect the systems (Manky, 2013). This crime can make files on a system or over a network to be inaccessible through infection or direct attack by cybercriminals.

2.3. Types of Cybercrime in Saudi Arabia

The increasing level of vulnerability has elicited the argument concerning the common types of crime in KSA. Elnaim (2013) emphasised financial fraud and social media related crime. This was substantiated using the Symantec research, which states that in 2012, about 3.6 million consumers were affected by an average loss of £1000 in direct financial losses while about 40 per cent of the social network sites (SNS) users have been cybercrime victims. The end-users were portrayed as highly vulnerable to an increasing number of financial losses. The impact is high demonstrating that financial loss is a major impact for users.

On the other hand, the most significant focus has been attacks against businesses, thereby neglecting the end-user. Khan (2012) argued that cybercrime in KSA could not be limited to fraud or social media related as evidence points to numerous types and nomenclature. This paper pointed to the different types of crime including child pornography, cyber terrorism, identity theft, cyberstalking and hacking. The variation and sophistication of cybercrime in KSA were further corroborated by Al-Kadhi (2011) who emphasised that despite the presence of an anti-spamming policy, the persistence of spam shows sophistication, thereby making it a serious problem in the country. Khan (2012) stated that the understanding of the psychological phenomenon and the internet crime had affected the measurement of their impact on the country.

Bronk and Tikk-Ringas (2013) further established the vulnerability through the detailed analysis of the cyber attack on Saudi Aramco with about 30, 000 machines infected with the self-replicating virus. This established the variation in the types of crimes and advancement in the cybercrime industry of KSA. Another identified pattern is the presence of activities such as Hacking of the Official Website of King Saud University (KSU), and several government Websites in KSA (Elnaim, 2013). It became evident that the type of crime has become highly sophisticated and demonstrating an evolution towards advanced perpetration. For example, A Saudi was arrested at King Khaled International Airport in Riyadh (Arab News, 2015).

2.4. Example of Cybercrimes in Saudi Arabia

A clone virus attacked a computer system in Saudi Aramco on the 15th of August 2012 and contacted over 30,000 of its Windows-based devices (Bronk and Tikk-Ringas, 2013). It took two weeks for Aramco to recoup from the destruction caused by the virus despite the large wealth of Saudi Arabia's national oil and gas organisation, as claimed by a study (Bronk and Tikk-Ringas, 2013). It was shocking that an assault of this magnitude was unleashed on an organisation that is very important to the world energy industry, even though viruses often emerge on the networks of global organisations. The virus resulted in a remarkable interference in the global biggest oil manufacturer and it was later called Shamoon (Bronk and Tikk-Ringas, 2013).

The primary purpose of Shamoon seems to have been the pointless removal of information from computer hard drives (Bronk and Tikk-Ringas, 2013). The attack impacted the operations of the organisation even though the outcome did not cause a severe issue in Aramco business process, explosion or oil spill; it is still possible that a few manufacture and drilling information was missing (Bronk and Tikk-Ringas, 2013). Inclusive of RasGas, Shamoon also diffused to the networks of various gas and oil companies. After a period of caution concerning the danger of cyber-attacks against essential infrastructure, the event took place (Bronk and Tikk-Ringas, 2013).

In Saudi Arabia, there is a national hub for Electronic Security that observes electronic attacks coming from external KSA on some government bodies and services (Al Amro, 2017). Several attacks are intended to render inoperative all servers and to end services that are connected to these servers (Al Amro, 2017). A study by the Saudi Press Agency (A1 Amro, 2017) shows an electronic assault, trying to capture data in the system, inputted malicious software to nullify the user's information comprising of the transport and government sector. The agency comments on its website, that the foundation of this assault originated from outside of Saudi Arabia, with numerous electronic uninterrupted assaults aiming at vital sectors and government agencies (Al Amro, 2017).

The agency drew government agencies and services' attention to a probable risk to facilities for the disabled. Some of the caution given included the necessary data to avert the attack and damage. There are many approaches to safeguard users and methodologies can be used to avert the penalty of the violation. The listed are the finest practices suggested by the PCHR in the safeguarding of electronic systems, most especially concerning the decrease of secluded admittance through VPN ''in the BNP'' (VPN) facilities to admit the Remote Desktop ''RBP'' (RDP). The requirement to pursue excellent practice utilised by companies in different sectors as emphasised by the agency, and the defensive methods that ought to be taken to sustain and safeguard the information and system against likely interference utilising electronic methods.

Additionally, the happenings in the locality influence the safety of the kingdom. In the period of the Saudi-led war against Houthi Militants in Yemen in April 2015, a class of Houthi's faction referred to as ''Yemen Cyber Army'' hijacked the website of a Saudi-financed daily tabloid, exhibiting images of the Hezbollah chief Hassan Nasrallah and inscription in Arabic: '' we have some words to inform you, plan your shelter'' [10]. Similarly, the sect in May assaulted the mail facility of the ministry of foreign affairs, distributing thousands of e-mails which they alleged to be "top secret".

The Saudi Interpol provides the statistic regarding the cybercrime in Saudi Arabia. The most popular type of cybercrime is the E-mail breach which is at 27%, while slander and denigration are at 13%, electronic fraud and deception are at 5%, child sexual mistreatment cases accounted for 14 %, electronic intended spiteful programs 6% and economic violation 12%. The ratio of radical intimidation crosswise sites is 4%, while objection of doubtful connections is not more than 1%, as revealed in Figure 1.

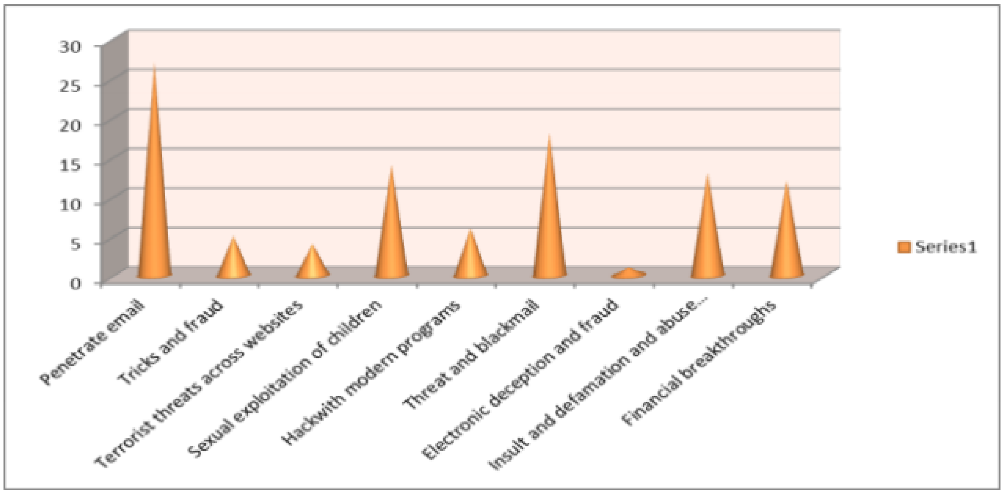


Figure 1: The cybercrime specified by the police of Saudi Arabia (Al Amro, 2017)

In the last ten months of 2016, an overall of 776 instances of digital crimes was dealt with by the KSA courts. The number of crimes of this kind increased in 20016 compared to the previous two years. In 2015, there were around 164 instances in the entire Kingdom and 2016, about 573 instances.

The increase in the number of instances is encouraging, mirroring the population's understanding and the efficiency of the data published on the Ministry of Justice website, including the data on informatics crimes made available by the Interior Ministry. To raise the number of instances of this kind in the ministry of justice indicators, the population's understanding of the necessity of combating IT crimes has proven to be useful. This will structure an upward curve in a strong centre of population, and later turn down after a period, requiring the unrelenting employment of unique necessities in opposition to cybercrime in a bid to dissuade criminals and decrease the number of crimes.

Internet Security Threat Report provided in 2016 by Norton's Symantec indicates that over 3.6 million individuals in the Kingdom of Saudi Arabia had been victims of cybercrime more than the year before, guiding them to each acquire express economic fatalities equalling US$195 or $730 SR (Electrony.net, 2012). The objectives of the study, which is one of the world's major researches of cybercrimes, was to observe the implication of cybercrime on customers, and how it influences the approval and growth of modern sciences considered to advance the safety of people (Al Amro, 2017). The 2012 edition of the Norton study following the outcomes of examinations of further 13,000 adult users in 24 countries, suggests that the undeviating expenditure connected with customer Internet crimes in the United States equalled around US$ 110 billion during the past one year (Al Amro, 2017).

For every 18 seconds, an adult becomes the butt of cybercrime, an established study which guides to additional 1.5 million individuals becoming the casualty of cybercrime each day all over the globe, with a typical failure coming to equal of US$197 for every casualty. The overall price of customer Internet crime is comparable to the price of a week's of food for a family of four people in the United States. Around 556 million adults all over the world have experienced internet crime in the past one year, a figure higher than the whole community of the EU (Al Amro, 2017). This number constituted 46 per cent of the number of adults who utilise the Internet, and in 2011, 45% of extremely related outcomes were acquired. 40 per cent of users of social networks in the KSA has experienced internet crimes on social networking platforms in Saudi Arabia (Al Amro, 2017). 20% of adults became a casualty to social networks and mobile devices amid social network users, in the past one year in the KSA, in contrast with 21% at the global stage (Al Amro, 2017).

On the report of the Symantec, a US security software provider that carried out a study in the KSA, in 2016, about 6.5 million individuals in the KSA were victims of Internet crime. There arises the urgency to teach young individuals about cybercrime and to pressure the government to deal with it. Much work is as of now required to increase alertness, and to demonstrate that method to deal with safety against IT crimes and violations are exceptionally pathetic in Saudi society. Symantec's statement indicates that a total of about 6538262 individuals was the number of casualty assault by hackers or those affected by online crime. The statement also discloses that about (46%) of millennial have been victims of cybercrimes compared to 37% of the younger ones (Al Amro, 2017). Almost about five of millennial astonishingly agreed on providing passwords for different individuals, even though they are aware of the dangers linked to this. Because of this, Ayas Houari, Regional Director of Symantec Saudi Arabia, said, "With 58% of the populace having experienced cybercrime last year, it has unfortunately become popular in Saudi Arabia." He also said that "On the international standard of 48%, it has increased by 10%, and thus, strengthens the urgency for a change in user's attitude in the kingdom." Users are expected to be more efficient at safeguarding their private information, and be informed that straightforward protective methods can effortlessly avoid likely assaults, he says (Al Amro, 2017).

With the growing amount of people connecting while utilising mobile gadgets, cyber intimidations are becoming more and more widespread amongst all age brackets. In every four individuals, one has had their mobile devices stolen, possibly revealing delicate data in their social media, banking applications and emails to web thieves. In every seven consumers, one would have his identity stolen, for every six, one has had their social account hacked, and in every four one has had their emails tampered with by hackers, this is from a statement of one study. To investigate the safety consequences of online user crime, the software provider also interviewed 1,000 individuals in the KSA. With the incidence of crime on the internet, users missed almost a day of trade. Also, that amounts to SR 3,230 for every individual, with customers losing over 21 billion SAR in sum (Al Amro, 2017).

Cybercrime furthermore charges the kingdom SR 2.8 billion yearly, showing that there are 1.5 million casualties every day in all countries, that are vulnerable to the elements of electronic crimes, as displayed in Figure 3. About 20% have adequate practical alertness. In Saudi Arabia and other Arab countries, the significant issue is the urgency to encourage young individuals about cybercrime and to reach out to the government to deal with it. An additional endeavour is presently required to increase knowledge, and to demonstrate that the method to deal with safety violations and IT crimes is incredibly pathetic in Saudi culture (Al Amro, 2017).

2.4. Cybercrime Awareness and Vulnerability in Saudi Arabia

Understanding the impact of cybercrime is hinged on the degree of awareness among users' n KSA. Khan (2012) concluded that the awareness level is shallow and decried that cybercrime is evolving in Saudi Arabia as witnessed across the globe with limited knowledge and awareness in the country. The finding of Alotaibi, Furnell, Stengel, and Papadaki, (2016) even among educated Arabians affirmed the weakness of cybersecurity. Their knowledge of ethical conduct to lower their degree of vulnerability online was very low as numerous still show an increasing level of naivety while using the internet.

Elnaim (2013) quoted Symantec report stating that 40 per cent of adults in KSA are not aware of the discrete functioning of malware thereby making it hard to determine if the computer has been compromised. From this argument, the degree of vulnerability within the Saudi cyberspace is high. Saudi lacks official figure of major cybercrime, thereby making it difficult to determine the level of impact. There are crime statistics publication in Saudi Arabia, despite the official restrictions on the subject matter. However, it was established that a large number of Saudis are vulnerable to numerous types of fraudulent (criminal) activities online (Algarni, 2013).

The vulnerability of internet users is not limited to KSA. Other countries have risks with their users having a significant level of exposure to crime. It is a global phenomenon with the increasing borderless attack. Bronk and Tikk-Ringas, (2013) noted the Stuxnet virus works in several countries, and as such, it is not based on any vulnerability. With cybercrime becoming trans-border, the vulnerability of Saudis must not be escalated beyond proportion.

2.5. The Impact of Cybercrime on Saudi Arabia

There are numerous incidences of cybercrime, especially when the end-user is regarded as victims. Hassan et al. (2012) stated that defamation of image is a fundamental impact of cybercrime on end-user. Cybercrime often exposes victims to embarrassment through the exposure of data and illegal access to private information. For example, the exposure of the nude pictures of Jennifer Lawrence by cybercriminals. It is evident that cybercrime directly undermines the image of end-users. Sturges (2015) noted that the internet is the major medium through which distribution of pornography dissemination is conducted.

Despite the high regulation of the internet in Saudi Arabia, pornography remains a major challenge. The Saudi Ministry of Justice identified that 20% of children are exposed to Pornography annually (Ministry of Justice, 2012). Despite the impact on the image of end-users, another angle is inappropriate access by minors and other public. Khan (2012) established that Pornography is a major adverse impact based on publishing in even religious websites. The pornography impact continues to antagonise the values of end-users as everybody in Saudi Arabia is a potential victim.

