A Survey of Cyber-Security Awareness in Saudi Arabia

Faisal Alotaibi[1], Steven Furnell[1, 2, 3], Ingo Stengel[1,4], Maria Papadaki[1]
[1] Centre for Security, Communications and
Network Research, Plymouth University, Plymouth, UK
[2] Security Research Institute, Edith Cowan University, Perth, Western Australia
[3] Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
[4] Hochschule Karlsruhe, University of Applied Sciences Karlsruhe, Germany
{Faisal.Aalotaibi, Steven.Furnell, Maria.Papadaki}@plymouth.ac.uk, Ingo.Stengel@hs-karlsruhe.de

***Abstract*—Rapid development has been observed in the deployment of communication technologies and the use of the Internet across the globe. Information exchange is the main aspect of use of such technologies in everyday life. Crimes associated with the misuse of information on the Internet are on the increase and are resulting in various losses. Saudi Arabia is one of the fastest developing countries in the Middle East, where the uptake of communication technologies such as the Internet and mobile technologies has risen sharply in recent years. These technologies are relatively new to the region when compared to developed countries. Therefore, the crimes associated with these technologies may be new to the people in the region. This paper investigates the cyber security awareness of the people in Saudi Arabia within different contexts. A quantitative online based survey was conducted to gather information related to cyber security awareness in Saudi Arabia. The study found that, although the participants had a good knowledge of IT, their awareness of the threats associated with cybercrime, cyber security practices, and the role of government and organisations in ensuring information safety across the Internet, is very limited. An application based model to create cyber security awareness in the region was preferred by the majority. The results indicated that, although cybercrime is on the rise, no specific approach is being followed to increase cyber security awareness in the region except for CERT regulations and online information on government websites. Additionally, *Chi-Square test* results (t(627)=3.85, p=0.013) indicated that Internet skills have an effect on cyber security practices from the users' end and there is an association between skill level and the security measures being implemented by organisations in the region. The study found that there is an immediate need to develop a model to create cyber security awareness in the region in order to combat cybercrime.**

Keywords - Cybercrime, Cyber Security, Communication Technologies, Cyber Security Awareness, Password Security, Mobile Applications

I. INTRODUCTION

The extensive developments in communication technologies are prompting many organisations to automate their processes to provide cheaper, faster and easier ways for their customers to access their services. The use of communication technologies such as email and mobile technologies such as apps has risen exponentially in recent years. According to KPMG International, there are more than 2 billion Internet users and over 5 billion mobile phone subscriptions worldwide [1]. Over 294 billion emails and 5 billion mobile messages are exchanged, and nearly 47% of the world population is using the Internet [1, 2]. These figures are expected to grow given the fast pace of technology deployment to developing countries and their continued spread in developed countries.

Automation is being increasingly adopted by organisations to increase the efficiency of their processes and to provide effective services. For many, technology has become a part of life with everyday activities such as shopping, banking, and entertainment being accessed on mobile devices. All these services are managed through effective information exchange using communication technologies. Unfortunately, crimes associated with these technologies are rising in parallel with the increase in the use of such technologies. Different methods are being adopted to steal information. Activities where computer networks are used to carry out illegal activities are known as cybercrimes[3]. As most businesses and organisations are increasingly relying on communication technologies, it is very essential that the information being exchanged is secured to prevent misuse.

However, the scale of the rise in cybercrimes is alarming. The cost of cyber breaches in the UK alone is estimated to be £3.14 million [4]. The Business Email Compromise (BEC) scams worldwide were estimated to be more than $ 3 billion [5]. The impact of cybercrime is not just assessed solely in terms of costs incurred but also in terms of breach of data privacy which can affect many consumers. The projected losses for the businesses by the year 2019 due to cybercrime are estimated to be in the region of $2 trillion [6]. While the number of cyber security attacks in large companies has been decreasing, in medium and small sized companies it is increasing significantly, which could be a major concern for developing countries [7].

