The Extent to which Individuals in Saudi Arabia are Subjected to Cyber-Attacks and Countermeasures

Abdullah A H Alzahrani[1]
Computer Science Dept. Computing College at Alqunfuda
Umm Al Qura University, Makkah, Saudi Arabia

***Abstract*—In light of the rapid development of technology and the increase in the number of users of the Internet via computers and smart devices, cybercrimes impact on enterprises, organizations, governments and individuals has been significant. Researches and reports on the impact of cybercrime and methods of prevention and protection are been introduced regularly. However, the majority focuses on the impact on organizations and governments. This paper aims to use a survey methodology in order to highlights the impact of cybercrimes on the individuals in Saudi Arabia and measure the awareness of cybersecurity among individuals. In addition, this research aims to investigate the common cybercrimes which target the individuals in Saudi Arabia and the countermeasure taken by them.**

Keywords*—Cybercrimes; cybersecurity; identity theft; cyberattacks

I. Introduction

Cybersecurity can be defined as a prevention, protection, and restoration of information technology and data to ensure the availability, integrity, and confidentiality [1] – [3] while, Cybercrime is any crime that is committed using the Internet, for example, by stealing a person's personal or banking data or by infecting their computer with a virus [4]. A number of cybercrimes are widely addressed such as Identity theft, online shopping fraud, and phishing [5]. These crimes cost the individuals and organizations annually a high amount of money.

According to Cybint Solutions 2019 [6] [1] "It is expected that approximately $ 6 trillion will be spent globally on cybersecurity by 2021". This number highlights the importance of cybersecurity and issue of cybercrimes. This is due to the increasing number of cyberattacks and the more complicated they become. However, it is difficult to estimate the annual expenditure of an individual of cybercrimes [5].

This research focuses on the impact of cybercrimes on individuals in Saudi Arabia. Therefore, it is important to highlight the cybersecurity issues in this region. in 2017, around 12000 incidents of cyber-related were reported. While, it is estimated that the number of Internet users is around 27 million users of in Saudi Arabia [7]. Alongside with the aforementioned widely addressed cybercrimes, Communication and Information Technology Commission in Saudi Arabia pointed out a number of other cybercrimes in Saudi Arabia these are blackmailing, Privacy violation, and Unethical content [7].

According to McAfee Security Report 2014 [8] "In 2014, cyberattacks cost the kingdom of Saudi Arabia about 4 billion riyals, or about 0.17% of GDP (Gross domestic products)". However, this percentage is less than the acceptable percentage which is 2% of GDP. This makes Saudi Arabia in a non-alarming area of cybercrimes.

According to National Cyber Security Center (NCSC) in Saudi Arabia, in 2018 the threat alerts was higher by (13.5 %) s compared to the Fourth Quarter of 2017 [9][2]. NCSC revealed that the government and Education sectors were the main target of cyberattacks by around 71% of the attacks [9]. However, there is an insufficient of research or scientific investigation of cyberattacks on Saudi Arabia [10].

The importance of this research is derived from the fact that individuals are composing organizations. Individuals are clerks working in the terminal of the systems that are target for attacks, administrators who have high privileges on systems that are target for attacks, and technical who are working on the data of these systems. Moreover, sometimes these individuals are working on the systems from their personal devices. Therefore, neglecting investigating the impact of cyber-attacks on individuals is a gap that makes the picture of the impact of cyber-attacks incomplete. Furthermore, most of investigations (which will be shown in related work section in this paper) relies on the experts' opinions with orientation to specific domain of attacks. However, as it has been evident that individuals are the major cause of attacks [21], it is important to measure the impact of cyber-attacks on them as well as countermeasure they adopt.

In this paper, the impact of cybercrimes on individuals in Saudi Arabia is investigated. In addition, this research employs a survey methodology to collect data from individuals' respondents in order to provide an empirical result. The next section, will highlight a number of related studies. Then, research questions and research methodology will be explained in more details. Finally, the main finding of this research will be shown and discussed with some conclusions on them.

II. Related Work

Momein et al. 2010 [4] have conducted a survey based study to investigate the size and patterns of cybercrimes in Pakistan. The main findings were that the majority of

[1] https://www.cybintsolutions.com

[2] https://www.ncsc.gov.sa

cybercrimes to Internet users are related to privacy intrusion, sexual offenses, and e-commerce. The authors compared the international rate of the cybercrime impact on users with the local rate and offered several recommendations such as developing a national cybersecurity system and enforcement of a national cybercrimes law.

Bernik 2014 [11] carried out an analysis study of the organizations investment in protections from cybercrimes. The author followed a methodology that analyses a set of reports of costs of cybercrimes which are published by governments and organizations. This is to search for the actual causes of these costs. The author found that different models of calculating costs are implemented by organizations and that that the security experts are influencing the calculation processes. In addition, the author stated that the majority of the costs studies of the cybercrimes are exaggerated and unrealistic. Moreover, raising of organizational culture and awareness of protection is more efficient and inexpensive than other implementation of cybersecurity.

Riek et al. 2016 [5] believed that investigating impact of cybercrimes on individuals obtained insufficient attention with comparison to impact on organizations. The authors attributed this to those difficulties that may be encountered. Consequently, the authors have developed a survey methodology to study the costs of cybercrimes on individuals in 6 European counties. They focused on 7 different types of cybercrimes and found that Identity theft gained the highest impact on individuals in these 6 EU countries.