Cybercrime impact can be financial. Khan (2012) maintained that losses of money are a significant impact that end-users experience. Algarni (2013) argued that fraud online could have other social consequences that will be difficult to measure. With the increasing level of financial crime on the internet, the impact cannot be directly associated to finance but to other social implications that emanate from crime. Anderson et al. (2011) noted that Advance Fee Fraud puts the victim in a position where they lose money. The impact is a financial loss for which the criminals make the victims lose money.

The theft of information expose end-users to significant loss of privacy, and regarding banking information, it can result in financial loss. Khan (2012) stated that Saudi Arabia experience theft of bank accounts and this makes their financial information to become susceptible to loss. Another aspect of this is that cybercrime attacks on the financial sector made it lose integrity and limited the quality of service to clients.

Measuring the depth of its impact can be challenging. In contrast, Khan (2012) maintained that cybercrime such as cyberstalking could have the psychological and social effect that is immeasurable. This is because these crimes directly impact the emotional well-being of the victims, thereby resulting in grave consequence. Al-Zharani (2015) noted the emotional impact that cyber-bully victims in Saudi Arabia are encountering. The variation in crime comes with different and numerous types of impact.

On the other hand, Elnaim (2013) pointed to another kind of impact which is the disclosure of sensitive personal information of victims. This was derived from the dumping of 812 user record online from the King Saud University (KSU) thereby making them be at risk online. This kind of impact can endanger the end-user in a way that cannot be determined.

Another argument from Algarni (2013) and Elnaim (2013) is that services can be disrupted and have different implications for end-users. Chan (2016) reported cyber-attack that affected the Aviation agency thereby clearing data and bringing the operations to a halt for some days. With this kind of attack, the entire immigration process in Saudi Arabia is impacted, thereby making the safety of the entire populace and users of the airports to be jeopardised. In this light, the impact cannot strictly be financial, psychological or social but carry public safety impact that is unprecedented.

2.6. Anti-Cybercrime Law in Saudi Arabia

The supreme body of Law in KSA is the Sharīʿah. It is made up of a compilation of basic ethics copied from different origins, some of which are the Holy Qu'ran and the Sunnah, that contains the witnessed statements and activities of the Prophet Mohammed. Forbidden actions under Sharīʿah are liable to be punished by exact penalties set out in the Holy Qu'ran or the Sunnah (Elnaim, 2013). If the Sunnah and Holy Quran do not have a similar instance, a moderator may utilise his judgment to decide the suitable punishment. Financial reparations, withdrawal of some privileges and incarceration are some of the punishments given. An adjudicator will consider the harm experienced by a victim or if the harm of that nature is real or significant in deciding the strictness of a punishment (Elnaim, 2013).

Compensation is nonetheless awarded by Saudi Arabian adjudicatory bodies generally. The latest Arab Cybercrime Agreement (no. 126 of 2012) was permitted in Saudi Arabia. Crimes like cyber terrorism, creation and distribution of viruses, credit card frauds, illegal access and interception, internet crimes, system interference, hacking, and so on are a list of some of the electronic crimes which this contract will primarily tackle. Its mission also includes inspiring collaboration among Arab nations to fight cybercrimes. The contract also states the significance of enforcing the Copyrights Law. Any violators of the Contract rules and regulations are punished. Saudi Arabia has in the past issued a strict Law on cybercrimes which was made up of 16 parts as a backdrop. The strict characteristics of the law comprise of the following: (Elnaim, 2013)

Table 4: Anti-Cybercrime Law in Saudi Arabia (Elnaim, 2013)

Crime	Fines	Imprisonment Term
Gaining entry into a government system, without intentionally seeking approval, and through this act, steal data which has been decided by the Saudi government to require safety from unapproved admittance for reason of country safety; - Utilizing the internet in advocating terror campaign.	Up to 5 million Saudi Riyal (around US $1.3 million)	Not greater than ten years
- Designing websites that support drug abuse or which are made up of explicit contents; - Designing websites or activities which breaches any of the Kingdom's common laws, Islamic morals or communal principles	Up to 3 million Saudi Riyals (around US $800,000)	Not greater than five years
- Having gained entry to a system without seeking approval, with the objective of destroying or altering its data.	Up to 3 million Saudi Riyals (around US $800,000)	Not more than four years
- Using websites to carry out counterfeit business	Up to 1 million Saudi Riyals (around US $260,000)	Not more than three years
- Gaining entry to a website without seeking approval, to destroy or alter its data.	Up to 500,000 million Saudi Riyals (around US $130,000)	Not more than one years

2.7. Summary

From the secondary research, it is identified that there are different types of cybercrimes experienced by Saudi Arabia. The government has implemented an anti-cybercrime law which has fines and imprisonment for cyber-attacks.

Chapter 3: Research Methodology

3.1. Introduction

This chapter mainly focuses on the methodology adopted for this research; Data Collection, Sampling and data analysis.

3.2. Method

The method adopted for this research is a mixed method. This method involves the combination of both the qualitative and quantitative method (Jha, 2008). The strength of this method is in the support for using more than one data collection instrument and can combine the two data types in the data analysis. Both qualitative and quantitative method has weaknesses that can weaken the quality of the research.

The qualitative methodology provides in-depth contextual information, thereby providing underlining reasons for the opinions of participants. However, it consumes a high level of resources and requires much planning, thereby making the number of participants to be lower, with analysis usually based on explanation (Jha, 2008). This project used the face-to-face interview method as a qualitative method.

The quantitative method is scientific with a focus on the statistical presentation of the distribution of opinion. The collected data is statistical and support the involvement of a high number of participants. However, the findings are not in-depth as new insight from the interpretation of participants cannot be retrieved because participants are often limited to options provided by the researcher. This project used an online survey using Google forms as a quantitative method. Mixing the two methods is often called triangulation and this research will use the strength of one method to cater to the weakness of the other.

3.3. Data Collection

Because of the selected method, questionnaire and interview will be employed for data collection. The questionnaire will be for the quantitative findings while the qualitative method will use the interview. The questionnaire will be distributed face-to-face by the researcher to ensure that the actual participants are involved in the research. The design of the questions will be in two sections. The first section will focus on collecting the demographic data of the participants. The second section will contain the core questions that will provide the information to satisfy the aim of the research.

The interview will be semi-structured. Semi-structured interview involves the design of core questions before the interview to control the information to be retrieved. The questions are not definitive as they only serve as a guide with the participants having the liberty to stretch the findings to other areas further. The drafted questions will be few. However, the demographic information collected in the questionnaire will be replicated for the interview to ensure that the overall participants are presented in the data analysis. The interview will be conducted face-to-face by the researcher.

The interview will help in providing rich contextual information and high level of information that will enhance the understanding of not just the impact, but the reasons for the impact and how the victims cope with the impact. This detailed explanation and information will enrich the understanding of the findings. The questionnaire will enable the collection of the opinion distribution from numerous participants, thereby substantiating the findings from the literature.

3.4. Sampling

Participation will be in two groups. The first group are individuals who have insights regarding IT security, which includes people who are working in the information security in any organisation or government in Saudi Arabia and the scholars who are involved in the research regarding the IT security in Saudi Arabia. This group will give an in-depth understanding of the vulnerability and the insider information on the cybersecurity impact within the Saudi cyberspace.

The second group of participants are members of the public that uses the internet. End-users are many and cover a significant population of Saudi Arabia. According to live Internet stats, there are over 20 million internet users as at July 2016. It suggests that the potential number of participants can be over 20 million. Also, in the business-to-business model of electronic commerce, the end-users can be businesses, thereby increasing the size of the research population. In this light, sampling has become necessary to have effective representation of the perspectives within the country. Sampling represents the process of selecting units from an entire population in order to derive information that will represent the unbiased opinion of the whole population (Kuada, 2012).

Considering the size of the research population, the use of sampling is inevitable for this research. Two factors will be used to recruit the participants at businesses. The two factors include position held in the organisation and the type of organisation (government or private business). Emphasis will be laid on individuals that work in the cybersecurity or information security department of their business and are in the middle or top management positions. Random sampling will be used for recruiting.

Overall, 300 participants are anticipated to be involved in this research. 50 of the participants will be recruited from businesses while the remaining 250 will participate using the questionnaire. Participants in businesses that will be recruited using snowballing as a single contact will be contacted initially and enjoined to suggest relevant people. This process will be continued until the number of participants is completed.

3.5. Data Analysis

Analysing the collected data will involve the use of the thematic approach. Bryan and Clarke (2006) presented a thematic approach as involving the definition of themes, where research findings can be discussed. The research questions will be used to define the themes under which the findings will be presented. The findings from the questionnaire will be analysed using statistical methods while the descriptive method will be used for the interview. While graphs and charts will be used to present the questionnaire findings, the interview findings will be used to explain the underlining reasons and justifications for the various opinion distribution in the questionnaire response. This combination will be used to present each theme of this research.

3.6. Ethical, legal and professional Considerations

In conducting this research, there are fundamental considerations that can adversely affect the conduct of the research and the overall quality of the findings. These considerations can be ethical, professional or legal. The first consideration is the difficulty in the recruitment of participants. When the consent of participants cannot be sought, it will be difficult to retrieve the necessary primary data for this research.

For research to achieve a high level of ethical standing, participation must be voluntary, and consent must be sought. Ethical consideration is critical to research by encouraging the environment of accountability, mutual respect and trust among researchers. Ethical standards must be adhered for the public to believe and support research. Two ethical issues in this research are voluntary participation and informed consent. Both issues ensure that all human subjects decided to participate out of their own free will and they have adequate information concerning the research project procedures together with any potential risks

Researchers must find a way to demonstrate that participation is voluntary while the participants must give their formal consent. As recommended by Jha (2008), surmounting this ethical challenge is possible using a consent form. This is a form (see appendix for sample) that contains details of the of the research with a definite statement of the willingness of the participants to voluntarily participate. The participants will be enjoined to append their signature in order to demonstrate third informed consent, and that participation is voluntary.

Professionally, the health and safety of participants regarding job security and their not being exposed to any form of risk are fundamental to this research. This is entrenched in the need to ensure anonymity of the participants in a way that their comments or responses will not be used to trace them, therefore not resulting in any adverse effect. When the participation in the research can negatively impact participants, they will be reluctant to provide safe answers. Students at the University must not experience an adverse impact on their studies or personal life because of this research.

Some steps will be taken to ensure this concern does not affect the participants. The first step is not collecting the personal details of participants in the research. Information such as names, address, contact phone number, the organisational name will not be gathered to ensure that they cannot be traced.

Furthermore, every communication will be between the researcher and the participants using a private communication channel. This implies that communication will not involve any third party and will involve the use of personal emails that can only be accessed by participants and the researcher alone. This will ensure that participants identity is safeguarded with no professional consequences.

On the legal side, since Saudi Arabia has no data protection law, the requirement of the data protection Act 1998 is necessary for this research. This makes it imperative that confidential data must not be accessed or disseminated without proper approval. This binding law will provide a challenge concerning the kind of information that can be sought from participants. Seeking information that can harm others or an organisation must be vehemently avoided in this research. This research is only interested in relevant information and will not insinuate any form of risk to their organisation as research participants.

During data collection, the researcher must ensure that sensitive organisational information is avoided and not collected. This will be initiated through the comments and discussions with participants before the data collection starts. Participants will be informed of their legal responsibilities before the data collections are initiated. This research must further ensure that the health and safety of participants are not jeopardised.

To reduce the minority concerns in this research, the participants will be 18 years and above. This is imperative to eliminate any risk of involving a minor in the research. These decisions are made to ensure that the standardised practices will not contribute to participants not regarded as viable to participate. Involving minors can result in complexities that will undermine his reaction to the researcher.

Another consideration in this section is the data protection of participants. As discussed earlier, the contact data of participants must be safeguarded. Furthermore, the content of the responses to question must be safeguarded against third parties and other stakeholders, to uphold the integrity and honesty of the research. This will be done by digitising the findings immediately and putting a password on the computer system to avoid any unauthorised alteration. The hard copies of the data including notes and questionnaire will be stored in a cabinet that is locked with the keys that only the researcher can access. The collected data will be used for the research purpose and will not be diverted to other interests.

This research faces a major challenge of eliminating bias. The researcher must remain objective and not sway participants to the previous belief or the desired direction. The failure to eliminate bias will result in bad research quality, therefore, providing information in the opinion of that participants.

Achieving the elimination of bias will be conducted and focused on during the data collection process. The research will exert no form of influence on participants. The influence will be eliminated by encouraging the participants to offer a response based on personal conviction. In the questionnaire, the participants will lead the discussion with the researcher, avoiding conjectures and comments that will point to a direction. The information will strictly be based on the opinion of the participants without any form of intrusion or grooming to provide researcher desired response. The use of these steps will reduce bias to the barest minimum and enable the researcher to thrive on quality informed participation.

3.6. The survey and interview questions

See Appendix D and E for the survey and interview questions.

3.7. Summary

This chapter gave a summary regarding the approach and data used for this research.

Chapter 4: Data Analysis

4.1. Introduction

This chapter provides the summary findings from the survey and interview.

The survey link for the general public who uses the internet in Saudi Arabia is provided below:

XXXXXXXXXXXXXXXXXX

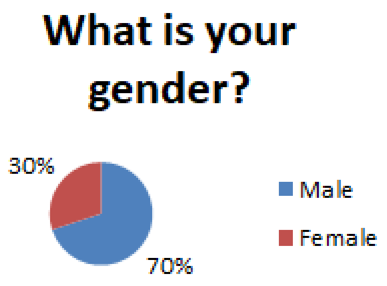
The survey link for people who have insights regarding the security and its impact are provided below:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

4.2. Survey Analysis

4.2.1. Survey responses for the general public who uses the internet in Saudi Arabia

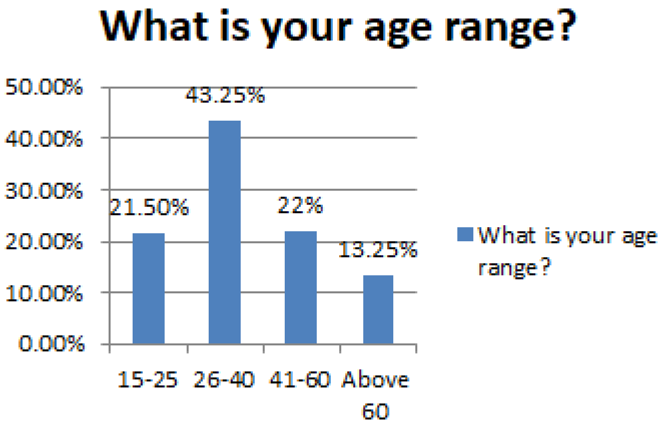
What is your gender?



