A Framework for Cybersecurity Awareness in Saudi Arabia.

Mead Rashed Albediwi [1], Kishwar Sadaf [2]

1. Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia, 411203859@s.mu.edu.sa

2. Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia, k.sadaf@mu.edu.sa

Abstract

The rapid advancement in technology has improved people's lives, but it has also increased the risks that come with using the Internet, including cybercrimes. Lately, Saudi Arabia, a booming economy, has become one of the prime targets of cyberattacks. The massive amount of cyberattacks targeting Saudi Arabia can be attributed to the lack of cybersecurity awareness among Saudi people. The objective of this study is to propose methods on the national level to increase the awareness of cybersecurity among Saudi people. We conducted a cybersecurity assessment survey to assess the cybersecurity awareness among Saudi people. The survey result indicated negligent behavior and lack of awareness. To address this issue, we proposed a cybersecurity awareness framework which targets all strata of Saudi Arabia demography. The proposed framework not only emphasized training programs in schools, universities and organizations but also addresses the awareness issue in people from informal backgrounds. The framework also includes the importance of incident response and its role in reducing incidents.

Keywords: Cybersecurity; Cybersecurity Awareness; Cybersecurity Framework.

Introduction

Cyberattacks are on the rise, and Saudi Arabia ranks second in terms of attacks, as the Kingdom issued an order to establish a specialized body in the field of cyber security to protect infrastructure from potential attacks. Internet users are on the increase which leads to an increase in cyberattacks and has caused financial losses. And if we compare between year 2019 and 2020, the statistics show an increase of 71% cyberattacks (Fig. 1) [1]. It shows the top ten sectors targeted in the first quarter of 2020. Therefore, there is a need for awareness programs because of their importance in raising the culture of smart users. Cybersecurity awareness has several definitions, including: "security awareness is the continuing learning and recognition of the importance of information security issues and the level required to achieve good security awareness and knowledge of individuals' security duties". Another definition of security awareness is "the knowledge and commitment of users to their security mission". These definitions of awareness do not include important elements like graduality and the process of progression which are important in any training. Authors in [2] defined awareness as the security knowledge that was gradually acquired during continuous and attractive training.

The Kingdom of Saudi Arabia is a target for many cyberattacks, due to the digital transformation and the use of technology in most areas. According to many reports, Saudi Arabia is the most vulnerable Gulf country to malicious cyberattacks which calls for the need for a strong structure for cybersecurity. Among the attacks that targeted the Kingdom, the attack on Saudi Aramco was well known. Saudi Aramco was exposed to multiple cyberattack attempts, including the Shamoon virus, which paralyzed computers by scanning the disks. Many attacks were targeted towards Saudi ministries and institutions [3].

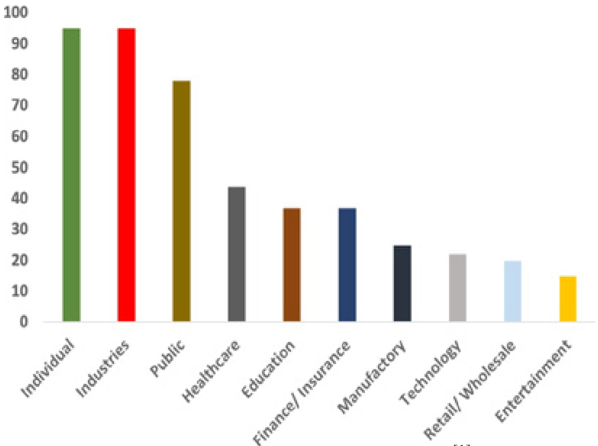

Fig. 1. Top 10 targeted sectors [1]

Irrespective of the high level of cybersecurity, naïve users can cause massive damage to their data as well as to the system. Therefore, awareness about the risks associated with internet technologies must be made prevalent among people to reduce the avenues of attacks. There are many studies [4], [5],[6], and [7] etc. on cybersecurity and how to activate awareness programs to raise awareness of cyber security in more than one way, but there is still a gap between Internet users and cybersecurity. The main reason is the user's lack of awareness, which leads to the attacker exploiting his weaknesses, as well as due to employee negligence in following the policies described in the organization, which leads to the continuation of cyberattacks, and this does not mean that the losses are limited to the physical aspect only, but include the loss of personal data. Cybersecurity is a growing concern in Saudi Arabia, as the country continues to develop its digital infrastructure and relies increasingly on technology. However, the country still faces a number of cyber threats, including cybercrime, hacking, and cyber espionage. Cybersecurity awareness is extremely important in today's digital world, as the number of cyber threats continues to increase. Fig. 2 shows our approach to develop a comprehensive cybersecurity awareness program for Saudi Arabia.