Kazmi et al. 2017 [12] investigated individuals' practices towards using internet banking. The research was conducted in three developing counties namely Saudi Arabia, Pakistan, and India. 1044 participants were asked to fill an online survey to measure their awareness of cybersecurity and internet banking threats. 272 participants were from Saudi Arabia. The authors found that there is a gap between the banks' expectations of individuals' practices and the individuals' actual actions. Consequently, the authors have introduced a two-part model that offers a set of security advices and instructions for the two parties (individuals – Banks).

National Cyber Security Centre (NCSC) in Saudi Arabia published a report in 2018 [9] that shows an empirical analysis of the cyber threats in Saudi Arabia. The report highlights the cyber threats for the years of 2017 and 2018. In addition, it has been noticed that the the cyber threats have increased since 2017 with 13%. As shown in Fig. 1, the majority of these threats targeted government and education sectors with percentage as 52% and 14% respectively. Furthermore, according to NCSC [9], malwares have been the observed to be the most common threats to all sectors. However, in the NCSC's report, the impact of cyber threats and attacks on the individuals was not highlighted in the investigation.

Another attempt of studying cybercrimes impact was carried out by Alelyani et al. 2018 [10]. The authors focused on the impact of cyberattacks on organizations in Saudi Arabia. In particular, the authors investigated the impact caused by Shamoon, Shamoon 2.0, and Ransomware on some well-known organizations such as Saudi Aramco. In addition, the aforementioned malwares were dissected. The authors relied on the results and solutions offered in [13]– [15] to provide a number of customized solutions and practices to be applied in the Saudi organizations. Raising awareness, heavy application of firewall, and decreasing the number of administrative accounts are the main solutions which are offered as customized solutions and practices to be applied in the Saudi organizations.

Harrell has published a series of investigations focusing on cybercrimes of identity thefts in US for years 2012, 2014, and 2016 [16] – [18]. In the latest one of investigations, the author studied the impact of identity theft on over 17.7 million persons whose data were brought from national authorities. It was found that the majority of surveyed persons have been impacted by financial losses and misuse of their data for other purposes. In addition, the majority of victims did not know how attackers collected their information. Furthermore, one out of ten of victims reported the incidents to authority. The author estimated the average financial losses of victims with 850$ and the median of 300$.

Important reports have been revealed by Symantec [19], [20] focusing on Internet Security Threat Report. In 2010, Symantec reported that an average of 260,000 identity theft or exposure is caused by a breach. In addition, although the majority of cybercrimes targeted government or organizations, individuals will be targeted in favor of identity thefts. Furthermore, Symantec estimated the individuals' financial loss associated to cybercrime with the around 100$ per year. Additionally, in 2019, Symantec revealed that more than 4,800 websites are exposed to attacks every month. Moreover, IoT (Internet of Things) devices and in particular smart phones are the favorite devices for attackers.

In conclusion, many studies have focused on the investigation of the impact of cybercrimes and attacks on governments and organizations. However, insufficient works have focused on the impact on individuals, in particular, in Saudi Arabia. In addition, the majority of these type of studies tends to offer expert opinions to mitigate the impact, whereas, a small number tends to study the actions taken by individuals against cybercrimes or attacks.

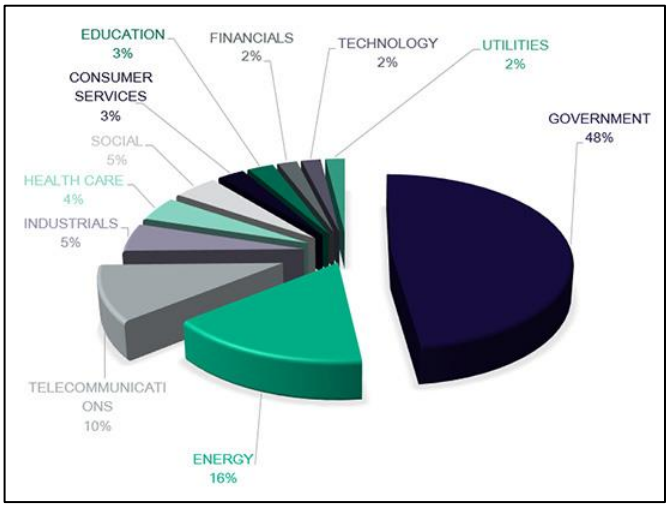

Fig. 1. Targeted Sectors According to NCSC [9].

The gap noticed is that the impact of cybercrimes on individuals in Saudi Arabia has not been sufficient covered. This includes the investigation of the actions and countermeasures which are applied by individuals in the case of cybercrime. In addition, it should highlight the matter of the individuals' knowledge of cybersecurity and protection methods. Although, the accurate estimation of the financial impact on individuals is difficult [5] in general, there has been no study that estimate a financial impact on individuals in Saudi Arabia. With all of the aforementioned, this research aims to fill this gap.

III. Research Questions

In order to achieve this research goal, three main research questions are framed. These questions are as follows:

RQ1. To what extent, is Internet network secure in Saudi Arabia? In order to answer this question, a set of factors was proposed that would imply the level of internet security in Saudi Arabia. These factors focus on knowledge of individuals of cybersecurity, and simple protection methods. Moreover, it was necessary to put some attention to the types and the use (public or private) of devices that are attacked when individuals are targeted.

RQ2. What effect does cybercrimes have on individuals in Saudi Arabia? To draw conclusion on this question, the experience of individuals with cybercrimes should be studied. This is in the light of questions focusing on the purposes of cyberattacks, recovery expenses of attacks, and attacks recurrences.