Saudi Arabia, which is one of the fastest developing countries in the Middle East, has seen enormous growth in the use of communication technologies, the Internet and mobile technologies in recent years. It is estimated that approximately 66% of the population, which equals more than 18 million users, have access to the Internet. Facebook and Twitter are used by the majority of these users [8]. About 39% of the population that uses the Internet buys products online, and the country's E-commerce business is about $520 million [9]. The

penetration of the Internet and the boom in smartphone usage in KSA is relatively new. Therefore, it can be assumed that understanding of the importance of cyber security and information on security measures which can be taken is limited. Furthermore, studies on cyber security awareness are largely carried out in developed western countries. KSA is vastly different from these countries in terms of culture, social attitudes, language, government regulations and understanding of the importance of security. Therefore, this paper focuses on the people of Saudi Arabia's understanding of security awareness and the security measures being adopted.

II. METHODOLOGY

This study used surveys as a research strategy in the process of investigating and understanding the levels of cyber security awareness among Saudi nationals.

A. Research Tools

This study used survey techniques as the tools for collecting qualitative information about cyber security awareness. The online survey questionnaire comprised 22 questions which focused on collecting information on different aspects including demographics (8 questions), cyber security practices (5 questions), cybercrime awareness (7 questions), and incident reporting (2 questions). The questions in these sections were selected from different sources [12] including surveys, reports and other research papers that focused on investing cyber security aspects across the globe. The questions put in the cyber security practices section aimed to analyse the current security practices in Saudi Arabia, while people's awareness levels were assessed by the questions posed in the cyber security awareness section. The incident reporting section was mainly included to analyse how people react when they come across an incident of cybercrime and to assess the current practices used in reporting cybercrime in the country.

B. Study Setting & Participants

Two pilot studies were conducted to validate the questionnaire used in the survey and the feedback received was used to improve the final survey process. In the first pilot study hard copies of the survey questionnaire were distributed to PhD students. 12 participants completed the survey. 8 participants were from the Communications and Network Research (CSCAN) and the remaining 4 had other different educational backgrounds. The first pilot study ensured that the survey is suitable for people with diverse backgrounds. The feedback received from this study was that the survey was too lengthy. Accordingly, the number of questions was reduced from 38 to 22. For the next pilot the updated survey questionnaire was translated into Arabic and hard copies were distributed. 16 participants completed the survey. 4 participants were from CSCAN and the remaining 12 had other different educational backgrounds. A common feedback comment received from participants other than the CSCAN participants (who had a computing background) was that they were unable to understand some of the technical terms used. Definitions of all the technical terms used in the survey questions were therefore included in the survey to help clarify the questions for the participants.

The next survey was conducted using the updated survey questionnaire using an online medium for greater accessibility and reachability. The online survey questionnaire was completed by 629 Saudi nationals. The survey link was initially forwarded to 234 participants using email and other social networking platforms. A request was placed in the message to forward the questionnaire to friends who met the criteria, thus adopting the snowball sampling technique to increase the sample population.

C. Inclusion & Exclusion Criteria

Participants of the survey had to be aged 18 and above to be included in the study. Anyone aged below 18 was excluded from the survey as this study focused on the level of cyber security awareness among adults.

D. Research Strategy

This study used a multi-level survey process. The first two pilot studies were used to validate and improve the survey questionnaire. The final online based survey was conducted to find out the level of cyber security awareness among Saudi nationals. The survey results were then used to develop measures to promote cyber security awareness.

III. RESULTS

629 Saudi participants took part in the survey out of whom 440 (70%) were male and 189 (30%) were female. There was no particular reason for the disproportionate male response, as the survey was distributed online without targeting particular groups. However, from other studies [11], it is evident that internet usage among males and youths is higher in Saudi Arabia than among females and members of the older generation. Rounding off to the nearest whole number, the participants were characterised as follows: 268 (43%) were aged 18-29 years, 267 (43%) were aged 30-39 years, 78 (12%) were aged 40-49 years, and 16 (2%) were aged 50 years and over. Out of the 629 participants, 325 (52%) had an undergraduate degree, 197 (31%) had a postgraduate degree, and 107 (17%) had secondary school or primary education. Out of the total number of participants, 569 (91%) access the Internet frequently throughout the day 60 (9%) access Internet once or twice a day. In terms of Internet or digital devices skills, 304 (48%) had intermediate skills, 246 (39%) had expert skills, and 79 (13%) had beginner or basic skills. Smartphones (90%), laptops (60%) and desktops (33%) are the most commonly used devices by the participants. Private Wi-Fi and mobile/cellular networks are the most commonly used networks by the participants. Social networking (84%), education (76%), government services/online banking/e-commerce (66%), and communication (61%) are the major purposes cited by the participants for accessing the Internet. These results indicate that the majority of the participants who are frequent users of the Internet belong to the age-group which generally uses the Internet for various services, as found in [11]. Therefore, the results achieved in this study could be considered as being both valid and reliable.