	What is your gender?
Male	70%
Female	30%

Based on the pie chart, it is clear that the majority of participants are males which constitutes about 70% and the rest of the 30% are females. There is no limitation since both the genders have participated in the study.

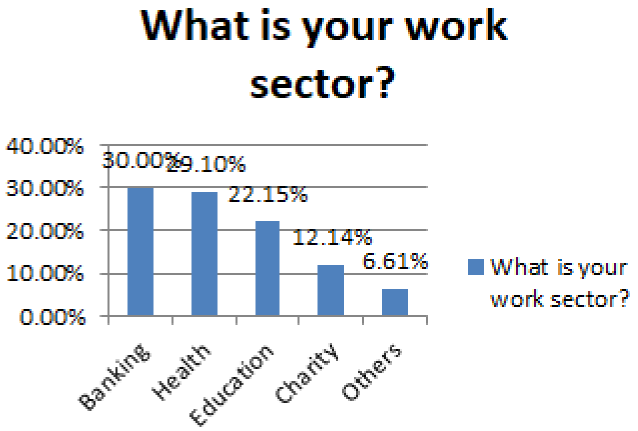
What is your age range?



	What is your age range?
15-25	21.50%
26-40	43.25%
41-60	22%
Above 60	13.25%

Four different age groups have participated in this research, out of the majority of participants are between the ages of 26-40, which constitutes about 43.25%. Those that fall under the age bracket of 15-25 constitute about 21.50%, while those within the age bracket of 41-60 are 22%. Those above 60 years of age are 13.25% of the participants. Comparatively, in all the age group, those above 60 years of age have the least percentage, while the age groups of 15-25 and 41-60 years old remain in a moderate range.

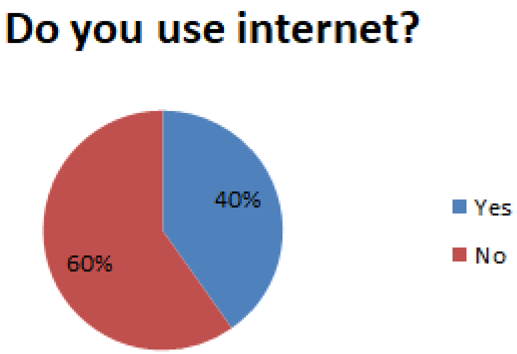
What is your work sector?



	What is your work sector?
Banking	30.00%
Health	29.10%
Education	22.15%
Charity	12.14%
Others	6.61%

People from different work sectors participated in the study, and they include the banking, health, education, charity and other sectors. Out of all these, the majority of people seem to work in the banking field, and this covers about 30% of the participants. The health sector stands next to health which covers about 29.10% of the participants. The field of education constitutes 22.15% of the participants, while charity has 12.14% participants. People from other sectors cover a small range of about 6.61% participants.

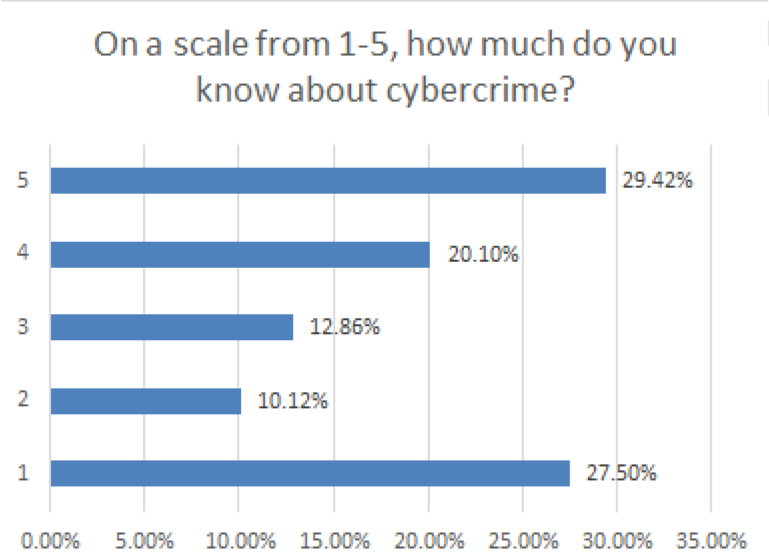
Do you use the internet?



	Do you use the internet?
Yes	40%
No	60%

It can be seen that 60% of the people do not use the internet, which also reduces their awareness to these type of cybercrime issues, while the other 40% of the people use the internet and they also would have faced some of these issues.

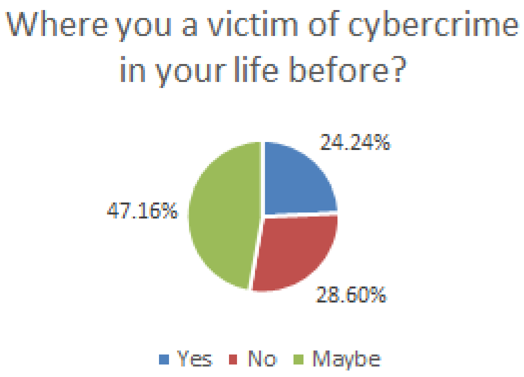
On a scale of 1-5, how much do you know about cybercrime?



	On a scale of 1-5, how much do you know about cybercrime?
1	27.50%
2	27.50%
3	12.86%
4	20.10%
5	27.50%

Based on the analysis, the rate of people that are aware of cybercrime is nearly equal to the rate of people who do not have an idea. Nearly 27.50% of the people have a detailed idea about cybercrime, while 27.50% have no idea of what cybercrime is. Therefore, this proves that people need more education on this matter. The participants that selected 2 are 27.50%, while those that selected 3 are 12.86%. The remaining 20.10% of the participants selected 4.

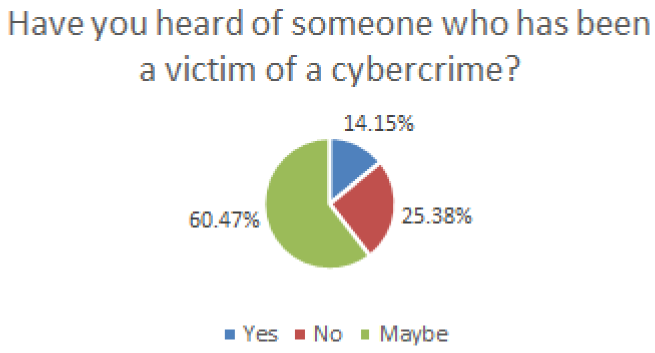
Where you a victim of cybercrime in your life before?



	Where you a victim of cybercrime in your life before?
Yes	24.24%
No	28.60%
Maybe	47.16%

When this question was asked, 28.60% of the people said they do not use the internet, while 24.24% of the people came forward and accepted that they had faced issues with cybercrime. The rest of the 47.16% of the participants selected ‘maybe’ as their response, since they did not know if they were affected or not, and some did not specify as to whether or not they have been victims of cybercrime.

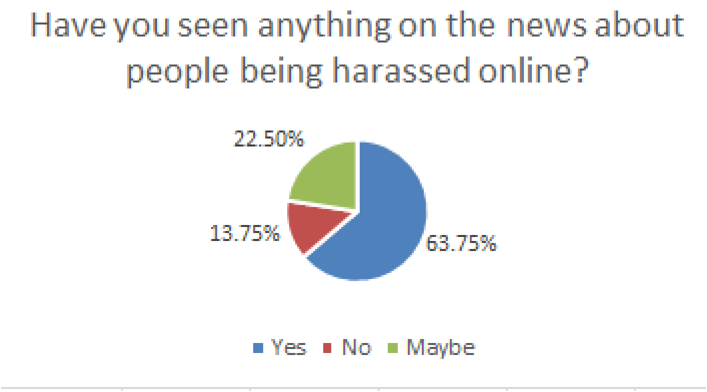
Have you heard of someone who has been a victim of cybercrime?



	Have you heard of someone who has been a victim of cybercrime?
Yes	14.15%
No	25.38%
Maybe	60.47%

Majority of the people indicated ‘maybe’, which constitutes about 60.47% of the participants. This is because they do not know if the others have faced the problem or not. This proves that not many people discuss this issue with each other. The number of participants that said ‘yes’ constitute 14.15% and the other 25.38% said ‘no’.

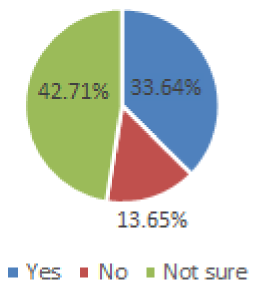
Have you seen anything on the news about people being harassed online?



	Have you seen anything on the news about people being harassed online?
Yes	63.75%
No	13.75%
Maybe	22.50%

From the chart, is it clear that people have been informed and are aware of the harassment issues in the newspaper since 63.75% of the people marked 'yes'. Even though there are such publications in the newspaper, some of the participants are not aware since 13.75% of them marked 'no', while the other 22.50% marked 'maybe'.

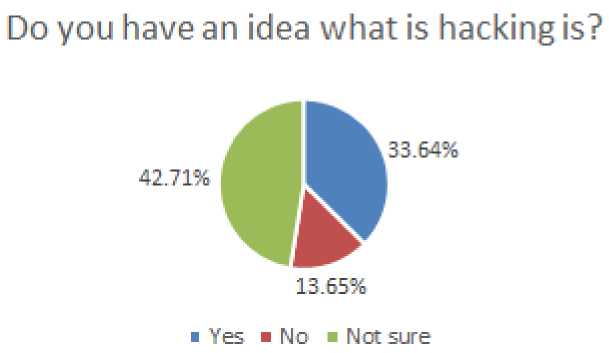
Do you have an idea on what online theft is?



	Do you have an idea on what online theft is?
Yes	33.64%
No	13.65%
Not sure	42.71%

The majority of the participants do not know what an online theft is since 42.71% of the people have marked ‘not sure’. The number of participants that know what online theft constitutes 33.64%, while 13.65% of them have accepted that they do not know.

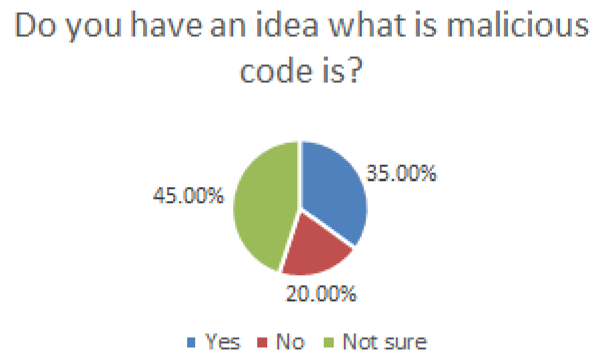
Do you have an idea on what hacking is?



	Do you have an idea on what hacking is?
Yes	33.64%
No	13.65%
Not sure	42.71%

The majority of the people do not know what hacking is since 42.71% of the people have marked ‘not sure’. The number of participants that know what hacking is, constitutes 33.64%, while 13.65% of the participants have accepted that they do not know.

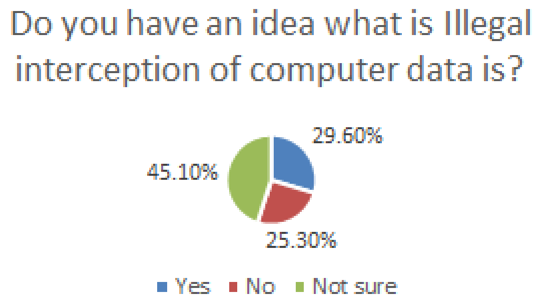
Do you have an idea on what malicious code is?



	Do you have an idea on what malicious code is?
Yes	35.00%
No	20.00%
Not sure	45.00%

The majority of the people are not sure of what malicious code is, hence, their selection of ‘not sure’ by 45.00% of them. The number of people who know what malicious code is, constitutes 35.00%, while 20.00% of them have accepted that they do not know what it is by marking ‘no.

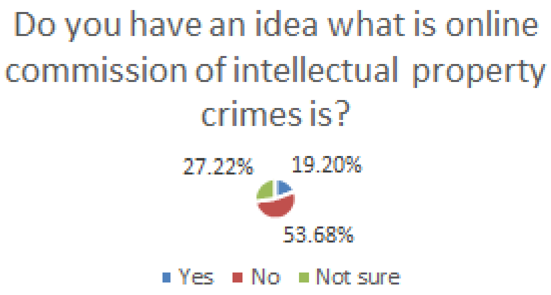
Do you have an idea what is Illegal interception of computer data is?



	Do you have an idea what is Illegal interception of computer data is?
Yes	29.60%
No	25.30%
Not sure	45.10%

The majority of the people do not know what illegal interception of computer data is, since ‘not sure’ has been marked by 45.10% of the people. Those that indicated ‘yes’ as their response to the question constitutes 29.60 %, while 25.30% of them have accepted that they do not know by marking ‘no’.

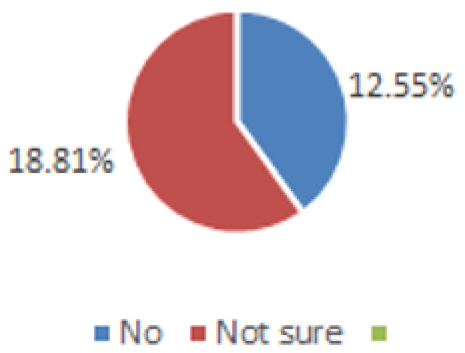
Do you have an idea on what an online commission of intellectual property crimes is?



	Do you have an idea on what an online commission of intellectual property crimes is?
Yes	19.20%
No	53.68%
Not sure	27.22%

The majority of the people do not know what an online commission of intellectual property crimes is since 'no' was marked by 53.68% of the people. Those that know what the online commission of intellectual property crime means, constitutes 10.20% of the participants while 27.22% of them marked 'not sure' as their response.