RQ3. What are the most common cybercrimes impacting individuals in Saudi Arabia and the causes of such attacks and what countermeasures are taken? To answer this question, the methods used in attacks should be investigated as well as the countermeasures against them. By carrying out such an investigation, a complete picture of the most common cybercrimes will be gained and the reactions taken by individuals will be highlighted. Therefore, respondents will be asked questions related to this as shown in the next sections.

IV. Research Methodology

Survey methodology has been adopted in this research. The survey was an online and links to it were sent to participants via emails and social media. This methodology is useful for gaining opinions from large number of respondents in Saudi Arabia. Thus, this study recruited 629 participants who are from different province, gender, qualification level, and work sector (public and private). The survey was divided into five main sections. The first section is intended to obtain the consent of participation and to gather some general information such as the province, gender, qualification level, and work sector.

The second section aims to identify the level of knowledge of participants in cybersecurity related topics. The third section focuses on measuring respondents' knowledge of cybersecurity related institutes and organizations in Saudi Arabia. Furthermore, it focuses on measuring their previous responses to these organizations, in addition to, their knowledge of the Cybercrime System in Saudi Arabia.

The fourth section is the main part of the survey and consists of 7 questions. These questions are to investigate the extent of effect of cybercrimes on individuals in Saudi Arabia. The questions cover the methods used in attacks, purposes of attacks, recovery expenses of attacks and countermeasures, and attacks recurrences. The fifth section focuses on the countermeasures taken by individuals when attacks occur. In addition, it uncovers the reactions of individuals towards attacks consequences.

Survey methodology has been adopted in this study in order to allow reaching an extensive number of respondents as fast as possible. In addition, a variety of tool supporting designing and spreading surveys are available such as Google Docs which has been used in this research. This allows conducting the research with cost efficiency and effectiveness.

The survey questionnaire was distributed online via emails and social media to 1000 respondents out of which 629 participated in the study and completed the questionnaire. The response rate of the survey is 61.9%. The participants of this research are individuals from Saudi Arabia who are using devices connected to the Internet. Out of the 629 participants, 70% are male and 30% are female. In addition, different levels of qualifications were noticed. The majority of the participants (50.40%) have Bachelor degree, while 33.23% are Postgraduate, 8.27% are High school diploma, 5.88% are Higher Diploma, and 2.23% hold Others education certificates.

The questionnaires were distributed to all of Saudi Arabia provinces. Participants were from all of the provinces as 63.59% of participants were from Makkah province, 13.99% were from Riyadh, 6.52% were from Eastern Province, 4.29% were from Madinah, 3.34% were from Asir, 2.23% were from Baha, 1.59% were from Jizan, 1.59% were from Tabuk, 0.95% were from Qassim, 0.64% were from Najran, 0.64% were from Northern Borders, 0.48% were from AlJawf, 0.16% were from Hail.

The majority of participants are employees who are working in both Government and Private sector as 69.79% are working Government sector and 13.51% are working Private sector. However, 16.69% of participants in this study stated that they are in Others sector of work. These might be students or unemployed people Finally, the ethical principles of research were followed in conducting the research keeping in mind the respect of the individual privacy and identity. Moreover, all data collected was for research purposes use only and participants were informed about this.

V. Results and Discussion

In this section, the results and their interpretation will be given. First the investigation results of the security of Internet in Saudi Arabia will be shown and discussed. Second, the results of the extent of effect of cybercrimes on individuals in Saudi Arabia will be illustrated and interpreted. Finally, the most common attacks and countermeasures of individuals in Saudi Arabia will be presented and discussed. This section aims to answer the research questions mentioned previously in this paper.

A. Security of Internet in Saudi Arabia

In order to study the effect of cybercrimes on individuals in Saudi Arabia, it is important to consider the security of the Internet in Saudi Arabia. In this research, it is not intended to evaluate technically the security of Internet in Saudi Arabia, rather than evaluating deductively from the users. Therefore, first, respondents were asked to express their thought of the Internet security in Saudi Arabia. As can be seen in Fig. 1 around 90% of Internet users believe that Internet is not secure. This result highlights the next question which draw attention on the knowledge of the users of cybersecurity, cybercrimes, and protection methods.

From Fig. 2, it is obvious that users have more knowledge in cybercrimes. However, they seem to know less about cybersecurity. Relatedly, increasing ignorance in protection methods can use to protect their devices and accounts from cybercrimes. Furthermore, surprisingly, around 65% of the respondents indicate very limited to limited knowledge in protection methods.

Protection method gives knowledge to probing practical questions. Therefore, respondents were asked about the basic methods of protection on their device and accounts. The focus was on the method of using Antivirus and regular change of passwords. Surprisingly, as shown in Fig. 3, around 60% of the respondents are not using an antivirus software. By having this practice, it can be understood that a considerable number of devices of individuals are exposed to attacks.

Moreover, Kazmi et. al. [12] described that a good practice of changing password is once every 3 months. However, Fig. 4 illustrates that 18% of respondents apply this practical method of protection. This leaves the majority of 82% jeopardizing their security in a simple way. Most importantly, is to highlight the high present of 43% of respondents are in an extreme risk of attacks as they never change their passwords.

Finally, with this result, it can be deduced that there is a considerable chance of attacks risks on individual's devices. However, the question of security of Internet network in Saudi Arabia rises. It can be concluded that security of Internet network in Saudi Arabia is competent. As with this results showing low level of individuals' knowledge of protection methods, around 67% of participants in this research have not experience cyberattacks. This will be illustrated and discussed more in the next section which focus on the extent of cyberattacks' effect on individuals.