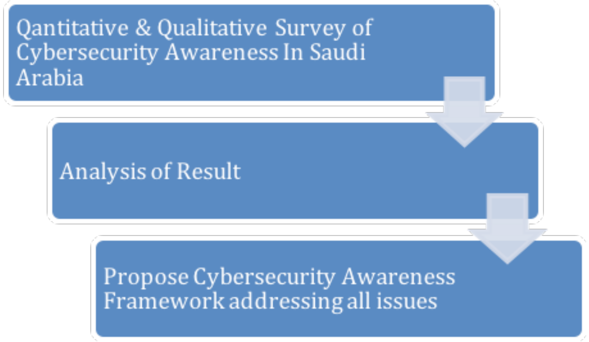
Qantitative & Qualitative Survey of Cybersecurity Awareness In Saudi Arabia
Analysis of Result
Propose Cybersecurity Awareness Framework addressing all issues

Fig 2. Workflow of our proposed approach of increasing cybersecurity awareness in Saudi Arabia

To assess the level of current cybersecurity awareness, we conducted a survey on Saudi people of all age groups who interact with the internet through smartphones, PCs, or any IoT devices. The survey result shows that people do not pay needed attention to the security concerns. The survey findings also confirm the survey done in [1]. In this paper, we propose a comprehensive framework to raise the level of awareness of cybersecurity targeting Saudi society in all its age groups. Our framework addresses awareness among common strata of people like students, employees, kids, older people etc. The framework includes elements of educational training, awareness program for general public and incident response and reporting process. Incident response is an important aspect of a comprehensive cybersecurity awareness program that helps minimize the damage caused by a security breach or cyberattack, respond rapidly to security incidents, and maintain public trust. As far as we know, our framework is the only work that focuses on engaging all strata of Saudi population in awareness program as well as encouraging an environment of reporting cyber incidents. Our framework explains how training people in formal sectors like school, universities, organizations etc. can be trained in cybersecurity irrespective of their specialties. The most important aspect of our framework is reaching out to people from informal sectors through planning, policy making and tools. Also, our framework makes cybercrime reporting interactive so that no incident goes unnoticed by the government and can be delt swiftly.

This paper is organized as follows. Section 2 present some related work in the field of cybersecurity awareness and cybersecurity awareness programs in different countries and discuss the current cybersecurity strategy of Saudi Arabia. In Section 3, we present an assessment of the survey that we conducted. Subsequently, an analysis is drawn subsection 3.1. In Section 4, our proposed framework is presented and explained. In Section 5, other cybersecurity awareness frameworks are compared with our proposed framework. Lastly, a conclusion is drawn in Section 6.

Related Work

Due to the shifting of all major processes from conventional methods to the smartphone or IoT platforms, security has become the biggest challenge for the governments. The cyber criminals take advantage of unaware, naive users by stealing their money or information. Nowadays governments have also become susceptible to cyberattacks resulting in massive data loss, national security breach, financial loss and many more compromised systems. Generally, a cyberattack starts by targeting a person who is not aware about the security concerns. One such small incident snowballs into a big catastrophic event resulting in huge loss. The research fraternity has been coming up with proposals, tool and techniques to address this issue. In [8], authors researched the efforts of South Africa in the field of awareness and education in cybersecurity, and it became clear that it does not have awareness and education initiatives in cybersecurity. So, they proposed a framework for cybersecurity awareness in South Africa and create a cybersecurity culture in South Africa among Internet users. Authors reviewed previous studies in cybersecurity to identify gaps in awareness research [9]. They found that there is still a lack of cybersecurity awareness, and they suggested improvements, to improve the current practices and target the youth section. In[10], author measured the level of situational awareness in the Internet users and then created a multi- level framework based on analyzing conditions. And based on these conditions, faster and more efficient actions are taken. Gcaza et.al in[11] studied the culture of cybersecurity. They emphasized that to reach a culture of cybersecurity, awareness and education must be raised. Alsmadi et.al in[12] discussed the extent of states 'commitment to cybersecurity through the Global Cybersecurity Index. There is a gap in teaching methods, so they suggested changing teaching methods. Authors in[13] highlighted the importance of cybersecurity and how organizations seek to defend their assets. They proposed cybersecurity models based on the sensitivity of the assets. In[4], authors addressed awareness of cybersecurity, and directed the effort at children and their use of smart devices. The built-in hardware restrictions successfully protect users. Alzubaidi[1] measured the current level of awareness in Saudi society and made recommendations to enhance awareness. Author also pointed out low incident reporting by people.

Cybersecurity Strategies in Developed Countries and Saudi Arabia

Authors in[8] reviewed the cybersecurity strategies in the United States of America (US), United Kingdom (UK), Canada and Australia. These countries have cybersecurity strategy in place for many years. All of these strategies have at least one national education and awareness initiative because it plays an important role in improving economic and social well- being. For the sake of brevity, we will not dwell into the details of these countries' strategies. Their strategies are summarized in Table 1.

Table 1. Cybersecurity strategies applied in the aforementioned countries

Country	US	UK	Canada	Australia
Year	2009	2011	2011	2009
The initiative	National Initiative for Cybersecurity Education (NICE)	Get Safe Online	Get Safe Online	Broadband Management, Communications and the Digital Economy (DBDCE) and the Australian Competition Commission (ACCC)
The campaign	stop think connect	Get Safe Online	Get Cyber Safe	*Stay Smart Online*
Host organization	DHS Department of Homeland Security	Get Safe Online	public safety canada	*Stay Smart Online*
The target audience	For all segments of society: children, college students, parents, teachers, professionals, Americans, the government, and companies.	Individuals and companies	General Canadian Audience	Home users, children, teenagers, schools and small businesses.

Topics they covered	Cyberbullying, identity theft and phishing, child protection online, and e-learning integration. Banking services, cybersecurity. Internet fraud and deception.	Fraud, games, dating, banking, money transfer, privacy, cloud computing, data encryption, data loss, protection of company sites	Email security, file sharing, mobile security, fraud.	Mobile parental controls, passwords, file sharing, spam, online shopping

Each country has its own cybersecurity target depending on native factors like level of education, infrastructure to support cybersecurity awareness, demography etc. Developed nations have different security needs as compared to developing nations. The countries have tailored made cybersecurity awareness policy which caters to their need.