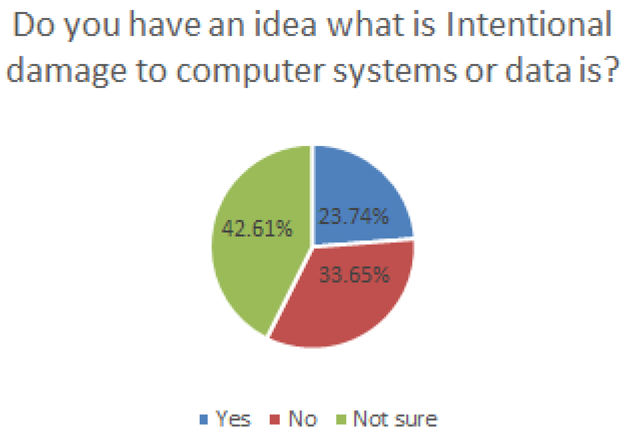
Do you have an idea on what child pornography and sex trafficking is?



	Do you have an idea on what child pornography and sex trafficking is?
Yes	68.64%
No	12.55%
Not sure	18.81%

The majority of the participants know what child pornography and sex trafficking is since 'yes' has been marked by 68.64% of them. The number of participants that did not know what the question means, constitutes 12.55 %, while the rest of the 18.81% of participants marked 'not sure'.

Do you have an idea on what Intentional damage to computer systems or data is?



	Do you have an idea on what Intentional damage to computer systems or data is?
Yes	23.74%
No	33.65%
Not sure	42.61%

The majority of the people are not sure of what intentional damage to computer systems or data means since 45.61% of the people have marked ‘not sure’. On the other hand, 23.74% do know what intentional damage to computer systems or data is, while 33.65% of them have accepted that they do not know by marking ‘no’ for their response.

What is an online commission of intellectual property crimes?

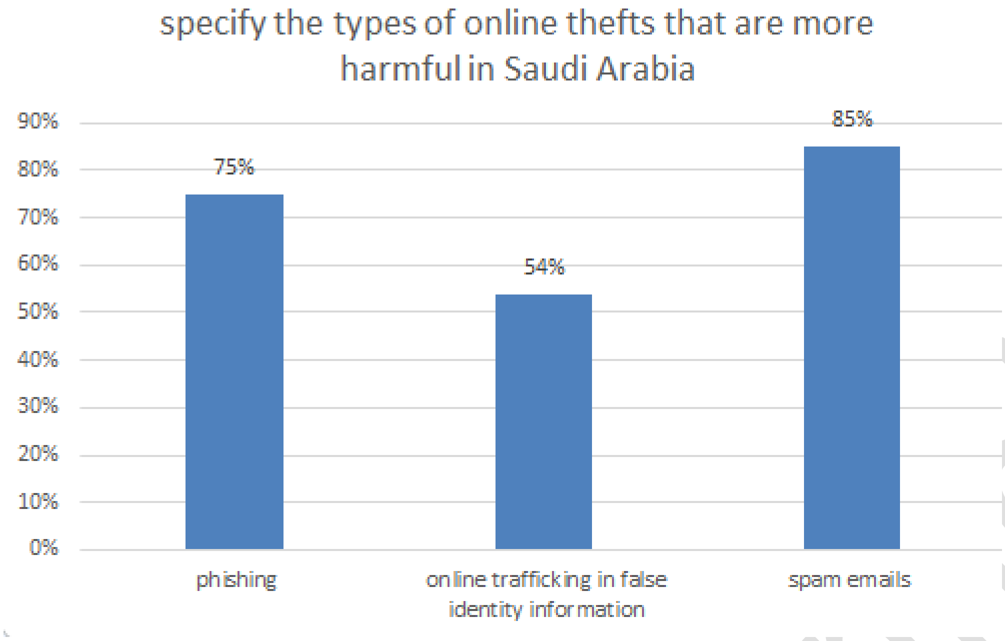
The following summary was extracted from the survey responses.

This is where we have the right to any material that we have created. This means that we have the right to use, sell and publish the materials that we create. However, when this information is published on the internet, it can be used and accessed by anyone else without the creator’s permission.

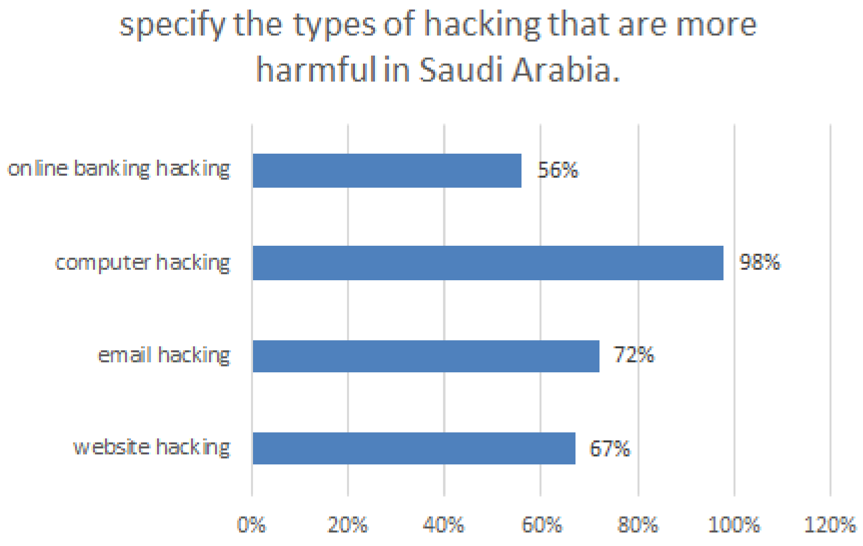
What is child pornography and sex trafficking?

The following summary was extracted from the survey responses.

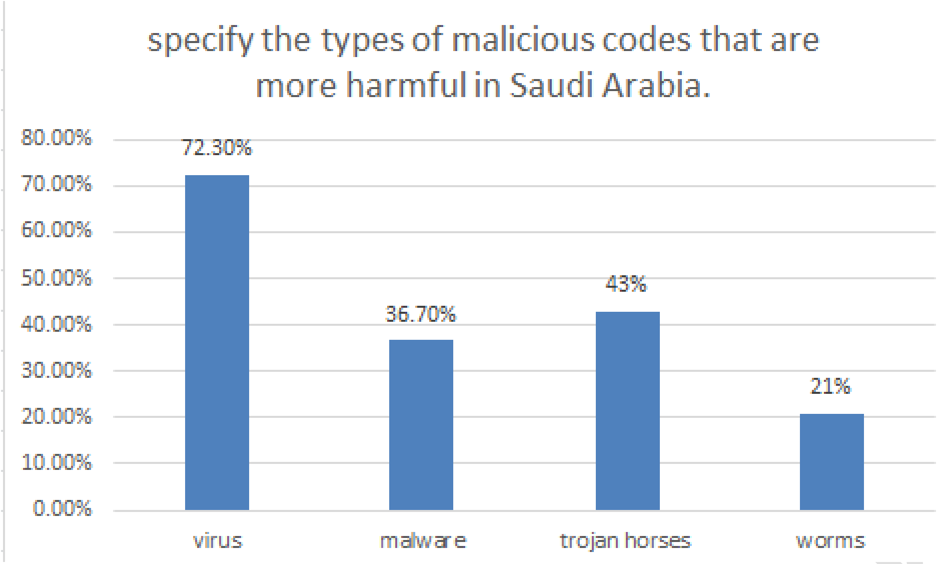
This is where a child is forced to get involved in sexually explicit activities. This is most of the time documented in crime scenes as videos and images and circulated among different people for personal consumption. This is an issue which happens globally but is also still not prohibited in some countries.



Many different types of theft have been mentioned by people including phishing, online trafficking, false identity, and spam emails. About 85% of the participants that make up the majority say they get spam emails, while the 75% of them ticked 'phishing' as their response. The least marked option was online trafficking in false identity which constitutes about 54% of the total participants.



There are many different types of hacking as shown above. Majority of the people said that computer hacking is very common, and they constitute 98% of the participants. The second highest option selected was email hacking, which was the response of 72% of the participants. Hacking of online banking had 56% respondents, while website hacking had 67% respondents. All the examples of hacking in Saudi Arabia given in this report are common.



There are many different types of malicious codes like virus, malware and so on. Most of the people are affected by a virus, and they make up 72.70% of the participants. Worms had the lowest marked one and the percentage of participants that selected it was 21%. while malware was 36.70%. Trojan horses had 43% respondents. This proves that the majority of the people are affected by malware.

Suggested steps that users should adapt to prevent online identity theft

The list of steps suggested by the general public who uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have a two-level authentication
- Include biometric authentication
- Do not distribute the personal information

Suggested steps that users should adapt to prevent hacking

The list of steps suggested by the general public who uses the internet is provided below:

- Do not connect the computer to the internet when it is not in use
- Have an anti-virus on the computer
- Never click on an unknown link
- Use different passwords on different sites
- Never reuse main email password

- Only shop online on secure sites
- Ignore pop-ups
- Avoid using public Wi-Fi

Suggested steps that users should adapt to prevent malicious code

The list of steps suggested by the general public who uses the internet is provided below:

- Have an anti-virus
- Keep platforms and scripts up-to-date
- Install security plugins, when possible
- Only visit sites that are https

Suggested steps that the users should adapt to prevent Illegal interception of computer data

The list of steps suggested by the general public who uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information

Suggested steps that the users should adapt to prevent the online commission of intellectual property crimes

The list of steps suggested by the general public who uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information
- Watermark the images to avoid people copying it.

Suggested steps that users should adapt to prevent online trafficking in child pornography.

The list of steps suggested by the general public who uses the internet is provided below:

- Create awareness among the children about child pornography
- Block the pornography websites

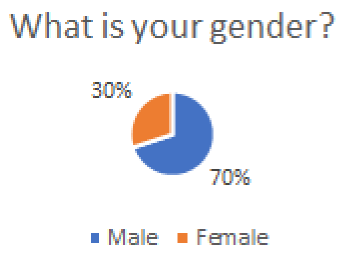
Suggested steps that users should adapt to prevent Intentional damage to computer systems or data

The list of steps suggested by the general public who uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information

4.2.2. Survey responses for IT specialists in Saudi Arabia

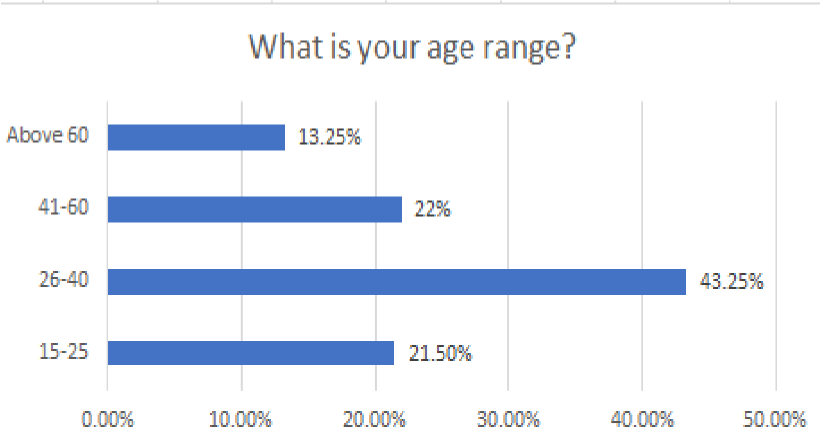
What is your gender?



	What is your gender?
Male	70%
Female	30%

Based on the pie chart, it is clear that the majority of the participants are males, and they constitute 70%, while the remaining 30% are females. There is no limitation since both genders participated in the study.

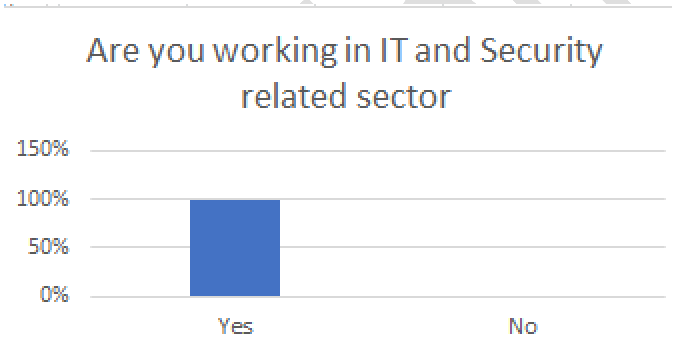
What is your age range?



	What is your age range?
15-25	21.50%
26-40	43.25%
41-60	22%
Above 60	13.25%

Four different age groups participated in the study and those within the age bracket of 26-40 years constitute 43.25%; they form the majority of the participants. Participants between the ages of 15-25 comprise 21.50% of the participants, whereas those between 41-60 years of age make up 22% of the participants. Those above 60 years of age constitutes 13.25% of those that participated. Compared to all other age group, the percentage of participants above 60 is the least, while those within the age bracket 15-25 and 41-60 remain in a moderate range.

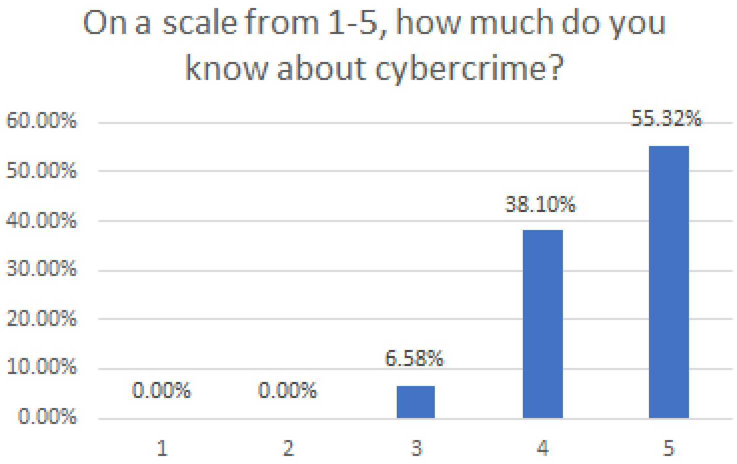
Are you working in IT and Security related sector?



	Are you working in IT and Security related sector
Yes	100%
No	0%

This questionnaire was given to technicians who worked in an IT and security-related sector. Therefore, this question has a 100% yes answer.

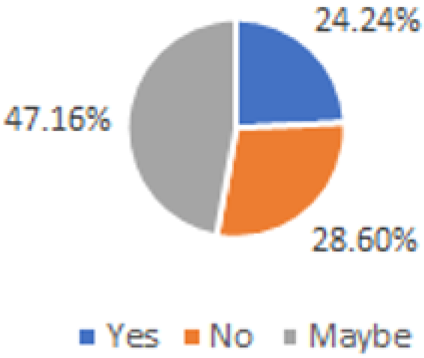
On a scale of 1-5, how much do you know about cybercrime?