B. Extent of Cybercrimes' effect on Individuals in Saudi Arabia

In this section, extent of cyberattacks' effect on individuals in Saudi Arabia will be illustrated and discussed. This will include the focus on respondents' experience with cyberattacks, knowledge of affected respondents of cybersecurity, purposes behind attacks, attacks recurrences, devices affected, and expenses related to cybersecurity.

It is essential to link results with each another. Therefore, in the previous section, the security level of Internet in Saudi Arabia was considered and it was concluded that it is competent level. This result was based on the low level of individual respondents' knowledge of cybersecurity and the high number of respondents who have not experienced cyberattacks. Fig. 5 illustrates that only 33% of respondents have experienced cyberattacks with around 14% of them are sure it was an attack and not only a device crash.

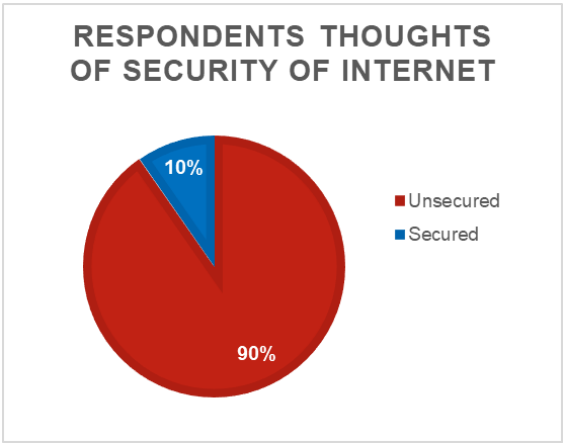

Fig. 2. Respondents thoughts of Security of Internet.

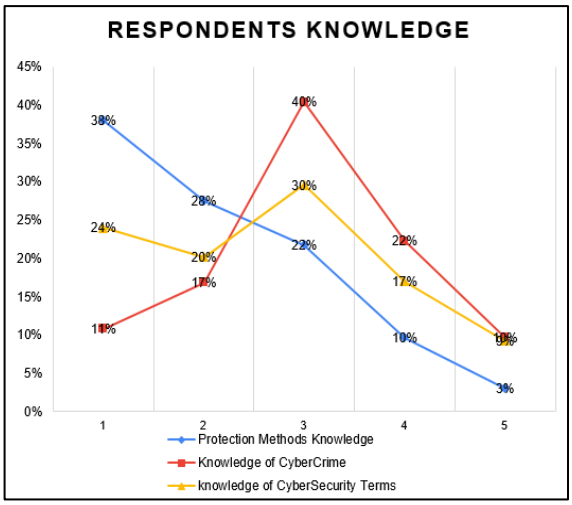

Fig. 3. Respondents Knowledge.

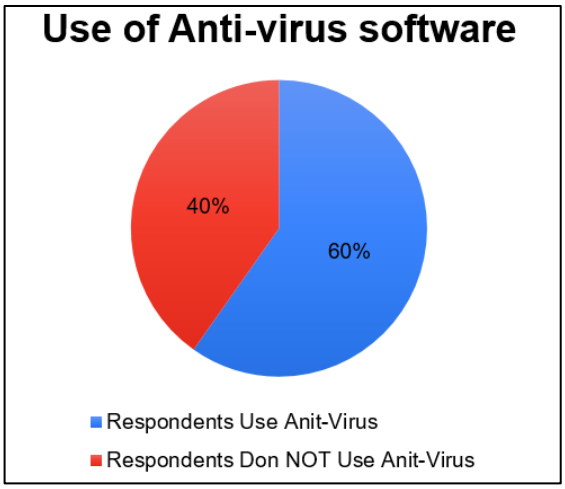

Fig. 4. Use of Anti-Virus Software.

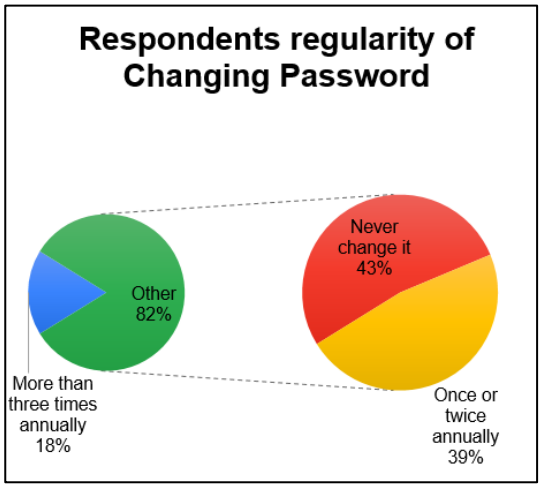

Fig. 5. Regularity of Changing Password.

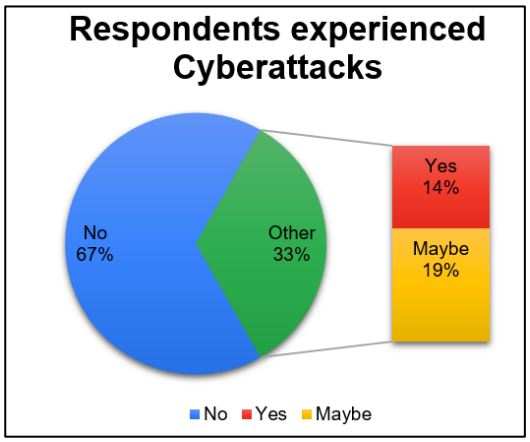

Fig. 6. Respondents Affected by Cyberattacks.