In terms of cyber security practices, the majority of the participants use the latest versions of operating systems including Windows 7 (or newer versions) on their computers,

and iOS/ Android on their mobile devices. Antivirus programs were the most commonly used security tools by the majority of the participants. Other tools used include authentication, updates and backups as shown in Fig 1. However, there is still a significant proportion of users that claims not to use Antivirus programs and it was also observed that the other security measures mentioned are reported to be used by less than half of the respondents. 55% of the participants use Windows/Android OS, and 42% use iOS. Conceivably, iOS users might have less need to use an Antivirus program when compared to Windows/Android users. Overall, however, the results indicate that there is a low level of implementation of security measures among the participants.

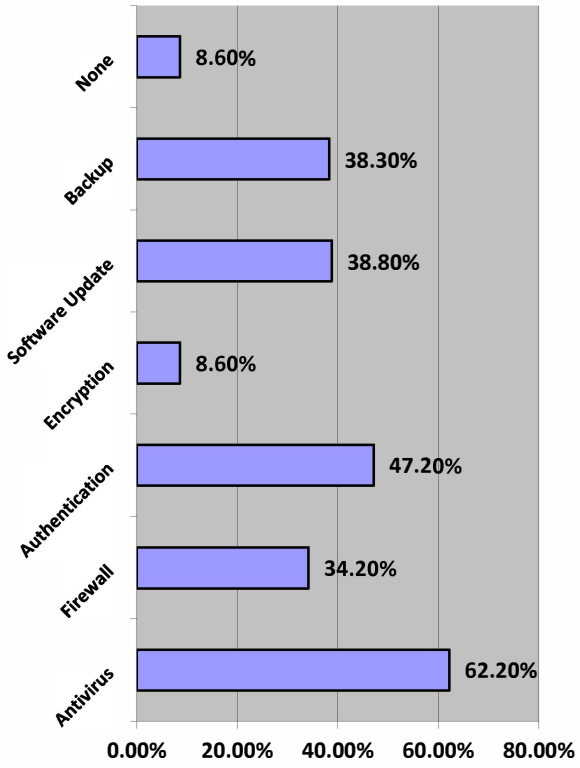

Figure 1. Security tools used by the participants

While considering different security practices, 63% of the participants stated that they were aware of the dangers associated with advertisements/banners/pop-ups, and about 41% said that they give due attention to the security settings on social networking sites. This indicates that the majority of the users are well aware of security threats or risks associated with internet browsing and the common approaches used in cybercrime. The majority of the participants store their sensitive data on their devices (70%), and this would imply that in the event of cybercrime, the losses incurred could be significant. Most of the participants (69%) use their personal information while creating passwords for different online accounts; 34% do not change their passwords regularly and 44% change their passwords sometimes. It is not recommended to use personal information to create passwords, as most people do, as such passwords can easily be discovered and used by other users. Only 54% of the participants regularly install software updates, and only 35% back up their data regularly. Updating systems would help to prevent new threats or crimes from happening; however only half of the participants update their systems, and very few back up their data, indicating poor awareness levels in terms of managing security updates and implementing risk mitigation plans in the event of cybercrime. Out of the total number of participants, only 33% (approx.) always feel that their devices and the data are secured. About 24% of the participants stated that they feel that they do not keep themselves updated about cyber security awareness, while 18% rely on automatic updates, 23% on Internet Service Providers (ISP), and 20% on government websites. The majority (65%) rely on the Internet, websites, emails, and blogs to raise their awareness. The results indicate that the need to increase security awareness is not effectively recognised by the participants and by responsible organisations.

The majority of the participants feel that one should avoid disclosing personal information online and are willing to accept increased Internet surveillance by the government. The most important finding in this category is that the majority of the participants (77%) feel that the risk of becoming a victim of cybercrime has increased in recent years. This is a major concern and an important finding which must be considered in instigating stakeholders to improve security awareness in the country. Among the experiences of cybercrime by the participants, most mentioned receiving phishing emails asking for personal information, 25% occasionally and 28% often experience malware infection, and 25% occasionally and 16% always experience identity theft. Most of the participants reported that they are concerned about cyber security and believe that it could become a serious issue in the near future. They also stated that the government, media, ISPs, and the education system/schools/colleges must take an active role to create cyber security awareness in the country.