	On a scale of 1-5, how much do you know about cybercrime?
1	0.00%
2	0.00%
3	6.58%
4	38.10%
5	55.32%

For this question, no one indicated that he or she does not know since all of them work in an IT field. Most people have a very detailed idea about cybersecurity, and they constitute 55.32% of the participants. The percentage of people that do not have a detailed idea about cyber security but knew what is was constitute 8.10% of the participants. A small percentage of participants ticked '3' and they constitute 6.58% of the participants.

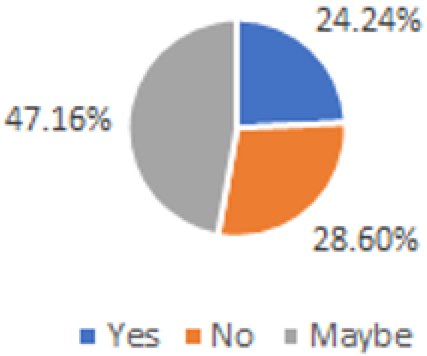
Have you ever been a victim of cybercrime?



	Have you ever been a victim of cybercrime?
Yes	24.24%
No	28.60%
Maybe	47.16%

When this question was asked, 28.60% of the people said that they do not have any experience on the internet while 24.24% of the people affirmed that they had been victims of cybercrime. The rest of the 47.16% marked 'maybe' since they are not aware if they had been affected or not, and some chose not to indicate if they have experienced cybercrime or not.

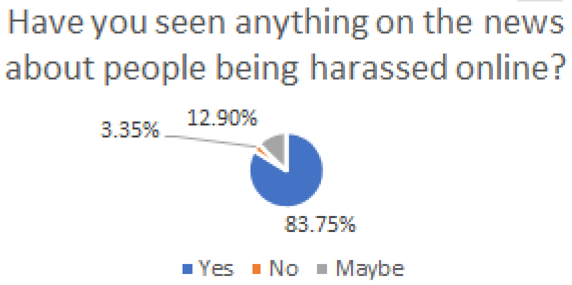
Have you heard of someone who has been a victim of a cybercrime?



	Have you heard of someone who has been a victim of a cybercrime?
Yes	14.15%
No	25.38%
Maybe	60.47%

Majority of the people said 'maybe' because they are not aware of whether or not they someone else has been a victim; they constitute 60.47% of the participants. This proves that many people do not discuss this kind of issue with each other. It is noteworthy that 14.15% of the people said 'yes' and the other 25.38% said 'no'.

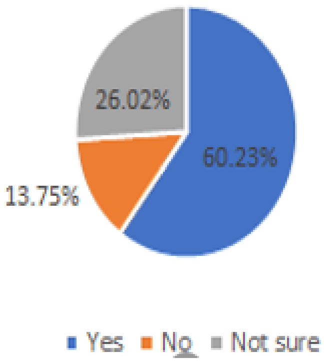
Have you seen anything on the news about people being harassed online?



	Have you seen anything on the news about people being harassed online?
Yes	83.75%
No	3.35%
Maybe	12.90%

It is clear that people have been informed and are aware of the harassment issues in the newspaper since 83.75% of the participants marked 'yes'. Some people are still not aware of this fact, even though such information is published in the newspaper. To this end, the pie chart shows that 3.35% marked 'no' while the remaining 12.90% of participants marked 'maybe'.

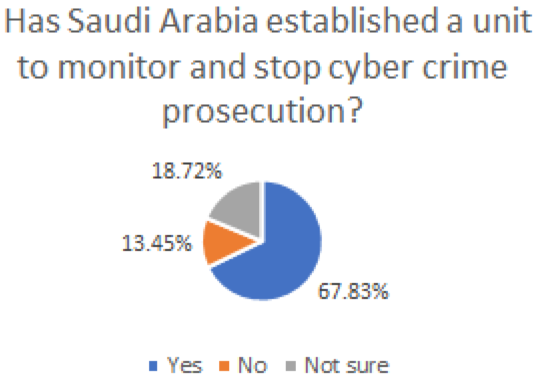
Does Saudi Arabia have experience in strengthening the relationship between authorities responsible for investigating cyber-crimes and internet service providers that may be shared with other States as a best practice in this area?



	Does Saudi Arabia have experience in strengthening the relationship between authorities responsible for investigating cyber-crimes and internet service providers that may be shared with other States as a best practice in the area?
Yes	60.23%
No	13.75%
Not sure	26.02%

Majority of the participants are aware of this question and responded with ‘yes’; they constitute 60.23% of the participants, while 13.75% of them marked ‘no’. The remaining 26.02% of the participants indicated that they are not sure about the answer to this question.

Has Saudi Arabia established a unit to monitor and stop cybercrime prosecution?



	Has Saudi Arabia established a unit to monitor and stop cybercrime prosecution?
Yes	67.83%
No	13.45%
Not sure	18.72%

Based on these answers, it can be said that 67.83% of the people are aware of the rules and steps were taken by the government to stop cybercrimes. The percentage of participants that ticked ‘no’ constitute 13.45%, while the remaining participants marked that ‘not sure’, which is 18.72% of the participants.

What is an online commission of intellectual property crimes?

The following summary was extracted from the survey responses.

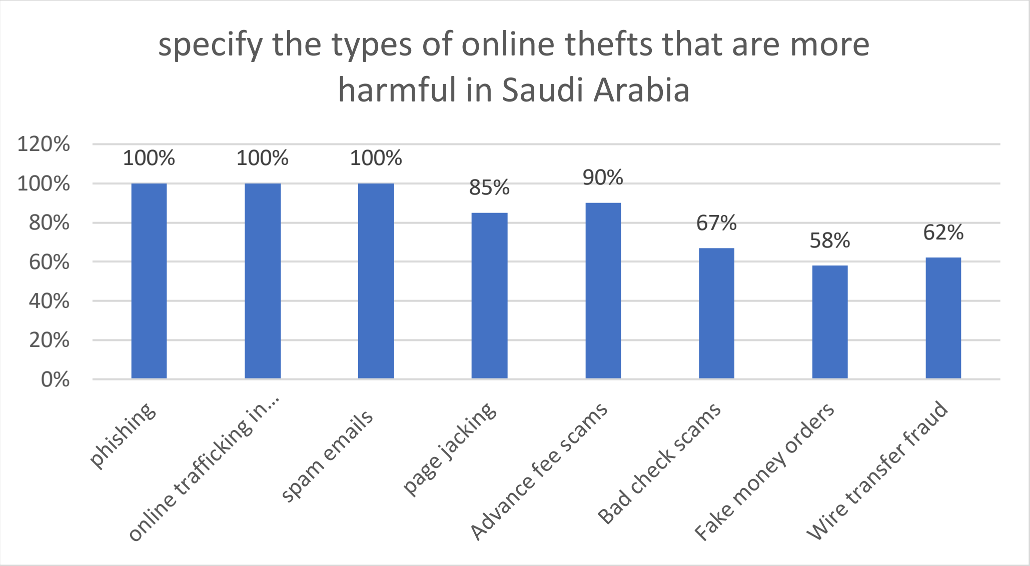
This is where the researchers of this report have the right to any material that they have created. This means they have the right to use, sell and publish the materials that they create. However, when this information is put into the internet it can be used and accessed by anyone else without the creator's permission. For example, multimedia and pictures

What is online trafficking in child pornography?

The following summary was extracted from the survey responses.

This is where a child is forced to get involved in sexually explicit activities. This is most of the time documented in crime scenes as videos and images and circulated among different people for personal consumption. This is an issue which happens world-wide, and as at yet, it is not prohibited in some countries.

Specify the types of online thefts that are more harmful in Saudi Arabia

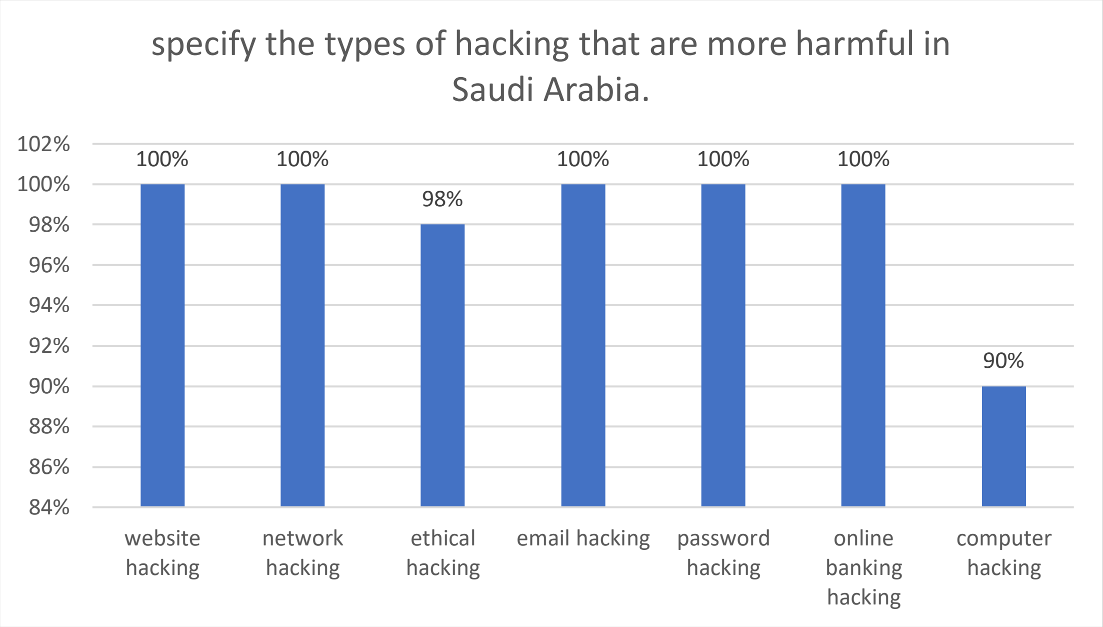


Online Crimes	**Percentage of participants that specify each of them**
phishing	100%
online trafficking in false identity information	100%
spam emails	100%
page jacking	85%
Advance fee scams	90%

Online Crimes	**Percentage of participants that specify each of them**
Bad check scams	67%
Fake money orders	58%
Wire transfer fraud	62%

All the responses agreed that phishing, online trafficking in false identity information and spam emails are the major challenges faced in Saudi Arabia. However, it is reasonable to say that all the given types of online thefts are challenging to Saudi Arabia.

Specify the types of hacking that are more harmful in Saudi Arabia.

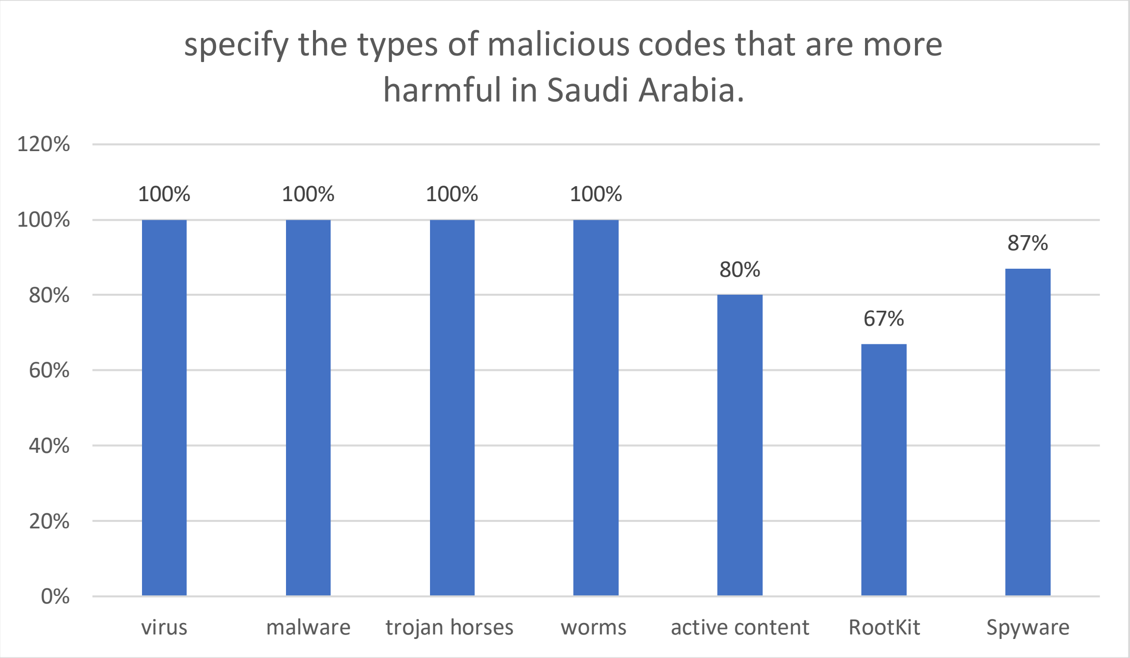


Types of Hacking	**Percentage of participants that specify the types of hacking that are more harmful in Saudi Arabia.**
website hacking	100%
network hacking	100%
ethical hacking	98%
email hacking	100%
password hacking	100%

Types of Hacking	Percentage of participants that specify the types of hacking that are more harmful in Saudi Arabia.
online banking hacking	100%
computer hacking	90%

All the responses agreed that website hacking, network hacking, email hacking, password hacking and online banking hacking are the major challenges faced in Saudi Arabia. However, it is reasonable to say that all the given types of hacking are challenging to Saudi Arabia.

Specify the types of malicious codes that are more harmful in Saudi Arabia



Types of Malicious Codes	Percentage of participants that specified the types of malicious codes that are more harmful in Saudi Arabia.
virus	100%
malware	100%
trojan horses	100%
worms	100%
active content	80%
Rootkit	67%

Spyware	87%

All the responses agreed that virus, malware, trojan horses and worms are the major challenges faced in Saudi Arabia. However, it is reasonable to say that all the given types of malicious codes are challenging to Saudi Arabia.