Cybersecurity in Saudi Arabia: The Internet became available to everyone in the Kingdom in 1999. Saudi Arabia's Security Vision 2030 emphasizes Saudi Arabia's need to advance safely and flexibly by providing a security basis to ensure the Kingdom's development into a knowledge-based economy. SA implemented the national cybersecurity into the presidency of the republic to become the focal point of cybersecurity in the Kingdom in 2017. The Ministry of Communications and Information Technology (MCIT) was the first national security strategy in 2011. In 2016, the Kingdom of Saudi Arabia faced a wave of cyber-attacks. The Director of the Saudi Cyber Security Center (NCSC) also stated that the Kingdom responded to nearly 1,000 attacks targeting infrastructure and seeking to steal data, and cause services interruption. These incidents fall under the responsibility of the Saudi Computer Emergency Response Team (CERT-SA), which was established in 2006 and is a trusted reference for information. CERT provides consulting services on how to deal with accidents. It collects information about a specific event, performs post-incident analysis and prepares reports if requested, conducting the analysis and developing prevention of cyber accidents. The cost of cyber accidents can also be determined. CERT-SA is not a responsible central authority and is often seen as an interactive organization providing information on current threats and supporting incident response. There have been efforts to create a support platform for CNI (Critical National Infrastructure) and government security and services such as: Incident Response Planning Malware Analysis, Supervision and Consultation. This platform has not yet been introduced.

The Kingdom is one of the 18 members to sign the Arab Convention to Combat Cybercrime, but it has not yet been ratified. The Kingdom of Saudi Arabia is keen to pay attention to information technology, communications and cyber and make it one of the main pillars. It is the largest market for information and communication technology in the East and invested nearly $ 14 billion in the technology and communications sector as well as cybersecurity in 2016. The Kingdom of Saudi Arabia has prioritized cybersecurity as the highest level. It has realized the increasing urgency to take over the defense against cyber-attacks due to the increase in attacks in recent years [14]. In Saudi Arabia there is National Cybersecurity Authority (NCA) which is responsible for handling cybersecurity in Saudi Arabia. They have a vision to seek to achieve cybersecurity that combines confidence, security and growth, which is comprehensive and in line with the vision of the Kingdom and strengthen the protection of technical systems and infrastructure as well as enhance the confidence of investors and individuals in cyberspace and supports economic growth. The authority has been keen on designing a cybersecurity reference framework based on best practices and challenges. It is a model that contains multiple aspects of cybersecurity. The framework includes six themes and eighteen elements for cybersecurity in order to develop the national strategy for cybersecurity. The six axes contained in the framework:

- Unify: in the sense of the integration of all components of cybersecurity.
- Manages: How to manage infrastructure and risks.
- Assure: which is to ensure that cybersecurity is protected.
- Defend: developing cyber defense mechanisms against risks.
- Partner: About building partnerships and sharing information.
- Build: is concerned with building a strong and secure base (NCA, 2021).

The Saudi Arabian Monetary Agency (SAMA) has developed a cybersecurity framework to enable member organizations to effectively identify and address cybersecurity risks. To be able to protect information assets and online services, member organizations must adopt the framework [15]. Although the Kingdom has several cybersecurity frameworks which encompass all the major security aspects, the aspect concerning awareness among people has little focus. As stated earlier, cyber users who are not aware of risks associated with technologies, applications etc. and their careless actions around these applications can have dire consequences. Our survey (discussed in next section) shows that people are not security conscious when it comes to cyberspace. Therefore, awareness of the security risks among people whether adults or kids is necessary for a secure cyberspace. Our framework is dedicated to increase the awareness through multiple channels and addresses all the age-group.

Cybersecurity Awareness Assessment

To assess the current awareness of cyber risks among Saudi people, we conducted a survey targeting technology savvy people. Using Google forms, a questionnaire was created. The questionnaire contains 30 questions. A question was also raised to the participants about who is responsible in their opinion for raising awareness in cybersecurity. And finally, reporting accidents and the extent to which individuals perceive its importance. 530 Saudi citizens completed the questionnaire. The survey was published using social media.

Upon completion of the questionnaire, we analyzed the results to assess the level of awareness of the end user in the Kingdom and verify reliability using the SPSS program. 7% of the participants were less than 18 years old, 13% were older than 45 years, and the largest percentage was 79% for ages between 18 and 45 years. Gender ratio was 60% of males and 40% of females. Participants were asked general questions about the type of operating system used and the extent of security in their devices according to their belief, as well as with regard to protection programs, their activation, the use of virus programs and the activation of updates in the devices etc. and about users' behavior to measure their awareness of cyber threats when they use cyberspace. Regarding the e-mail address and whether the sender and recipient address is verified, the answers were as follows: 53% answered yes, 30% answered sometimes, 16% said no. Regarding sharing the email address, 73% said no, and 26% said yes. For the question "are you logging out of the email account when you finished it", the answers were: 27% answered yes, and around 70% answered they don't. Regarding passwords, the questions were "Do you prefer simple or complex passwords?" 52% answered simple and 47% complex, "in terms of changing passwords continuously, 13% answered yes, 30% answered occasionally, and 56% answered no, about using different passwords for accounts, the answers were 55% yes and 44% no.