212 (34%) of the participants have been victims of cybercrime while the rest have not. Among those who experienced cybercrime only 23 (11%) reported the crime. Out of those who reported the crime, only 6 (26%) reported it to the police, 4 (17%) reported it to the Saudi CERT, 3 (13%) reported it to the Saudi e-Government Portal, while 2 (8%) reported it to the Committee for the Promotion of Virtue and the Prevention of Vice (a Saudi Arabian government agency employing religious police to enforce Sharia law). Out of those who have not experienced cybercrime, 84% stated they would report a cybercrime if they experienced it and 16% stated they would not. Approximately 44% stated that they would ask their friends for advice. The majority of the participants (90%) feel that measures to raise security awareness are necessary. The results can be understood from two perspectives. Firstly, the number of participants who experienced cybercrime is comparatively low; however, among those who experienced an incident of cybercrime very few reported it. This reflects either lack of awareness or problems in the process of reporting an incident. Secondly, the response of participants who did not experience cybercrime, but said they would seek advice from friends/family before reporting an incident reflects a lack of awareness among people and indicates a lack of initiatives by responsible organisations to create awareness.

The reliability of the results was calculated and tested using Cronbach's alpha, and it was found that the results relating to all the aspects scored higher than 70%, indicating good reliability. The results are arranged under five scales and the correlation between the scales is calculated as shown in Table 1.

TABLE I. PEARSON'S CORRELATION COEFFICIENT AND THE SIGNIFICANCE LEVELS

Correlations						
		1	2	3	4	5
1.Opinions	Pearson Correlation	1	.234**	-.107**	.196**	.164**
	Sig. (2-tailed)		.000	.007	.000	.000
	N	629	629	629	629	629
2.Experiencing Cybercrime	Pearson Correlation	.234**	1	.112**	.079*	-.010
	Sig. (2-tailed)	.000		.005	.046	.798
	N	629	629	629	629	629
3.Concerns	Pearson Correlation	-.107**	.112**	1	-.168**	-.260**
	Sig. (2-tailed)	.007	.005		.000	.000
	N	629	629	629	629	629
4.Responsible parties	Pearson Correlation	.196**	.079*	-.168**	1	.181**
	Sig. (2-tailed)	.000	.046	.000		.000
	N	629	629	629	629	629
5.Applications	Pearson Correlation	.164**	-.010	-.260**	.181**	1
	Sig. (2-tailed)	.000	.798	.000	.000	
	N	629	629	629	629	629
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

It is evident that opinions about cyber security and cybercrime is positively and significantly correlated with having experienced cybercrime with r(629)=0.234, p=0.000. This indicates that the more a person has experienced cybercrime the more likely they are to agree with opinions about cyber security and cybercrime. Opinions also had a significant positive correlation with parties responsible for raising awareness, with r(629)=0.196, p=0.000 and with application based cyber security awareness r(629)=0.164, p=0.000

IV. DISCUSSION & CONCLUSION

An Independent Samples t-test was used to investigate the gender effect on the results. The results indicated that a significant difference exists only in the opinions about cyber security and the scale of cybercrime where male participants (M=3.99) had a higher level of agreement than female participants (M=3.85). Significance was found at t(627)=2.89, p=0.004. Similarly, in analysing the effect of Internet usage on the four scales, that is the participants' experiences, concerns, responsible parties, and applications, significant differences were found in terms of awareness of increasing cybercrime where participants who frequently use the Internet throughout the day showed a higher agreement (M=4.49) when compared to those who use the Internet once or twice (M=4.19). Significance was found at t(627)=3.85, p=0.013. No significant differences were found on the other scales (p>0.05).

A chi-square test was also used to determine the association between the skills' level in using the Internet and digital devices with cyber security practices. Evidence showed that there is a significant association between skills and security practices with p=0.000 in all the cases. Similarly, level of skill in Internet and digital device use was associated with the role of the government in combating cybercrime. A significant association was found in all the cases. The results indicate that Internet skills have an effect on the cyber security practices of the users, and association of the level of skills of the people with the security measures to be launched by the government or responsible parties.