Suggested steps that users should adapt to prevent online identity theft

The list of steps suggested by the specialist that uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information

Suggested steps that users should adapt to prevent hacking

The list of steps suggested by the specialist that uses the internet is provided below:

- Do not connect the computer to the internet when not in use
- Have an anti-virus on the computer
- Never click on an unknown link
- Use different passwords on different sites
- Never reuse main email password
- Only shop online on secure sites
- Ignore pop-ups
- Avoid using public WI-FI

Suggested steps that users should adapt to prevent malicious code

The list of steps suggested by the specialist who uses the internet is provided below:

- Have an anti-virus
- Keep platforms and scripts up-to-date
- Install security plugins, when possible

- Only visit sites that are https

Suggested steps that users should adapt to prevent Illegal interception of computer data

The list of steps suggested by the specialist that uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information

Suggested steps that users should adapt to prevent the online commission of intellectual property crimes

The list of steps suggested by the specialist that uses the internet is provided below:

- Have complex password
- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information
- Watermark the pictures

Suggested steps that users should adapt to prevent online trafficking in child pornography

The list of steps suggested by the specialist that uses the internet is provided below:

- Create awareness among the children about child pornography
- Block the pornography websites

Suggested steps that users should adapt to prevent Intentional damage to computer systems or data

The list of steps suggested by the specialist that uses the internet is provided below:

- Have complex password

- Change password frequently
- Always use updated anti-virus with firewall protection
- Have two level authentications
- Include biometric authentication
- Do not distribute the personal information

Suggested steps that the private and public (government) organisations should adopt to prevent online identity theft

The list of steps suggested by the specialist that uses the internet is provided below:

- Create laws and policies
- Have a separate team with high quality IT specialists
- Adopt new technologies to ensure safety
- Encrypt the computer systems and storage systems.
- Ensure to adopt human biometric recognition for authentication
- Ensure to implement a minimum of two-level authentication
- Must change the password within a specific time frame

Suggested steps that the private and public (government) organisations should adopt in hacking

The list of steps suggested by the specialist the uses of the internet are provided below:

- Create laws and policies
- Have a separate team with high quality IT specialists
- Adopt new technologies to ensure safety
- Encrypt the computer systems and storage systems.
- Ensure to adopt human biometric recognition for authentication
- Ensure to implement minimum two-level authentication
- Must change the password within a specific time frame

Suggested steps that the private and public (government) organisations should adopt in malicious code

The list of steps suggested by the specialist that uses the internet is provided below:

- Create laws and policies

- Have a separate team with high quality IT specialists
- Adopt new technologies to ensure safety
- Encrypt the computer systems and storage systems.
- Have strong firewalls and online antivirus protection

Suggested steps that the private and public (government) organisations should adopt in Illegal interception of computer data

The list of steps suggested by the specialist that uses the internet is provided below:

- Create laws and policies
- Have a separate team with high quality IT specialists
- Adopt new technologies to ensure safety
- Encrypt the computer systems and storage systems.
- Have strong firewalls and online antivirus protection
- Ensure to adopt human biometric recognition for authentication
- Ensure to implement minimum two-level authentication
- Must change the password within a specific time frame

Suggested steps that the private and public (government) organisations should adopt an online commission of intellectual property crimes

The list of steps suggested by the specialist who uses the internet is provided below:

- Create laws and policies
- Have a separate team with high quality IT specialists
- Adopt new technologies to ensure safety
- Encrypt the computer systems and storage systems.
- Ensure to adopt human biometric recognition for authentication
- Ensure to implement minimum two-level authentication
- Must change the password within a specific time frame

Suggested steps that the private and public (government) organisations should adopt in online trafficking of child pornography

The list of steps suggested by the specialist that uses the internet is provided below:

- Create laws and policies
- Introduce serious punishments
- Create awareness among children regarding pornography
- Create an on-call police service
- Block the pornography websites

Suggested steps that the private and public (government) organisations should adopt in Intentional damage to computer systems or data

The list of steps suggested by the specialist that uses the internet is provided below:

- Create laws and policies
- Have a separate team with high quality IT specialists
- Adopt new technologies to ensure safety
- Encrypt the computer systems and storage systems.
- Ensure to adopt human biometric recognition for authentication
- Ensure to implement minimum two-level authentications
- Must change the password within a specific time frame

4.3. Interview Analysis

4.3.1. Analysis of Interview Questions for Users who use the Internet

Most of the people that participated are males, and they constitute 85% of the participants, while the remaining 15% of participants were females. People from different age groups participated, and the age group with the highest percentage was 60%. Based on the questions asked, it was clear that not many people were aware of these types of cybercrimes, even though the government created awareness through newspapers; this group of people constitute 88.5% of the participants, while the remaining participants were aware of these issues. The cause of this problem was discovered to be because nearly 67% of the people appear not to use the internet. Cybercrime awareness among men is more than women. Some of the men and women were also victims of the cybercrimes while using the internet, while some of them were being harassed online. Their details were hacked, and most of them seem to get emails which contain the virus. More people seem to be aware of child pornography, and they constitute 79.07% of the participants. It was concluded that their government is taking some basic steps to make people aware of these cybercrimes but is just not enough.

4.3.2. Analysis of Interview Questions for people who have insights regarding IT security

More males are working as technicians than women. The percentage of the male technicians is 90%. While carrying out the interview, the IT technicians seemed to be more worried about the cybercrime issues and that people were not aware of it. Nearly 80% of the technicians said that the government must take more steps to make people aware of cybercrime issues. Most of the participants were between the age group of 41-60 year, and this constitutes 55.76% of the participants. The percentage proves that the older adults have more experience and knowledge in this area. Moreover, nearly 45% of the technicians have been victims of cybercrime, while the rest ensured that they were not victims of such crimes since they are aware of the issues they might face. When the participants were questions about cybercrime faced by them, most of them seemed uncomfortable to answer. All of them said that the public must be made aware of the cybercrime issues, some even suggested of giving a workshop to kids in school to create awareness.

4.4. Summary

The results received from the interview and survey shows that the majority of the people in Saudi Arabia are not aware of cybercrime exposure and its impact. Also, the specialist who has insights regarding the security and its impact are worried about it. However, the Saudi government is trying to take steps to minimise the exposure and the impact.

Chapter 5: Discussion and Recommendation

5.1. Introduction

This chapter provides the discussion and the recommendation.

5.2. Discussion

From the primary research conducted, it is clear that most of the people that use the internet in Saudi Arabia are not aware of the types of cybercrime that they can get exposed to and what impact it will cause them personally and financially. This indicates that the government and private sectors of Saudi Arabia should focus on creating awareness among their citizens regarding cybercrime and its impact. It is possible to say that the Saudi Arabian government is taking steps to reduce the impact as well as reduce the exposure to cybercrime. However, the results from the steps are low because the end-users of the Internet in Saudi Arabia are not following the security precautions.

The most common type of cybercrime in Saudi Arabia that the primary and secondary research identified are an online commission of intellectual property crimes, online trafficking in child pornography, online theft, hacking, and types of malicious codes. However, the most important topic discussed in the primary research was online trafficking in child pornography.

Some of the discussed difficulties in controlling the internet child pornography are listed below;

- **The structure of the Internet:** Control of child pornography can be such a difficult task. This is because of the structure of the Internet. The Internet structure does not have any existing storage facility, neither does it have any controlling body. Due to its structure, several pathways can be used to achieve the same result, even when one pathway is blocked. The closure of a newsgroup or website can never serve as a deterrent since another one can be created instantly. This poses a great threat in inhibiting child pornography distribution. It is possible to spread child pornography even without the use of a central server. There is a debatable fact that the internet is uncontrollable.
- **The jurisdiction of the Internet is unpredictable:** The Internet is used globally and cuts across jurisdictional boundaries. In track defaulters, there must be a collaboration of intelligence and resources between law enforcement agencies across jurisdictions. If par adventure, operations run simultaneously from different jurisdictions, it may result in the pursuit of a particular defaulter. It is also complicated to decipher who has the duty of carrying out an investigation into child pornography culprits on the internet since the source of the images are unknown. It is difficult to investigate

offences related to child pornography since it cannot be categorised under any particular law enforcement jurisdiction.

- **No regulatory agency:** It is difficult to regulate the Internet because of its structure. Many law enforcement agencies across various jurisdictions are also hesitant in introducing policies that could control the Internet. Some people have argued about the most suitable weight to slam on defaulters to secure a community. It is also faced with considering how to avoid breaching the law of liberty and commercial interests. There is also an issue of unclear policies on whether ISPs should be held responsible for their contents or should be simply seen as channels in which contents are distributed. In a nutshell, there are no specific law binding ISPs regarding child internet pornography.
- **The differences in legislation:** The differences in laws and extents to which child pornography is allowed across jurisdictions had made it very difficult to attempt to regulate the Internet with regards to child pornography. Besides, different countries apply different approaches towards dealing with crimes associated with child pornography. The reason could be related to culture or simply because of corruption.
- **Defaulters' professionalism:** Defaulters have various sophisticated methods of evading being caught. There is a good number of veteran defaulters. Some of them are highly skilled with technology, and they have been actively participating in online paedophile newsgroups for over 20 years. The older ones give technical advice to the newcomers in paedophile bulletins. Many people have argued that the only defaulters caught are the inexperienced ones.
- **The sophistication and adaptation of Internet technology:** Defaulters are skilled and up to date with Internet technology. Also, it is possible for mails not to contain the identity of its senders. They also make use of file encryption. There has been an emergence of technological race between law enforcement agencies and pornographers.
- **The volume of Internet activity:** There is heavy traffic of activities in child pornography, and this makes it difficult to fish out its offenders. Most of the defaulters are fully aware of the fact that they cannot be caught.

Moreover, it is also specified in the primary research that the hacking is becoming a trend and people are doing it without any serious motive. Additionally, several materials are freely available for people to learn regarding the hacking procedures and writing of malicious codes. It is also commonly believed that children can easily learn how to program by learning how to write anti-virus. This indicate the current increasing trend in the cybercrime.

5.3. Recommendations

The recommendations to reduce the intellectual property crimes, hacking, online theft, online trafficking in child pornography and the reduce types of malicious codes are provided below:

5.3.1. The recommendations to reduce intellectual property crimes

The recommendations for the Saudi Arabian organisations and the general public that uses the internet to reduce the effect and vulnerability of intellectual property crimes are provided in table 5.

Table 5: The recommendations to reduce intellectual property crimes

Recommendation	Explanation
Organisation	The most important issue found within an organisation is most likely found in its security reports. In successfully tackling of security issues, a chief security officer should be appointed. He will be responsible for giving a detailed report to either the chief financial officer or the chief executive officer. He should be familiar with the boardroom. He should oversee personnel security, information security and also physical security.
Awareness and Education	It is important for an owner of intellectual property to regularly teach his workforce on the dangers of undercover financial operations, intellectual property theft, piracy, and counterfeiting. He should vividly explain to them that they have the obligation of securing the intellectual property of the organisation and also, their upkeep. He should give the workforce general training, then give specialised training to the administrators, managers, specialised staff, and so on. The responsibility of carrying out "Personnel Security" is done by Personnel Security. They are responsible for carrying out background checks and termination processes. He should put in place certain policies and ensure he implements them. He should get to know his potential employees. He should have constant interactions with them when he finally recruits them. He should deal with termination and resignation process tactfully. Information Security has the responsibility of employing certified information security professionals like CISM, CISSP, and so on. He should embrace best practices and create a pattern. He should employ the use of suitable technologies for information security like encryption, firewalls, strong authentication devices, intrusion detection, and so on. He should focus on maintenance of information, information access and also information destruction.

Physical Security	Try not to disregard the "Duh" factor. If information security is porous, then it will be senseless to invest in information security, talk less of carrying out background checks.
Intelligence	It is imperative for an owner of intellectual property to have security and business intelligence. He should have a good knowledge of his customers, his competitors and his associates. He should do a comprehensive study on the market environment. He should be up to date on recent patterns of financial fraud, state-sponsored economic undercover work, organised crime and hacking. He may not necessarily do this in his organisation. He can contract it out to professionals.
Industry Outreach	He should be a part of the groups that are related to his business. He should have constant interactions with them with the aim of finding out the threats and attacks they are experiencing.
Government Liaison	He should use his tax dollars. He must be abreast of the threat information from law enforcement, trade organizations within and outside the country his business is situated, or where he carries out his businesses, regulatory bodies, foreign ministries and government officials. It is possible for him to legally lose a market, even while he is on his right, and at the same time, it secures a part of the global market. This is seen as a possible survival strategy. The way out of this is not through lawsuits but the acceptance of the fact that there has been intellectual property theft. An intellectual property owner should put in efforts to secure his intellectual property. That way, he can save himself from the trouble and costs of lawsuits. He should ensure that he employs the services of professionals whenever he is having issues related to intellectual property.

5.3.2. The recommendations to reduce hacking

The recommendations for the Saudi Arabian government, organisations and general public that use the internet to reduce the effect and vulnerability for hacking are provided in table 6.

Table 6: The recommendations to reduce hackings

Recommendations	Explanation
Automatically update the OS and other software	Automatically update the OS and other software or do so frequently if it is not possible to do so automatically. This will make it difficult for

	hackers to access a user’s computer through vulnerabilities in outdated programs. Enable Microsoft products updates for extra protection; Office Suite will be updated simultaneously. Get rid of vulnerable software like flash or java.
Download the latest versions of security programs	Download the latest versions of security programs like firewall, antivirus, anti-spyware and anti-malware software in case they are not included in the OS. To avoid any form of attacks, get an anti-exploit technology like Malwarebytes.
Should get rid of every personal data contained in a computer	A user should get rid of every personal data contained in his computer if he intends to sell it. He can make use of D-ban to wipe out the hard drive. By so doing, the data is irrevocably destroyed. He should use a chainsaw if the data he needs to secure is crucial
Avoid using open WIFI	It will expose a user to cyber thieves to connect to his computer and download illegal files. He should use encrypted passwords to secure his WIFI. He may have to refresh the equipment every few years. Some routers do not have patched schemes. He should get newer routers because, with them, he can allow guests access segregated wireless access. They also can make regular changes in passwords simpler.
Securing devices with passwords.	All devices like laptop, desktop, tablet, phone, smartwatch, and so on, can be secured with the use of passwords. A user should lock his phone and ensure that the timeout is very short. For iPhone users, he can secure his phone with his fingerprint. Android users can do same with swipe or passkey. Every mobile device is made up of the good quantity of personal data. If exposed, the result can be devastating.
Make use of complex passwords and regularly change them	Use different passwords for different services. To make a user’s device more secure, utilise two-step authentication. The user is expected to initiate the procedure. This process makes the device harder to access and on the other hand, it is a lot easier to reclaim the device when the need arises.