Regarding browsing websites, downloading applications, and using public networks, the questions were as follows: Checking addresses and links before clicking on them, 44.3% answered yes and 55.7% answered no. With regard to sharing personal information with anyone, the answers were as follows: 41% answered with those we know, and 57% said no. Due to the importance of this question and its connection to some extent with social engineering, it was necessary to ask a question about the meaning of social engineering. 17% said they knew about social engineering and 83% said they did not know. With regard to communicating with people you do not know, 13% answered yes, 45% said no, and 42% sometimes. On downloading applications, is the application developer checked? Answers were 32% yes and 67% no. About the permissions allowed for the app before it is loaded, 38% responded by reading the permissions before downloading the app, and 61% answered no. This question is every important. When users install malicious applications without verifying the permissions needed by those applications, they unknowingly give full control of their device to the application developer. The developer or publisher can exploit this condition. About the use of Wi-Fi networks in public places 17% answered yes, 37% answered occasionally, and 45% said no. For the question about reporting any security incidents or cybercrimes, 55% answered yes and 41% said they did not know the authorities responsible for handling such incidents. And the importance of knowing the opinions of the participants about who is responsible for raising awareness in the Saudi society (Government, media, individuals, education) the answers varied as follows: 62% answered the government, 66% of the media, 32% of individuals and 57% education. Answers were taken using a Likert scale (yes, no, I don’t know, sometimes).

Assessment Result Analysis

In this study, the different participants’ practices and knowledge in cybersecurity were evaluated through a survey. To measure the reliability and consistency of the survey, we employed Cronbach’s Alpha assessment method (Table 2). Table 3 shows the demographic information of the participants of the study.

Table 2. Reliability Statistics

Cronbach’s Alpha	No. of Items
.708	27

Table 3. Demographic information of research respondents

	Variables	Numbers	Percentage
Sex	Male Female	317 213	59.8% 40.2%
Age (year)	Under 18 18-45 Over 45	39 422 69	7.4% 79.6% 13%
Technology usage time	1-4 hours 4-8 hours More 8 hours	101 286 143	19.1% 54% 27%

With regard to the user’s behavior when using technology and the extent of his keenness in securing his data, there are a number of questions given using the Likert scale (yes, no, sometimes) and the results (Table 4) are as follows:

Table 2. Reliability Statistics

Question	Yes	No
In public places, do you use Wi-Fi networks?	94	239
Do you verify the sender and address before opening emails?	285	86
When you finish your e-mail, do you log out of your e-mail?	144	282
Do you regularly back up programs?	137	214
Are you constantly changing your passwords?	71	300
Do you respond and communicate with people you do not know?	70	243

There are many risks in accessing the Internet and therefore, potential threats must be prevented. For this, 10 questions were asked about monitor user behavior, and users’ answers were yes or no, as shown in the table below (Table 5).

Table 5. Questions for monitoring user behavior

Question	Yes	No
When downloading an application from the stores on mobile devices, do you check with the application publisher?	174	356
Do you know about malware such as virus and worm?	230	300
Do you know what are the allowed permissions of the application before downloading it in your devices?	204	326
Do you check the URLs and links of the internet pages before clicking on them?	235	295
Do you know what social engineering means?	90	440
Do you know what does the word hacker mean?	500	30
Do you use different passwords for your accounts?	293	237
Do you know the importance of backup?	350	180
Do you know what is a phishing attack?	117	413
Do you share your email address with everyone?	139	391

Authors [1] conducted a survey to measure the level of awareness, and the questions about cybercrime and reporting them. The results are that 21.7% were victims of cybercrime and 29.2% reported the crime, while 70% did not report and the reasons are shown in the following figure (Fig. 2) adapted from [1].

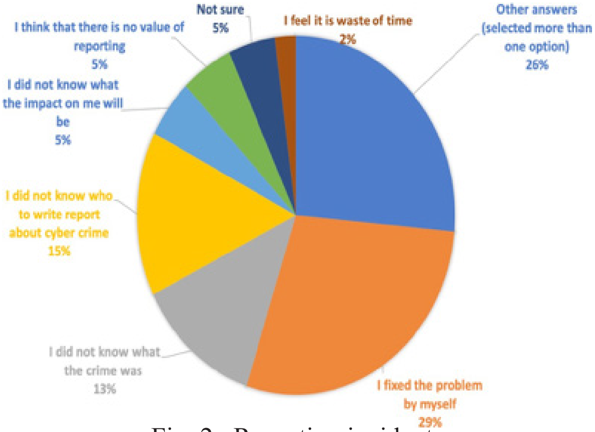

Fig. 2. Reporting incidents

Regarding cybercrime and the way individuals deal with it, a question was asked to the participants "in case you were exposed to a cyber-attack, do you report it?". The answers are shown in Table 6. The participants were also asked about their opinion on the responsibility to raise awareness of cybersecurity in Saudi Arabia. More than 60 % considered the government and media responsible for creating awareness.