However, when it is about security, hesitated answers should be taking serious are attacks or threats, especially with the results of low knowledge of cybersecurity that is shown in the results previously. Therefore, in this research, affected respondents' percentage was determined to be 33% of total of 211 participants.

In order to investigate the extent of cyberattacks effects on individuals and to give a sharper focus to the study, the responses of affected people were separated. This is starting from the knowledge of this group of respondents in cybersecurity, cybercrimes, and protection methods. The results in Fig. 6 shows a similar result of the overall investigation results on the whole group of respondents as shown in Fig. 2. It seems that around 65% of the affected respondents of cyberattacks indicate very limited to limited knowledge in protection methods. This is along with the results that show users have more knowledge in cybercrimes, however, they seem to know less about cybersecurity.

It is reasonable to questions the clear effect cyberattacks had on the effected people. Fig. 7 illustrated that around 80% of affected respondents of cyberattacks in the study had their attitude toward using the Internet changed. They become more cautious and careful. This can be seen in Fig. 8 as 60% of them have not been attacked again. Importantly to notice in Fig. 8 is that 19% have been attacked again with different approach and for different purpose. This means that attackers either are seeking for different ways of attacks or new attackers with new approaches are introduced in the field.

In order to have sufficient information on the cyberattacks frequency or recurrence, effected respondents were asked to range the cyberattacks frequency for the past 5 years. Fig. 9 illustrates that 67% have been attacked less than 10 times. From such a result, it can be concluded here that the maximum 10 cyberattacks are impacting individuals. However, a considerable percentage of 22% are not sure about the number of times they have been attacked. This might be related to their low level of knowledge about the concepts cybercrimes and cybersecurity.

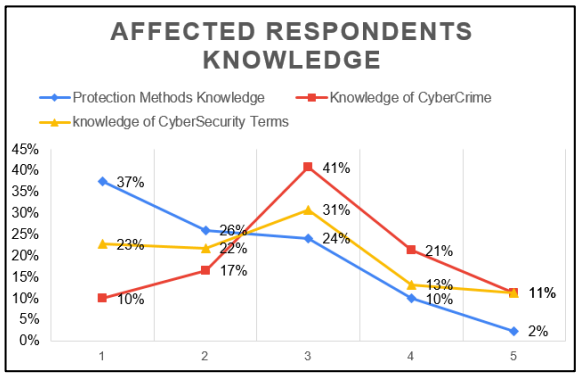

Fig. 7. Affected Respondents Knowledge.

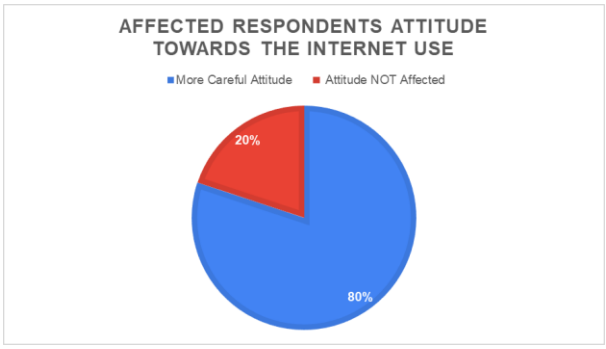

Fig. 8. Affected Respondents Attitude Towards the Internet use.

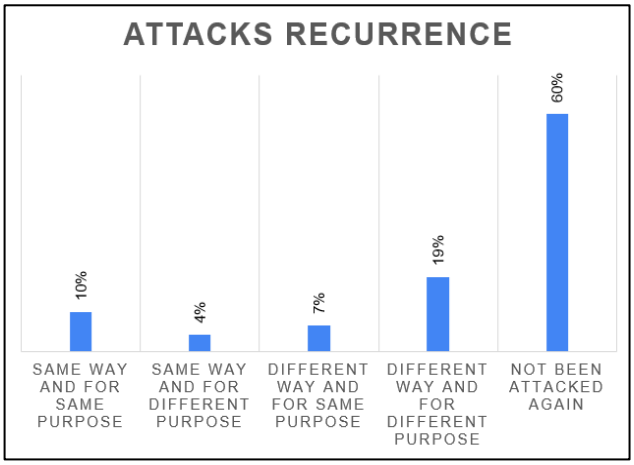

Fig. 9. Attacks Recurrence.

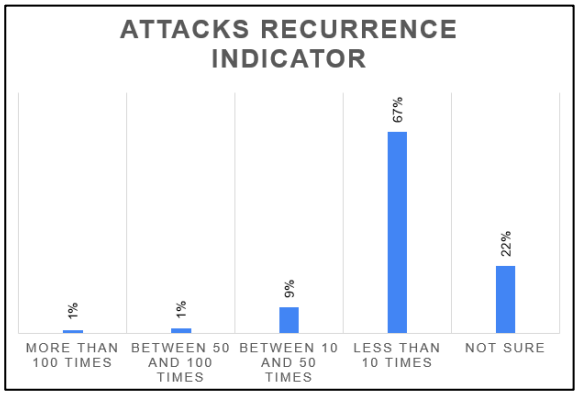

Fig. 10. Attacks Recurrence Indicator.

Investigating the knowledge, attitude after experiencing a cyberattacks, and and the frequency of attacks, leading the investigation towards the purposes of these attacks. Therefore, three categories of purposes were introduced to participants who are affected by cyberattacks. these categories are as follows: 1) identity theft; 2) blackmailing and money transfer; 3) damaging the devices and data. In addition, respondents were allowed to address their own interpretation of attacks purposes. However, an analysis of responses was conducted to check the respondents' entries to those aforementioned categories. The results of the analysis allow linking respondents' entries to those aforementioned categories.