Use uncommon answers for the security questions.	Do not make the answer to security questions easy for people to guess.
Be smart when assessing the internet.	A user should be smart when browsing and accessing his email. Cyber thieves still make use of phishing campaigns. He should confirm the email address he receives before giving out his personal details. He should ensure that the email is from a trusted source. If he is not sure of the source, he should quickly do a search on the Internet for the subject line. Other victims may have reported it online.
Do not link your social media accounts.	Do not respond to when prompted to link your social media accounts if you simply want will have access to most of your personal information.
Do not store sensitive information in the cloud.	Information stored in the cloud can never be private. Only a few cloud storage solutions have the option of encryption available. It’s ok to use cloud services but do not use it for very sensitive information.

5.3.3. The recommendations to reduce online theft

The recommendations for the Saudi Arabian government, organisations and general public that use the internet to reduce the effect and vulnerability to online theft are provided in table 7.

Table 7: The recommendation to reduce online theft

Recommendation	Explanation
Check bank statements regularly	Online banking makes it easier for fraudsters to chase after bank details. In the same way, a bank account holder has easy access to his/her bank statements by simply pressing a button. In some cases, certain banks alert their customers once they detect suspicious activity. Cultivate the habit of checking account balance regularly.
Be cautious when opening the attachment	Very destructive viruses are usually in attachments of files, especially from strange senders. It is advisable to open only trusted attachments. A user should open attachments from only senders that he has an idea of the content of the file.

Regularly update operating system (OS) and software	It is of utmost importance that a user should regularly update his software to avoid being a victim of cybercrime. Cybercriminals create malware regularly that helps them access unsuspecting users, so it is crucial for a user to secure his software by updating them on a regular basis. Although the majority of software manufacturers and OS providers frequently release security patches that makes it hard for cyber thieves to access details easily.
Disable file sharing on the computer	Most computers with some Windows version have file sharing enabled by default. With this people can easily access a user's files. Once he disables file sharing, he can have the liberty of allowing only preferred people to access his files. Computers with older versions of Microsoft, most especially Windows XP are at risk and they have less support. The only support they can have can be accessed by simply updating Windows. o Go to My Computer o Click Folder Options from the Tools menu o Click the View tab o Uncheck Use simple file sharing from Advanced Settings (Recommended).
Use a strong password	Users should make use of a strong password for all services they use. It is more advisable to use different passwords for each service used. In that way, fraudsters cannot easily access a user's details. A user should use a minimum of 8 characters for his password. He can make it a little complex by simply toggling between cases, use special characters and numbers. He should try not to use interests or names as passwords. Anybody can easily guess that or decipher that from his profile on social media. Usually, passwords are encrypted by Norton Internet Security for secure storage. Norton monitors them for unauthorised usage so that a user does not mistakenly enter his password anywhere. He will get notifications from them if they observe that he is entering a website with secure login details.

Read through the website's privacy policy	Privacy policy of most websites is usually displayed at the footer or in some cases, more conspicuously. First, take a good look at the privacy policy of a site before entering any confidential information. Do not enter any information into an untrusted site.
Do not disclose the PIN code	A user should not disclose his PIN code to anyone. No bank will ever request for it either through email, over the phone or on their website.
Open websites in new browser windows before entering confidential data	A user should enter his personal data only on new browser Windows. He should type the URL into the address bar to certify the legitimacy of the site. He should not enter any confidential data if he is accessing a website from an external link or pop-up ad, even on a real site. Although through pharming, a genuine website can redirect a user to a malicious webpage. He should verify that the pagehe is about to put the details is genuine before doing so.
Avoid leaving financial information on the laptop	A user should not store his financial information except it is inevitable. Laptops can be easily misplaced or stolen. He should secure his laptops with passwords.
Utilize encrypted sites where necessary	Sometimes certain websites or social media may prompt a user to switch on encryption. He should go ahead and do so when prompted. A site preceded with 'https' is a secured site. Therefore, it can be trusted. The padlock icon seen in the address bar indicates that payments and logins made on it are safe.
Look for the company's email addresses	Every bank, social network, online store or other organisations usually send emails from a registered email extension to the organisation itself. They usually do not send emails from yahoo.co.uk, gmail.com, and so on. A user should not provide his personal details if the email has no connection with the organisation.
Avoid sending or receiving money on behalf of others	Saudi Arabian banks usually do not allow their customers to carry out international transactions via Internet banking services. This is because of a high rise in international fraudulent online activities. Responding to unsolicited emails requesting for funds transfer is not just an offence, but a user would be exposing his personal details to cyber fraudsters by so doing.

Report fraudulent online activities	A user should report any cybercrime or identity theft if he falls a victim of such to the appropriate authority. He should not waste any time in doing so. For more information, visit the Action Fraud site.

5.3.4. The recommendations to reduce online trafficking in Child pornography

The recommendations for the Saudi Arabian government, organisations and general public that use the internet to reduce the effect and vulnerability of online trafficking in child pornography are provided in Table 8.

Table 8: The recommendations to reduce online trafficking in Child pornography:

Recommendation	Explanation
Education	Study more about child sex trafficking. When one is more knowledgeable about child sex trafficking, one is better equipped to tackle the issue. Study books and articles, listen to experts and watch videos to be better informed about it.
Identify the Signs	It is compulsory to find out what a child trafficking victim looks like. An individual or a government that can identify what they look like can help whenever they notice any child in that situation in any public place.
Create Awareness	An individual or government personnel should create awareness of child trafficking with everyone within their sphere of contact; their family, friends, colleagues, local churches, schools close to them, local politicians or legislators. With the awareness, people will know how best to protect their children against child sex trafficking offenders.
Act	People should take a stand against child sex trafficking. They should become strong promoters against child sex trafficking. They should tell everyone within their contact about the issue. They should write letters and articles to the newspaper editors within their locality and politicians. They should participate actively in anti-trafficking efforts within their locality, in their city and community.

5.3.5. The recommendations to reduce the types of malicious codes

The recommendations for the Saudi Arabian government, organisations and general public who use the internet to reduce the effect and vulnerability to types of malicious codes are provided in table 9.

Table 9: The recommendations to reduce the types of malicious codes

Recommendation	Explanation
Install quality antivirus	Many computer users are comfortable with using free antivirus applications that usually comes with a bundled service offering purchased from an Internet service provider. What they do not know is that such antivirus cannot adequately protect their computers from the rising threats of virus or spyware infections. It is more advisable for users of Windows to install professional, business-grade antivirus software on their computers. Antivirus programs like Pro-grade frequently update throughout the day. That way, the computers are protected against the ever-growing threats of viruses, spyware, malware, rootkits and enable more protective features such as custom scans.
Install real-time anti-spyware protection	A good number of computer users have this erroneous belief that installing one antivirus program that has spyware protection incorporated in it adequately protects computers against spyware and adware. Some others believe free anti-spyware applications with antivirus utility incorporated in it can sufficiently protect against the soaring number of threats from spyware.
Use the latest versions of anti-malware applications	A computer is adequately protected against the latest threats only when the antivirus and antispyware are updated regularly. According to statistics antivirus provider, AVG released in early 2009; it was revealed that majority of devastating computer threats are fast moving and usually discreet. Although the infections do not last long, notwithstanding, they approximately infect between 100,000 to 300,000 new websites daily.
Carry out daily scans	Virus and spyware threats can sometimes evade a computer's security and infect it. This is possible because of the fast-growing number and potentials of new threats. It will make it easy to outsmart security software. In some cases, some computer users may unwittingly permit the running of a virus or spyware program. Regular scanning of the entire hard drive of a system is helpful in detecting, isolating and deleting infectious threats that were not initially detected by the computer's security program.
Disable autorun	Many viruses operate by simply joining themselves to a drive and installing themselves automatically on any media connected to the system. The threats can easily spread once contact is made by an external drive, network drives

	or even thumb drive. To avoid this, disable autorun feature on Windows, using recommendations from Microsoft which varies from one system to another.
Do not click on email links or attachments	The warning on not clicking on email links or attachments has been on for a long time and yet, quite often, many computer users do not listen to the warning. Irrespective of the source of the email, it is unwise to click on links and attachments included in email messages. This could expose the computer of infections which could in turn destroy critical information. Before clicking on email attachments, first, scan them for viruses with a business class antimalware application. Instead of clicking on links, go to websites rather, open a new browser and navigate to the site in question manually.
Surf smart	Most of the business-class anti-malware applications have browser plug-ins for securing drive-by against infections, phishing attacks and similar exploits. Some others protect the links by running a check on them against databases of blacklisted web pages.
Use a hardware-based firewall	The advantages of software over hardware-based firewalls have been argued by some technology experts. Some computer users sometimes are faced with difficulties in sharing printers, accessing network resources, carrying out other tasks when using software-based firewalls from third parties. This sometimes results in totally disabling firewalls altogether.
Deploy DNS protection	The use of the Internet makes it possible for computers to be prone to many security threats. A computer can be infected simply by a user visiting a compromised website. An infected computer exposes other users connected to it to malicious threats. Websites that spread infected applications, programs and Trojan files also constitutes a great concern. Poisoned DNS attacks also constitute a great threat. A poisoned DNS service has the capacity or redirecting a user to a fraudulent web server

5.4. Summary

The recommendations provided in this chapter can be followed and implemented to reduce the vulnerability to the exposure of cybercrime and can be used to reduce the impact of cybercrime in Saudi

Arabia. However, the work should be done not just by the government but also by the general public and private sectors.

Chapter 6: Conclusion and Future works

6.1. Introduction

This chapter provides the conclusion, future works, time plan, Gantt chart and risk table.

6.2. Conclusion

Cybercrime across the globe has become a major phenomenon with difficulty in prevention and reduction, together with rising vulnerability of the different kinds of internet users. Saudi Arabia has become the number one target of cybercrime in the Middle East (Elnaim, 2013). It is noted from the primary research conducted that the people in Saudi Arabia are not aware of the cybercrimes. Therefore, this project provides the recommendation to the people that use the internet, government and organisation in Saudi Arabia and also offer recommendations on how to minimise the impact of cybercrime as well as to reduce the exposure to the cybercrime threat which are intellectual property crimes, online trafficking in child pornography, online theft, hacking, and malicious codes, using the secondary and primary research.

6.3. Future works

The suggested future work for this project are listed below:

- The interview and survey should involve more participants to get a more accurate results
- The focus group should be organised to get some detailed information regarding the questions

6.4. Risk Table

Table 10: Risk table

Risk	**Impact**	**How to minimise the risk**
Getting responses to the survey	High	Share the online survey link using social media like Facebook, Twitter and so on.
Not meeting the deadline	High	The strict schedule was planned and maintained.
System fault	Medium	Have a regular backup of the report online using google drive.

Illness	Low	Intent to finish the project before the time to avoid any unexpected delays.
Access to materials	Low	Google scholar and the university library were used to get the journals and other materials.

6.5. Project Plan

Table 11: Project plan

Task Name	**Start**	**End**	**Duration (days)**
Secondary Research	6/1/2017	6/15/2017	14
Primary Research - Interview	6/5/2017	6/30/2017	25
Primary Research - Survey	6/5/2017	6/30/2017	25
Report Writeup - Introduction	6/16/2017	6/18/2017	2
Report Write-up - Literature Review	6/19/2017	7/15/2017	26
Report Write-up - Methodology	7/16/2017	7/30/2017	14
Report Write-up - Survey Analysis	8/10/2017	8/14/2017	4
Report Write-up - Interview Analysis	8/15/2017	8/19/2017	4
Report Writeup - Discussion	8/20/2017	8/24/2017	4
Report Writeup - Recommendation	8/25/2017	8/30/2017	5
Report Write-up - Conclusion and Future works	9/1/2017	9/5/2017	4
Report Proofreading	9/5/2017	9/10/2017	5
Presentation	8/20/2017	9/4/2017	15

6.6. Gantt Chart

See Appendix A for the Gantt Chart

Reference

Al Amro, S., 2017. Cybercrime in Saudi Arabia: fact or fiction?. International Journal of Computer Science Issues (IJCSI), 14(2), p.36.

Alahtani, F.S. (2015). Saudi Anti-Cybercrime Law of 2007 (A Comparative Study with the UAE Combating Cybercrimes Law of 2006 Amended 2012). Retrieved from http://repository.nauss.edu.sa/bitstream/handle/123456789/62862/The%20Saudi%20Anti-Cybercrime%20Law%20of%202007.pdf?sequence=1

Alanezi, F. (2015). Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions. An unpublished thesis at the Brunel University. Retrieved from http://bura.brunel.ac.uk/bitstream/2438/12003/1/FulltextThesis.pdf

Algarni, A. F. (2013). Policing Internet fraud in Saudi Arabia: expressive gestures or adaptive strategies? *Policing and Society*, *23*(4), 498-515.

Algarni, A.F. (2012). Policing Internet Fraud in Saudi Arabia: The Mediation of Risk in a Theocratic Society. Retrieved from https://hydra.hull.ac.uk/assets/hull:13584a/content

Al-Kadhi, M. A. (2011). Assessment of the status of spam in the Kingdom of Saudi Arabia. *Journal of King Saud University-Computer and Information Sciences*, *23*(2), 45-58.

Almerdas, S. (2014). The criminalisation of identity theft under the Saudi Anti-Cybercrime Law 2007. Journal of International Commercial Law and Technology, 9(2), 80-93.

Al-Murjan, A., & Xynos, K. (2008, January). Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case. In Proceedings of the Conference on Digital Forensics, Security and Law (p. 15). Association of Digital Forensics, Security and Law. Retrieved from http://commons.erau.edu/cgi/viewcontent.cgi?article=1065&context=adfsl

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016, December). A survey of cyber-security awareness in Saudi Arabia.In: 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016 (pp. 154-158).

Al-Sanea, M.S., & Al-Daraiseh, A.A. (2015, November). Security evaluation of Saudi Arabia's websites using open source tools. In Anti-Cybercrime (ICACC), 2015 First International Conference on (pp. 1-5).

Al-Zahrani, A. M. (2015). Cyberbullying among Saudi's Higher-Education Students: Implications for Educators and Policymakers. *World Journal of Education*, *5*(3), 15-26.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg.