Table 6. Incident Response

In the future, if you are exposed to a cyber-attack, will you report it?		
	Frequency	percent
Yes	295	55.7
No	15	2.8
I do not know the responsible party	220	41.5

In this survey, the following is evident:

- About passwords and their importance in terms of security, the largest percentage prefer simple passwords, and about changing passwords, 56% replied that they did not change passwords.
- About the importance of backing up and doing it, 66% knew about the importance of backup and only 25% were the ones doing the backup.
- Regarding the sharing of personal information and its connection with social engineering, the percentage was 41.7% who responded by sharing information with those they know about their knowledge of social engineering, and 83% said they did not know it.
- Despite the threats that occur when connecting to public networks, 17.7% answered that they use public networks. 37.2% answered sometimes.
- With regard to cyber incidents and the process of reporting them, 41.5% replied that they did not know the responsible authorities.

From our survey result, it is evident that there is a need for a rigorous cybersecurity awareness program that increases the level of sense of cybersecurity among people. It is also important to have awareness programs for unqualified people and nontechnical person, such as housewives and elderlies. These findings validate our awareness framework. All the components of our framework address these issues.

Proposed Framework

The cybersecurity framework aims to enrich information technology security and contains a set of policies and procedures to enhance cybersecurity strategies

[16]. The Fig. 3 adapted from [16] shows the five main basic processes that define the cybersecurity framework.

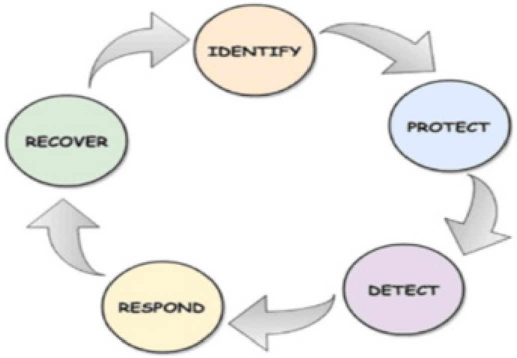

Fig. 3. Cybersecurity Framework Strategies

The framework for cybersecurity proposed here (Fig. 4) focuses on enhancing the cyber awareness of the Saudi society. The framework depends on following key factors, namely:

- The objective must be clear.
- Availability of tools and resources.
- Developing an action plan to implement the policies.

The framework is based on the needs and requirements of individuals to reach a good level of awareness of cybersecurity, and it targets all groups of society to eliminate avenues through which attackers can take advantage. The framework includes a number of strategies and policies which are important for a clear and efficient awareness program. The following figure presents our proposed framework for cybersecurity awareness and its components. An aware and able society makes a strong shield of defense against attackers. Cybersecurity awareness among mass can be effective against cyberattacks if all the sections of society become conscious while interacting with internet technologies thus closing avenues through which attacks can happen.

Our framework considers all those sections of society who use internet technologies through smartphones, computers, tablets or IoTs etc. Our framework proposes cybersecurity training in schools, universities, colleges and organizations as well-trained persons can educate others. The main awareness program targets those sections of Saudi society who do not possess the required technological knowledge. Our framework proposes different tools and methods to increase awareness among these people. Beside awareness and training, the framework also offers incident response which addresses the issues related to attack incidents like how there are responded to and make it easier for people to report incidents so that these incidents would not become major crisis.

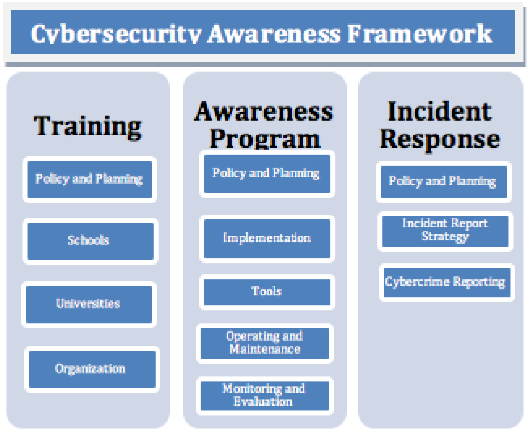

Fig. 4. Cyber Security framework

Training

Students and employees whether government or non-government make the majority of tech savvy population of Saudi Arabia. As many universities in Saudi

Arabia are providing cybersecurity related programs, schools and various organizations are yet to include a rigorous approach towards increasing cybersecurity awareness. To have an effective training across these institutes policies must be defined to layout the ways in which the training will be carried out.

- After implementing the cybersecurity policy, ensuring regular monitoring and evaluation of the executed process.
- Continuing and expanding awareness programs and campaigns to reach specific target groups.
- Ensuring that there is a link between awareness efforts and the national cybersecurity strategy.

Training in schools

This program targets students in schools. Since cyberattacks target all segments of society, including school students, the attacks lead to losses in various fields. So, it is necessary for learners in the school to realize their responsibility to protect themselves and their information while using the Internet. It is necessary to equip them to be able to take responsibility for their security through awareness and education programs. Authors explained that awareness programs for school students are of great importance because most students do not understand the concept of cybersecurity, so it is important to develop awareness programs in education as a curriculum [17]. A strategy must be developed to improve cybersecurity in the school environment. Some important points to consider for defining the training policy:

- Having a plan that clarifies the basics of cybersecurity within the school and improving the educational efforts of learners in schools.
- For the government to undertake a unified policy for schools and ensure its implementation.
- Providing schools with how to deal with cybersecurity incidents.
- Providing training packages for learners with regard to cybersecurity and making them aware of the importance that the topics are appropriate for the age of the learners.
- Providing the necessary resources for training and education in the field of cybersecurity through cooperation with the academic community.
- Emphasizing importance of parental involvement through assistance in cybersecurity awareness efforts and the exchange of instructions with teachers.
- Including cybersecurity in school curricula.
- Ensuring that educational investments are effective and that they fulfill the needs of the cybersecurity environment.
- Implementing strategies are mandatory for students and teachers [17].