The key findings of this study are that there is a high use of the Internet mostly on a daily basis among participants. Another important observation was that over 90% of the participants use smartphones primarily for Internet access to various activities including banking and shopping. The general observation was that even though the survey shows good IT knowledge among users, their cyber security awareness was weak. It was observed that, apart from their implementation of relatively common cyber security measures such as anti-virus programs and firewalls, the participants showed relatively low

cyber security awareness and were likely to carry out risky practices such as using weak passwords. The use of security technologies (and level of awareness) has not kept up with the significant growth in the use of technologies in Saudi Arabia. Users are experiencing problems and would prefer responsible organisations to play an effective role in improving cyber security awareness. They also support the concept of using mobile applications to increase security awareness among them.

One of the best ways to combat cybercrime is by creating awareness and adopting better cyber security practices by users. The survey responses indicated that users are insecure about their data security and are willing to adopt better practices to secure their devices and data. The survey responses also indicated that a cyber-security awareness application would enable users to improve their cyber security practices. Therefore, it is important to create different approaches to increasing cyber security awareness in Saudi Arabia to help combat cybercrime. The participants would welcome an application which would help combat cybercrime and raise awareness.

V. FUTURE WORK

On the basis of this study, it is evident that there is a need to raise cyber security awareness in Saudi Arabia as the number of Internet and mobile users are rapidly increasing and the level of security tools being used and the levels of security awareness being generated are comparatively low. The role of responsible organisations in creating awareness is comparatively limited at this stage. Therefore, awareness programmes that consider the lifestyles and cultural practices in the country must be developed to address the changing needs of the people. Therefore, future studies could consider developing a mobile application coupled with gaming technology to generate security awareness in the region and analyse its efficiency, performance, reliability and usability. This approach can have good reachability as the number of mobile users is increasing and their interest in apps and entertainment is high [11]. This could also lead researchers to investigate other aspects that can be used in conjunction with mobile technologies to create cyber security awareness.

REFERENCES

[1] KPMG International, "Issues Monitor Cyber Crime – A Growing Challenge for Governments", 2016.

[2] International Telecommunications Union, "ICT Facts & Figures, 2016", 2016.

[3] J. Liu, Y. Xiao, S. Li, W. Liang and C. Chen, "Cyber Security and Privacy Issues in Smart Grids", IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981-997, 2012.

[4] W. Ashford, "Top 10 cyber crime stories of 2015", Computer Weekly, 2015.

[5] "Internet Crime Complaint Center (IC3) | Business E-mail Compromise: The 3.1 Billion Dollar Scam", Ic3.gov, 2016. [Online]. Available: https://www.ic3.gov/media/2016/160614.aspx. [Accessed: 16- Sep- 2016].

[6] Juniper Research, "Cybercrime will Cost Businesses Over $2 Trillion by 2019 - Juniper Research", Juniperresearch.com, 2016. [Online]. Available:http://www.juniperresearch.com/press/pressreleases/cybercrime-cost-businesses-over-2trillion. [Accessed: 16- Sep- 2016].

[7] Symantec, "Attackers Target Both Large and Small Businesses", 2016. [Online].Available:https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf. [Accessed: 16- Sep- 2016].

[8] Miniwatts Marketing Group, "Middle East Internet Statistics, Population,Facebook and Telecommunications Reports", Internetworldstats.com,2016.[Online].Available:http://www.internetworldstats.com/stats5.htm. [Accessed: 16- Sep- 2016].

[9] CMO Council Middle East, 'Facts & Figures', 2015. [online]. Accessed: http://www.cmocouncil.org/mena/facts_stats.php [Accessed: 28- Nov- 2015]

[10] Sonderegger, A. and Sauer J. 2010. "The influence of design aesthetics in usability testing: effects on user performance and perceived usability". Applied Ergonomics, 41, 403–410.

[11] M. Simsim, "Internet usage and user preferences in Saudi Arabia", Journal of King Saud University - Engineering Sciences, vol. 23, no. 2, pp. 101-107, 2011.

[12] Australian Cyber Security Centre, "2015 CYBER SECURITY SURVEY: MAJOR AUSTRALIAN BUSINESSES", Commonwealth of Australia 2015, Australia, 2015.