Arab News (August 4, 2015). Saudi arrested for hacking govt site. Retrieved from http://www.arabnews.com/saudi-arabia/news/786301

Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Bronk, C. and Tikk-Ringas, E., 2013. The cyber attack on Saudi Aramco. Survival, 55(2), pp.81-96.

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival, 55*(2), 81-96.

Chan, S. (December 1, 2016). Cyberattacks Strike Saudi Arabia, Harming Aviation Agency. Retrieved from https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html?_r=0

Das, S., & Nayak, T. (2013). Impact of cyber crime: issues and challenges. International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142-153.

Den Hengst, M., & Warnier, M. (2013). Cyber Crime in Privately Held Information Systems. In Intelligence and Security Informatics Conference (EISIC), 2013 European (pp. 117-120).

Electrony.net. (2012). Cybercrimes cost the kingdom 2.6 billion Saudi riyals. [online] Available at: https://goo.gl/gnCHe4 [Accessed 1 Sep. 2017].

El-Guindy, M. N. (2008). Cybercrime in the Middle East. *ISSA Journal, June* (2008), 16-19.

Elnaim, B.M.E. (2013). Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. *Information and Knowledge Management, 3*(12), 14-19.

Elnaim, B.M.E., 2013. Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. In Information and Knowledge Management(Vol. 3, No. 12, pp. 14-19).

Gilden, A. (2013). Cyberbullying and the innocence narrative. Browser Download This Paper. Retrieved from http://harvardcrcl.org/wp-content/uploads/2011/09/CRCL_Gilden_print-version.pdf

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology, 2(7), 626-631.

Higgins, George E., Catherine D. Marcum, Tina L. Freiburger, and Melissa L. Ricketts (2012). Examining the Role of Peer Influence and Self-Control on Downloading Behavior. Deviant Behavior 33(5), 412–423.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35(1), 20-40.

Jha, N.K. (2008). *Research methodology*. Chandigarh, India: Abhishek Publications.

Kaboub, F. (2012). Postivist Paradigm. Retrieved from http://personal.denison.edu/~kaboubf/Pub/2008-Positivist-Paradigm.pdf

Khan, N. K. (2012). Taxonomy of Cyber Crimes and Legislation in Saudi Arabia. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1*(8), 207-209.

Kothari, C. R. (2004). *Research methodology: methods & techniques.* New Delhi: New Age International (P) Ltd.

Kuada, J.E. (2012). *Research Methodology: A Project Guide for University Students (1st ed.).* Frederiksberg C, Denmark: Samfundslitteratur Press.

Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. European Journal of Criminology, 12(2), 226-241.

Manky, D. (2013). Cybercrime as a service: a very modern business. Computer Fraud & Security, 2013(6), 9-13.

Ministry of Justice (2012). Retrieved from http://www.moj.gov.sa/adl/ENG/attach/28.pdf

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. Children and Youth Services Review, 34(1), 63-70.

Neufeld, D. J. (2010, January). Understanding cybercrime. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* (pp. 1-10).

Rajkhan, S.F. (2014). Women in Saudi Arabia Status, Rights, and Limitations. Retrieved from https://digital.lib.washington.edu/researchworks/bitstream/handle/1773/25576/Rajkhan%20-%20Capstone.pdf?sequence=1

Redford, M. (2011, September). US and EU Legislation on Cybercrime. In Intelligence and Security Informatics Conference (EISIC), 2011 European (pp. 34-37).

Robson, C., & McCartan, K. (2016). Real world research: a resource for users of social research methods in applied settings (4th ed.). Chichester, West Sussex, United Kingdom: Wiley.

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. Digital Investigation, 14, 36-45.

Simpson, B. (2015). Sexting, digital dissent and narratives of innocence–controlling the child's body. Sociological Studies of Children and Youth, 19, 315-349.

Steinmetz, G. (2005). Positivism and its others in the social sciences. In G., Steinmetz (Ed.), The Politics of Method in the Human Sciences: Positivism and Its Epistemological Others. Durham, NC: Duke University Press: 1–56.

Sturges, P. (2015). Regulating the press: Ensuring responsibility, or road to censorship. Retrieved from http://www.beaconforfreedom.org/liste.html?tid=415&art_id=613

Wall, D.S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. The European Review of Organised crime, 2(2), 71-90.

Yar, M. (2013). Cybercrime and society (2nd ed.). Los Angeles: Sage.

APPENDIX A: Gantt Chart

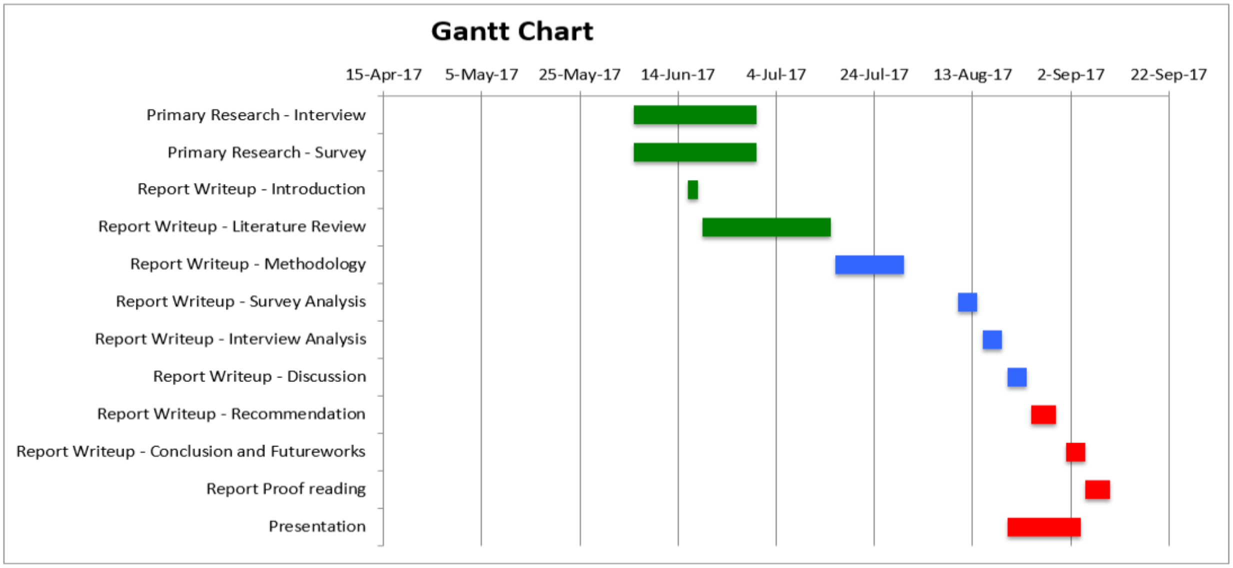


Figure 2: Gantt Chart

APPENDIX B: Ethics Certificate

APPENDIX C: Justification for the research questions

Research question 1: What are the types of Cybercrime available?

This question was answered by the secondary research. Several journals provide their categorisation for the types of Cybercrime. However, after the critical analysis, this project will provide the final suggestions for the types of cybercrimes in Saudi Arabia

Research question 2: What are the laws that govern the cybercrime issues in Saudi Arabia?

The current laws and policies in Saudi Arabia will be studied to identify the strengths and weaknesses in the law and suggest suitable amendments to it.

Research question 3: What kind of impacts of cybercrime are identified in the literature already?

The secondary research is used to identify the impact of cybercrimes in Saudi Arabia that is addressed in the literature. However, the impacts are also studied using primary research to critically evaluate the literature with the primary research conducted for this project.

Research question 4: Which kind of impact from the experiences of end-users in Saudi Arabia?

This question directly answers the aim of this question. It enables the collection of information from end-users to determine the kind of impact they feel or have had from cybercrime perpetration. The vulnerability and the types of cybercrimes will be used to form data collection instruments that will provide real-time information concerning how the end users should cope and deal with cybercrime.

On the other hand, it will provide experiential details of the variation in terms of the impacts that are attached to internet crimes. This question should further extend the understanding of the impact that each type of cybercrime can have on end-users. The only difficulty identified with answering this question is the reluctance of participation, based on cultural or individual reasons.

Research question 5: What is the opinion of cybercrime in Saudi Arabian internet use?

The answer to this question was derived from the primary research which includes interview and survey.

Research question 6: What is the level of cybercrime perpetration in terms of technology and targets in Saudi Arabia?

This question is focused on discovering the degree at which cybercrimes are being conducted in Saudi Arabia. This question is concerned with understanding the overall cybercrime industry in Saudi Arabia.

It is important to understanding the kind of technology, targets and mode of operation being adopted by cybercriminals. The question will provide an intricate understanding of the role of the internet, and the means through which these crimes are committed.

Furthermore, the answer to this question provides huge background information that showcases the details of cybercrime in Saudi Arabia. It is a theoretically based research in which previous research findings and scholarly articles will be used to elaborate on cybercrime perpetration in the industry. The question will provide details concerning the sources of cybercrime, whether it is in Saudi Arabia or from other countries.

In answering this question, it is possible to present high level of technical information based on the experience of the researcher, without explaining the user-oriented perspective. Another potential obstacle is the lack of research materials, and government published data that can give the current situation of cybercrime in Saudi Arabia.

Research question 7: What is the level of vulnerability of end-users to cybercrime in Saudi Arabia?

This question is important because it enables the exploration of risks attached to users in the Saudi cyberspace. This will enable the understanding of the types of protection and the possibility of becoming a victim of cybercrime for users. It will provide an in-depth understanding of the impact of governance, user awareness and prevalence of this crime concerning users.

It will allow the matching of cybercrime types with the various risks existing for internet users in Saudi Arabia. Different sectors online and the level of risks they are exposed to will be explored. It will enable the understanding of the risks attached to a different aspect of usage including e-commerce, communication, electronic banking, social media amongst others.

Research question 8: What are the recommendations to minimise the exposure to cybercrime?

The recommendations are derived using the primary research and secondary research conducted.

Research question 9: What are the recommendations to minimise the impact of cybercrime?

The recommendations are derived using the primary research and secondary research conducted.

APPENDIX D: Survey and Interview questions for the general public in Saudi Arabia that use the internet

1. What is your gender?
2. What is your age range?
3. What is your work sector?
4. Do you use the internet?
5. On a scale of 1-5, how much do you know about cybercrime?
6. Where you a victim of cybercrime in your life before?
7. Have you heard of someone who has been a victim of a cybercrime?
8. Have you seen anything on the news about people being harassed online?
9. Do you have an idea what is online theft is?
10. If yes, specify the types of online thefts that are more harmful in Saudi Arabia.
11. Do you have an idea of what hacking is?
12. If yes, specify the types of hacking that are more harmful in Saudi Arabia.
13. Do you have an idea on what malicious code is?
14. If yes, specify the types of malicious codes that are more harmful in Saudi Arabia.
15. Do you have an idea on what Illegal interception of computer data is?
16. If yes, specify the types of Illegal interception of computer data that are more harmful in Saudi Arabia.
17. Do you have an idea on what an online commission of intellectual property crimes is?
18. If yes, specify the types of the online commission of intellectual property crimes that are more harmful in Saudi Arabia.
19. Do you have an idea on what online trafficking in child pornography is?
20. If yes, specify the types of online trafficking in child pornography that are more harmful in Saudi Arabia.
21. Do you have an idea on what Intentional damage to computer systems or data is?
22. If yes, specify the types of Intentional damage to computer systems or data that are more harmful in Saudi Arabia.
23. Does your country have a current Policy on cybercrime?
24. If yes, please list the policies.
25. Suggested steps that users should adapt to prevent online identity theft
26. Suggested steps that users should adapt to prevent hacking

27. Suggested steps that users should adapt to prevent malicious code
28. Suggested steps that users should adapt to prevent Illegal interception of computer data
29. Suggested steps that users should adapt to prevent the online commission of intellectual property crimes
30. Suggested steps that users should adopt to online trafficking in child pornography
31. Suggested steps that users should adapt to prevent Intentional damage to computer systems or data.

APPENDIX E: Survey and Interview questions for people who have insights regarding the security and its issues in Saudi Arabia

1. What is your gender?
2. What is the age range?
3. Are you working in IT and Security related sector?
4. On a scale of 1-5, how much do you know about cybercrime?
5. Where you a victim of cybercrime in your life before?
6. Have you heard of someone who has been a victim of a cybercrime?
7. Have you seen anything on the news about people being harassed online?
8. Provide appropriate online thefts that are more harmful in Saudi Arabia.
9. Provide appropriate hacking that is more harmful in Saudi Arabia.
10. Provide appropriate malicious codes that are more harmful in Saudi Arabia.
11. Provide appropriate Illegal interception of computer data that are more harmful in Saudi Arabia.
12. Provide appropriate online commission of intellectual property crimes that are more harmful in Saudi Arabia.
13. Provide appropriate online trafficking in child pornography that is more harmful to Saudi Arabia.
14. Provide appropriate Intentional damage to computer systems or data that is more harmful to Saudi Arabia.
15. Provide an appropriate list of the policies.
16. Does Saudi Arabia have experience in strengthening the relationship between authorities responsible for investigating cyber-crimes and internet service providers that may be shared with other States as a best practice in this area?
17. If yes, please explain.
18. Has Saudi Arabia established a unit to monitor and stop cybercrime issues?
19. If yes can you please explain?
20. Has Saudi Arabia established a unit to monitor and stop cybercrime prosecution?
21. If yes can you please explain?
22. Suggested steps that users should adapt to prevent online identity theft
23. Suggested steps that users should adapt to prevent hacking
24. Suggested steps that users should adapt to prevent malicious code

25. Suggested steps that users should adapt to prevent Illegal interception of computer data
26. The suggested step that users should adapt to prevent the online commission of intellectual property crimes
27. Suggested steps that users should adopt to online trafficking in child pornography
28. Suggested steps that users should adapt to prevent Intentional damage to computer systems or data
29. Suggested steps that the private and public (government) organisations should adopt to prevent online identity theft
30. Suggested steps that the private and public (government) organisations should adopt in hacking
31. Suggested steps that the private and public (government) organisations should adopt in malicious code
32. Suggested steps that the private and public (government) organisations should adopt in Illegal interception of computer data
33. Suggested steps that the private and public (government) organisations should adopt an online commission of intellectual property crimes
34. Suggested steps that the private and public (government) organisations should adopt in online trafficking of child pornography
35. Suggested steps that the private and public (government) organisations should adopt in Intentional damage to computer systems or data