Training in universities

The training in universities is of paramount importance as graduates with advanced cybersecurity skills will form an effective defense against the cyberattacks. Various universities across Saudi Arabia are offering courses related to cybersecurity. However, requirement for state-of-the-art cybersecurity courses in universities and colleges have become inevitable. There must be a plan that clarifies what will be the cybersecurity within the university and improving the educational efforts of learners at the university.

Followings are some points to consider while developing cybersecurity program for universities and colleges:

- The government should undertake a unified technology policy for universities and ensure its implementation.
- After implementing the cybersecurity policy, ensure regular monitoring and evaluation of the executed process.
- Providing universities with how to deal with cybersecurity incidents.
- Recruitment of cybersecurity professional and providing training packages for learners with regard to cybersecurity.
- Provide the necessary resources for training and education in the field of cybersecurity through cooperation with the IT industry.
- Following up on cybersecurity developments nationwide through social media, the media, posters, brochures and workshops.
- Including cybersecurity in the curricula.
- Ensure that educational investments are effective and that they fulfill the needs of the cybersecurity environment.
- Implementing strategies are mandatory for students and teachers.

All of the above recommendations are the responsibility of the government in the first place, especially the Ministry of Education, as it is responsible for the school and university system, and schools and universities are responsible for implementing the policies, measures and procedures. This means cooperation between government, schools and universities by working together to optimize and raise cyber awareness. In addition to the importance of providing tools that help in implementing the procedures and measures, with the importance of monitoring what is being implemented and continuous evaluation to ensure the effectiveness of the procedures and that they lead to the desired goal. If these recommendations are taken into account, the state of cybersecurity awareness in schools and universities will improve greatly [17].

Training in organizations

This cybersecurity training targets employees at their workplace whether government or non-government. Cyberattacks also target workers in different sectors. It is necessary for employees to realize their responsibility to protect themselves and their information while using the Internet as their ignorance can pose threats to the organization’s data and eventually leading to massive cyberattacks resulting in financial loss, credit loss etc. Therefore, it is necessary to equip them to be able to take responsibility for their security through awareness and education programs. Therefore, there must be a strategy to improve cybersecurity awareness in the work environment. Followings are some key points to consider:

- Having a plan that clarifies what will be cybersecurity within the company or organization and improving awareness efforts for employees.
- Providing the organization with how to deal with cybersecurity incidents.
- Providing training packages for employees with regard to cybersecurity and making them trained.
- Provide the necessary resources for training and education in the field of cybersecurity through cooperation with the academic community.
- Ensure that there is a link between awareness efforts and the national cybersecurity strategy.
- Implementing strategies are mandatory for employees.

Responsibility of all the aforementioned recommendations falls on companies and managers to impose policies on employees and they must comply with them and apply measures and procedures. This means collaboration between managers and employees working together to improve and raise the level of cyber awareness. In addition to the importance of providing tools that help in implementing the procedures and measures, with the importance of monitoring what is being implemented and continuous evaluation to ensure the effectiveness of the procedures and that they lead to the desired goal [17].

Awareness Program Policy

The awareness programs are directed at people who are not technology professionals and do not have any background on cyber safety such as housewives, the elderly, general businessmen etc. There are various methods which can help in increasing and educating non-technical people about the dangerous of using the internet via smartphones, computers, tabs etc. The existence and diversity of technologies can contribute in achieving the desired goals, which can raise the level of cyber awareness in Saudi society of all age groups. The power and widespread use of social media, television etc. can play a major role in increasing the cybersecurity awareness. The security awareness program can be defined as a program whose main objective is to train users on the threats they may face during their use of cyberspace and how to deal with situations that may endanger sensitive data [18].

In this section, we discuss awareness programs components and how to use them. Basic components of a security awareness program can be summarized as:

1. Planning
2. Implementation
3. Operating and Maintenance
4. Monitoring and evaluation

Planning: Planning is very important before undertaking any awareness program operations. With only proper and effective planning, awareness program can achieve maximum outreach and awareness among people. During planning, requirement analysis is done. Tools, personnel, organizations, strategies etc. are decided which will be utilized in awareness programs.

Implementation: After planning, implementation of operations described in planning is carried out. The implementation must include all the steps in their entirety. An awareness program can become successful only if all each and every component are properly deployed.

Operation and Maintenance: This phase ensures that the program is effective and efficient in increasing the awareness and is sustainable.

Monitoring and evaluation: Periodic monitoring and evaluation of the awareness program assess the effectiveness of the program and check if all the components are working properly as intended and has not lost its efficiency.

Below are some tools which can be used in the awareness programs:

1. Social media: social media is considered one of the successful methods due to its ubiquity and frequent use in almost all circles of society. It can help in cyber awareness and has an effective role in creating public opinion, as well as regarding awareness of cybersecurity through a group of thinkers and influencers and their presentation of issues of interest to cybersecurity that help in forming the awareness of users.
2. Campaigns: Campaigns can be used to create and implement cybersecurity awareness programs at the district level. Responsible individuals are given the task of supervising the campaigns and evaluating them periodically to ensure their effectiveness. The campaigns deal with different topics, according to the category they are directed to.
3. Educational games: A number of studies have proven the effectiveness of educational games in raising the level of cyber awareness and are directed towards those under 18 years old.
4. Victims' stories: A neglected entity but can prove instrumental in raising awareness. People can become conscious while using cyber applications if they get testimonials from cyber victims and learn how even simple action can cause severe damage. Social media, television, websites can be used to relay these stories to people and let them know that ordinary people can also become a victim of cyberattacks.
5. Blogging, special publications, television programs, advertisements, hoardings can also be utilized to increase awareness among those sections of society which are not alert about the dangers of internet if not used properly.