From Fig. 10, it can be seen that around 42% of attacks are related to identity theft. This can be linked to possibility that attackers would use individuals as a breach to attack Saudi government sector, as a report published in [9] shows that 57% of attacks on Saudi network targeted government sector. Another possibility is that as Saudi Arabia is considered to be a wealthy country, identity theft would allow attackers to access and steal money. In addition, Fig. 10 illustrates that cyber-blackmailing gained a considerable amount of attention from attackers with that 29% of attacks experiences were linked to cyber-blackmailing.

Devices connected to Internet vary at the present. It is important to investigate the attacks are targeting which devices and whether these devices are for public or private use. Therefore, respondents experienced cyberattacks were asked to address the usual type and the purpose devices when attacks occur. From Fig. 11, it can be seen that around 51% of cyberattacks were experienced on Smart phones, however, closely 47% were experienced on computers. This is along with 90% of these devices are for private use as shown in Fig. 12.

Having 90% of cyberattacks on private devices leads to the question of individuals' expenditure on cybersecurity which means all spending on assurance of security such as antivirus software license etc. In addition, expenditure on cybersecurity can include dealing or recovering costs of cyberattacks. By addressing cybersecurity and expenses, it is reasonable to allow all respondents to participate in ranging their spending on it.

In this research, annual basis was opted. Therefore, respondents were offered three main categories of expenditure as follows: 1) Less than 500 Saudi Riyal; 2) Between 500 and 2500 Saudi Riyal; 3) More than 2500 Saudi Riyal. Fig. 13 shows that 64% of respondents spend maximum of 500 Saudi Riyal. This comes to equality of around 134$ (US dollar).

In conclusion, the main findings of the effects of cybercrimes on surveyed individuals in Saudi Arabia can be summarized as 33% of surveyed individuals have experienced cyberattacks on their private use smart phones or computers. In addition, the dominant cybercrime is Identity Theft with 42% of respondents. Although, the majority of 65% of attacked individuals have limited to very limited knowledge of protection methods, 60% of the attacked individuals have not experienced cyberattacks again, whereas 19% of them have been attacked again with different ways of attacks and different purposes of cybercrimes. In addition, 67% of surveyed effected respondents articulated that they have experienced cyberattacks less than 10 times. Finally, 64% of all surveyed individuals spend less or equal 500 Saudi Riyal (134$ US dollar) annually for cybersecurity reasons.

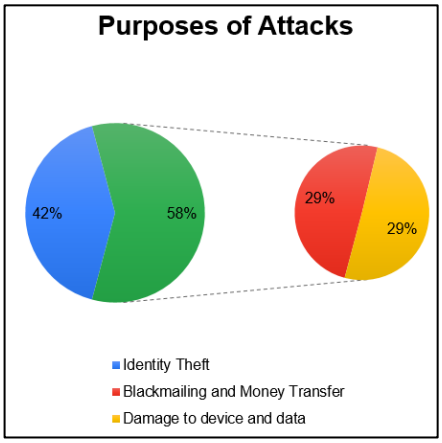

Fig. 11. Purposes of Attacks.

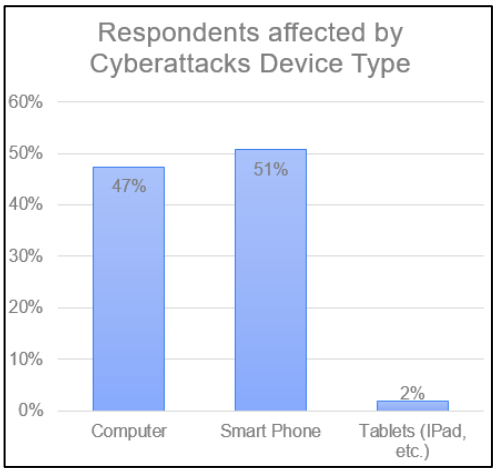

Fig. 12. Device Type.

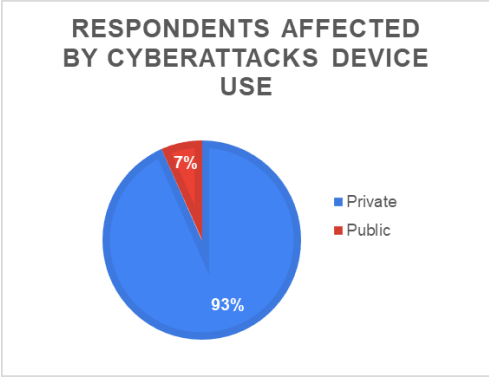

Fig. 13. Device use.

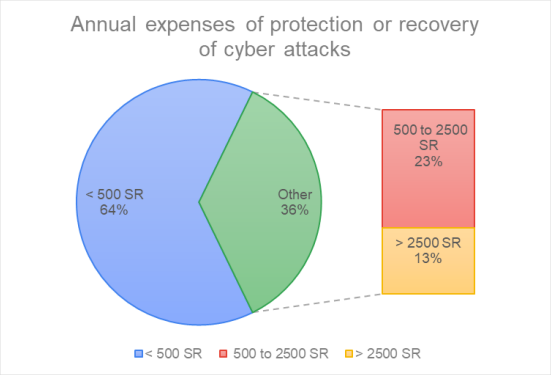

Fig. 14. Annual Expenses.