Incident Response

The massive increase in cybercrime demonstrates the need for strategies to address these attacks. In [19], authors discussed the UK's approach to countering these attacks, with an explanation of the importance of participation by all. The United Kingdom has established a Government Response Center (the new National Cyber Security Center (NCSC)), which is a bridge between the government and users and is the source of advice and guidance on cybersecurity. The importance of developing basic criminal laws against cyber-crimes would enhance users' confidence in cyberspace. The Anti-Cyber Crime Law in the Kingdom of Saudi Arabia was established in 2007 (ACCL). It defines crimes and their penalties, and covers the basic areas for combating cybercrimes, such as data interference, privacy infringement, maintaining public order and morals, as well as punishing attempts to commit cybercrimes even if they do not succeed. However, this law does not provide adequate protection against identity theft and does not adequately protect data privacy. The definition of bullying in this law does not contain provisions against aiding or abetting the commission of a cybercrime. Saudi Arabia has also established a national CERT (Computer Incident Response Team) (CERT-SA, 2018). It is a group of information security experts responsible for protecting against security incidents, discovering them, dealing with them and responding to them, as well as providing instructions on how to deal with incidents [20]. Despite having CERT in Saudi Arabia, our survey reveals that cyberattack victims seldom report to the authorities. There are several reasons behind this hesitancy on the part of victims. One, the people are not aware that there is a government authority to which they can report the attacks, second, there is a lack of interactive portals/applications through which they can report the crime and third, they don't care as they don't understand the consequences of a simple cyberattack. To overcome this issue, an incident response strategy is needed focusing on the importance of easy and interactive cyber incident reporting and, speedy response.

To have a successful incident response strategy, policy and proper planning are necessary. Without them, security incidents cannot be resolved in time. Planning: The effectiveness and efficiency of incident response depend on coherent and lucid planning. Planning defines the role and responsibility of the stakeholders; procedures and processes to undertake in events of incidents, continuity plans etc. When cyber-attacks occur, it is best to have ready procedures, tools etc. to investigate the attacks, limit their spreading and stop them from turning into disaster or crisis.

Policy: A policy is the law or order of guidelines for reaching specific goals. This is done by clarifying the steps and being implemented as a protocol. Incident response policy may explain:

- The way the incident response program works.
- The expectations from the program.
- Whom to contact, how to report an incident.
- Management members.
- Various governmental and non-governmental constraints.
- Incident response procedures and processes.

Incident response strategy

Well-prepared strategies are essential in the event of a cyberattack. The most important strategy is protecting the state's infrastructure. When a cyber incident is reported and is accepted and contained and treated before more damage occurs can be attributed as an effective incident response strategy.

There are a number of steps involved in incident response strategy:

- The attack. When it occurs, it may be a simple virus in the form of a code that infects a computer or a complex multi-stage malware by cyber criminals/ agents. The organization detects the attack using security sensors or control devices.
- Investigation of the attack. After the attack is discovered, the process of investigating the attack begins and gathering evidence to ensure that the sensor has reported an active cyber-attack, then the incident response process begins.
- Containment. After investigating the incident and the response of the agency, it moves to contain the attack, first removing the attacker, then fixing the vulnerability that allowed the attacker to enter.
- Reform. The defenders repair the damage, return the agency to normal operation, and officially close the incident.
- After the accident. After handling the incident, attacks from the same attacker are followed up using the same tools and techniques to detect it and respond quickly, which increases security.

Cybercrime reporting

There are ways through which people can report cybercrime but these are not specific, well known and interactive. In the event of a cyber-crime or cyberattack some questions must be addressed, like:

- Are there competent authorities that the victim can turn to report the crime?
- If there is a competent authority, will it be known to everyone?
- The procedures used for reporting the crime are simple or complex?
- It is important when a cyber-crime occurs that there are official bodies that the victim can resort to report the crime and try to reach the person responsible, either through the helpline number or a website.

There are sites that provide these procedures, for example in the Kingdom of Saudi Arabia, there is a site of the National Cybersecurity Authority (NCA). CERT is a part of NCA. The victim can report the cyber incidents through emails, or logging into their Absher (a governmental portal for residents and citizens) account. The victim is required to fill out certain fields for reporting with attack details data knowing that this data will be dealt with complete confidentiality. But such kind of sites are not known to all members of society. Therefore, it is necessary for the awareness and training program to include the definition of such sites and their importance in trying to reduce cybercrimes as well as to address them and to help address security vulnerabilities. We recommend the use of hotline numbers, applications through which victims can report the issue quickly without delay. Dedicated smartphone application having simple and interactive interface should be developed to address the reporting issue. A 27 X 7 Hotline numbers should be publicized to reach every section of society. NCA should provide separate reporting mechanisms for individual users as well as organization. NCA also provides a platform where organizations can report vulnerabilities in applications. NCA then publish these vulnerabilities. After fixing them, updates are also published by NCA.

Comparison

In this section, we present a comparison (Table 7) of our proposed framework with other awareness frameworks. Based on the target audience, we compared our framework with other available frameworks. We found many articles [5], [7], [21] etc. assessing the level of cybersecurity in either educational institutions or private/public organizations. We assessed the cybersecurity awareness among people from formal and non-formal sectors. Our framework provides an all-inclusive approach of creating awareness among the masses to circumvent any cyberthreat vector. The frameworks [22], [23], [24], [25], and [26] are directed towards either academia or organizations. Moreover, these frameworks do not particularly focus on incident reporting and response process and people from non-organized sectors.

Table 7. Framework Assessment

Framework	Educational Institution	Organizations	General Public	Incident Reporting
`Proposed Framework	✓	✓	✓	✓
[22]	X	✓	X	X
[23]	✓	X	X	X
[24]	✓	X	X	X
[25]	X	✓	X	X
[26]	X	✓	X	X

Conclusion

The cyberspace is not limited to only tech savvy people but general people of all sorts. So, the need for cybersecurity emerged. It is important to spread awareness and educate users about the risks of cyberspace and how to protect themselves and their data while using internet-based applications as well as when cyber-attacks occur and the ability to deal with them. In this paper, we conducted a survey aimed at all age groups in Saudi society that examines the users' behavior about their use of technology as well as their background knowledge in terms of information security. The result showed a lack of awareness in cybersecurity. And, since the Kingdom is considered a target for cyberattacks, and there were a number of attacks that targeted important and vital areas therefore, awareness is important for people, especially non-tech. Based on our survey and available research, we proposed a cybersecurity framework to increase the level of awareness among Saudi people. The framework delivers components which aim at training in schools, universities and organizations, with clarification of policies at each point along with the training programs, their components and the tools used, to suit all groups and interests. Our framework also targets the section of people who are neither school/college/university students nor employees in any organization. So, reaching this section and creating awareness about cybersecurity is very crucial in having a robust defense against the cyberattacks. Apart from these creating awareness, our framework considers the element of incident response and its related policy and planning and, illumination of its importance in responding to attacks and the ability to deal with the incident.

Acknowledgements
The authors would like to extend thanks to College of Computer and Information Sciences, Majmaah University for providing support for this study.

References

[1] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," 2021.

[2] M. M. Al-Daeef, N. Basir and M. M. Saudi, "Security awareness training: A review," 2017.

[3] L. Ajmi, N. Alqahtani, A. U. Rahman and M. Mahmud, "A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia," 2019.

[4] F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, "A review of using gaming technology for cyber-security awareness," 2016.

[5] W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. International Journal of Advanced Computer Science and Applications, p. 3., 2021.

[6] H. De Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," 2017.

[7] R. Sabillon, J. Serra-Ruiz and V. Cavaller, "An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada," 2019.

[8] N. Kortjan, "A cyber security awareness and education framework for South Africa," 2013.

[9] N. H. Abd Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," 2015.

[10] H. Tianfield, "Cyber security situational awareness," pp. 782—78.

[11] N. Gcaza and R. von Solms, "Cybersecurity Culture: An ill-defined problem," pp. 98--109, 2017.

[12] I. Alsmadi and M. Zarour, "Cybersecurity programs in Saudi Arabia: issues and recommendations," 2018.

[13] F.F Alotaibi, "Evaluation and Enhancement of Public Cyber Security Awareness," 2019.

[14] M. Hathaway, F. Spidalieri and F. Alsowailm, "Kingdom of Saudi Arabia cyber readiness at a glance," 2017.

[15] A. Al-Sheikh, "Cyber Security Framework Saudi Arabian Monetary Authority," 2017.

[16] "Cybersecurity Framework" https://thehackernews.com/2019/07/best-cyber-security-frameworks.html, 2019.

[17] E. Kritzinger, M. Bada and J. R. Nurse, "A study into the cybersecurity

awareness initiatives for school learners in South Africa and the UK," 2017.

[18] B. Gardner and V. Thomas, "Building an information security awareness program: Defending against social engineering and technical threats," 2014.

[19] J. Saunders, "Tackling cybercrime--the UK response," pp. 4--15, 2017.

[20] T. S. Alshammari and H. P. Singh, "Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index," Archives of Business Research, vol. 6, 2018.

[21] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," Big Data Cogn. Comput., vol. 5, no. 2, May 2021, doi: 10.3390/BDCC5020023

[22] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," PeerJ Comput. Sci., vol. 7, p. e703, Sep. 2021, doi: 10.7717/PEERJ-CS.703.

[23] H. K. Alkahtani, "Raising the Information Security Awareness Level in Saudi Arabian Organizations Through an Effective Culturally Aware Information Security Framework - Search." , Doctoral Thesis, Department of Computer Science, Loughborough University, 2018.

[24] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," Inf. 2021, Vol. 12, Page 417, vol. 12, no. 10, p. 417, Oct. 2021, doi: 10.3390/INFO12100417.

[25] M. Hijji and G. Alam, "Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees," Sensors (Basel)., vol. 22, no. 22, Nov. 2022, doi: 10.3390/S22228663.

[26] F. A. Almarshad, A. I. A. Alzahrani, and G. Wills, "A Framework to ensure Information Security Awareness in the Middle East," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 22, no. 1, 2022, doi: 10.22937/IJCSNS.2022.22.1.76.