C. Most Common Cyberattacks Methods on Individuals

In this section, most common cyberattacks types on individuals will be investigated and discussed. In addition, reactions or countermeasures taken by the individuals will be studied. Finally, the linkage of each reaction to the attack methods will be made and discussed. This is to have a general view of the common cyberattacks types and the individuals' reactions and their priority to them.

First, Effected individuals have been asked to state the methods attackers used to them. From surveyed individuals' responses shown in Fig. 14, it can be seen clearly that the common attacks method on individuals is Tracking Ads links with 27% of responses. However, Surfing Untrusted Website, Downloading Unreliable Software, and Opening Unknown Senders' Emails gain a considerable attention of respondents with 21%, 19% and 18%, respectively.

Second, it is important to study the individual reactions toward any cyberattacks that might happen to them. Therefore, Fig. 15 shows the reactions of all and affected individuals. Three possible reactions respondents addressed as follows: 1) Format device and reset it to factory status; 2) Seek for an advice from a friend or a specialist; 3) Report to authority. As can be seen in Fig. 15, Seeking for an advice and Formatting device seems to be at the high priority of the individuals. However, individuals who have experienced cyberattacks seem to give more attention to actions like Formatting device. Interestingly, all individual respondents appear to deprioritize the action of reporting to authority to allow investigating on the cybercrime.

Third, it is meaningful to link each reaction to the attack methods. As can be seen in Fig. 16, individuals who have experienced cyberattacks tend to choose Formatting Device for all attacks in general. However, it seems that when an attack is suspected to be from an untrusted website, individuals tend to prioritize Seeking for an Advice over Formatting Device. Noticeably, Report to authority seems to be at the least priority to the individuals.

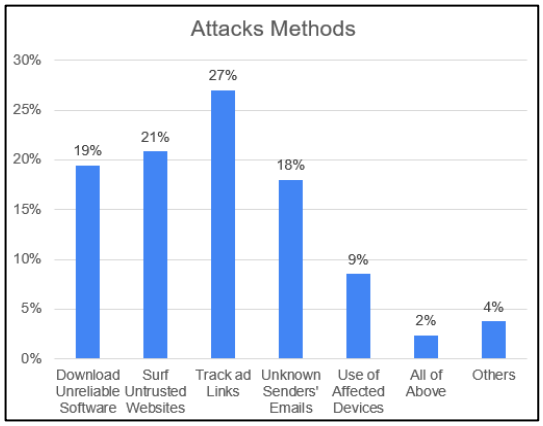

Fig. 15. Attacks Methods.

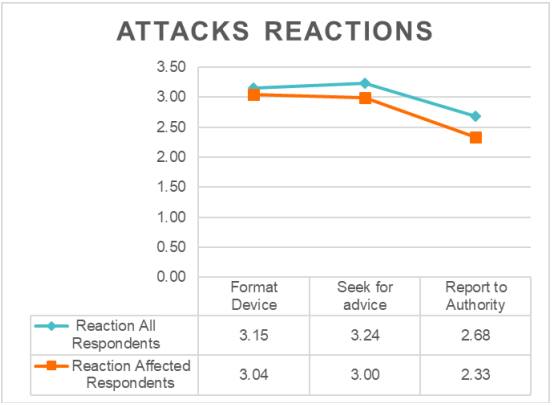

Fig. 16. Attack Reactions (Results is based on Average).

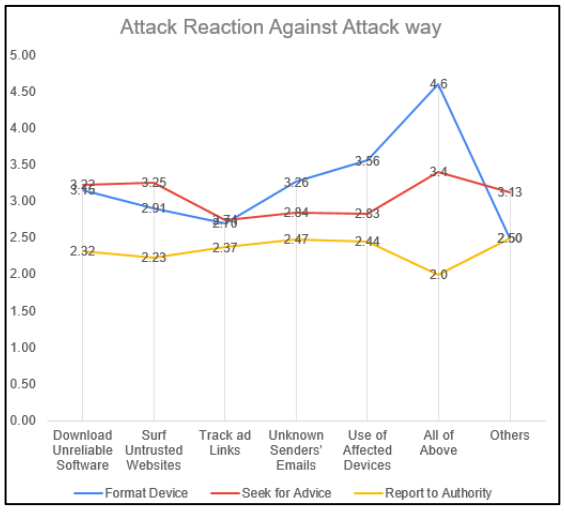

Fig. 17. Attack Reaction against Attack Method (Results is based on Average).

In conclusion, as can be seen in Fig. 17, Tracking Ads links seems to be the most common cyberattack methods that surveyed individuals have encountered. However, Surfing Untrusted Website, Downloading Unreliable Software, and Opening Unknown Senders' Emails are candidate methods used by attackers. In addition, reactions and countermeasures Seeking for an Advice, Formatting Device, and Report to authority are the common actions taken by individuals who either have or not have experienced cyberattacks.

VI. Conclusion

In the research the impact of cybercrimes on individuals in Saudi Arabia has been investigated. A number of findings were emerged. First, an undeniable ignorance of cybersecurity is noticed in individuals. In addition, Saudi networks is a competent secure network. This has been justified by the number of individuals who experienced cyberattacks with comparison to the low level of knowledge of protection methods. Furthermore, unlike organizations, individuals are not targeted by cyberattacks as the majority of 67% of respondents expressed that they have not experienced cyberattacks. However, they might be used to be the breach to organizations as Identity theft is the main purpose of cyberattacks on individuals.

Second, identity theft is the most common purpose of cyberattacks that targeted individuals. Furthermore, it was found that the majority of 64% of respondents spend less than 500 Saudi Riyal (134$) annually on cybersecurity which is less than the average annual spending of a US citizen. In addition, cyberattacks recurrences on individuals are less than 10 times over 5 years.

Finally, Tracking Ads links is the most comment approach used to attacks individuals, while, the Formatting device countermeasure is the popular action taken by individuals for most cyberattacks. Noticeably, report to authority action seems to be at the least priority to the individuals when attacks occur.

VII. Future Work

As the number of internet users is increasing in Saudi Arabia with 26 million as current number of user, more participants are needed in order to have more accurate and reliable conclusions. In addition, studying the impact on different age categories will enrich the research and provide clustering of responses to gain more conclusions. Finally, the financial impact on individuals has been estimated using one factor which is the participants' data. More resources are needed such as data from NCSC and national authority of cybersecurity.

Acknowledgment

I would like to express my special thanks of gratitude to my University (Umm Al Qura University) which gave me the golden opportunity to do this research on the topic Software Engineering. Secondly I would also like to thank my friend (Dr Ahmad Albasheri) who helped me a lot in finalizing this research within the limited time frame.

References

[1] Paulsen and P. Toth, 'Small business information security', US Dep. Commer. Doi, vol. 10, 2016.

[2] CNSS Instruction (CNSSI), 'Committee on National Security Systems', 2015.

[3] T. A. Johnson, 'National Security Presidential Directive/NSPD-43 Homeland Security Presidential Directive/HSPD-14', in National Security Issues in Science, Law, and Technology, CRC Press, pp. 651–654 , 2007

[4] F. A. Momein and M. N. Brohi, 'Cyber crime and internet growth in Pakistan', Asian J. Inf. Technol., vol. 9, no. 1, pp. 1–4, 2010.

[5] M. Riek, R. Böhme, M. Ciere, C. Gañán, and M. van Eeten, 'Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries', in Workshop on the Economics of Information Security (WEIS), University of California at Berkeley, 2016.

[6] D. Milkovich and Cybint Solutions, '15 Alarming Cyber Security Facts and Stats', 23-Sep-2019. [Online]. Available: https://www.cybint solutions.com/cyber-security-facts-stats/., 2019

[7] Communication and Information Technology Commission, 'Digital security and user protection of Internet risk', 2018.

[8] Center for Strategic and International Studies and McAfee, 'Net losses: estimating the global cost of cybercrime: economic impact of cybercrime II', Jun. 2014.

[9] Saudi National Cyber-Security Authority, '2018 First Quarter Statistical Report about Cyber Threats and Risks', 2018. [Online]. Available: https://www.ncsc.gov.sa/wps/portal/ncsc/home/Reports/!ut/p/z1/hY5dC4JAEEV_jc8z64r5uhW4ZhAWmM2LbIvUhq5Z0se_z0V6tObpDPdyOUBQAFn1MCfVm9aqevgPFJaMLSPpx7iO5jOBGWKeiCTlWRrC_l-BhhgnTiDs1A1WYykJAskCP91sXcRzKXm0YBhzZ2EuXUcCSLe2r149FFbfdW2OHjrw8Nw21cilw7Kygxr9Hva_hWm9a1M83xzNB_MOTj8!/dz/d5/L2dBISEvZ0FBIS9nQSEh/. [Accessed: 11-Oct-2019]., 2018

[10] S. Alelyani and H. Kumar, 'Overview of Cyberattack on Saudi Organizations', J. Inf. Secur. Cybercrimes Res. JISCR, vol. 1, no. 1, 2018.

[11] I. Bernik, 'Cybercrime: The Cost of Investments into Protection.', Varstvoslovje J. Crim. Justice Secur., vol. 16, no. 2, 2014.

[12] Z. Kazmi, J. M. Alghazo, and G. Latif, 'Cyber Security Analysis of Internet Banking In Emerging Countries: User and Bank perspectives', presented at the 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), pp. 1–6. , 2017

[13] Shaunak and Gregory Paul, 'Detailed threat analysis of Shamoon 2.0 Malware', vinransomware, Feb-2017. [Online]. Available: http://vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware. [Accessed: 28-Oct-2019]., 2017

[14] Devika Jain, 'Shamoon 2: Back On the Prowl', NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks., 2017. [Online]. Available: https://nsfocusglobal.com/shamoon-2-back-on-the-prowl/. [Accessed: 28-Oct-2019]., 2017

[15] Codymercer, 'StoneDrill – Shamoon & Shamoon 2.0 Variant', 2017. [Online]. Available: https://blog.nsfocusglobal.com/categories/stonedrill-shammon-shammon-2-0-variant/. [Accessed: 28-Oct-2019],2017.

[16] E. Harrell and L. Langton, 'Victims of Identity Theft, 2012', US Department of Justice, Office of Justice Programs, Bureau of Justice, 2013.

[17] E. Harrell, 'Victims of Identity Theft, 2014', US Department of Justice, Office of Justice Programs, Bureau of Justice, 2015.

[18] E. Harrell, 'Victims of identity theft, 2016', US Department of Justice, Office of Justice Programs, Bureau of Justice, 2019.

[19] Symantec, 'Internet Security Threat Report (ISTR)', Symantec, 24, 2019.

[20] M. Fossi et al., 'Symantec internet security threat report trends for 2010', Symantec, 2011.

[21] M. Ovelgönne, T. Dumitraş, B. A. Prakash, V. S. Subrahmanian, and B. Wang, 'Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach', ACM Transactions on Intelligent Systems and Technology (TIST), vol. 8, no. 4, pp. 1–25, 2017.