IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 3, 2020, accepted March 18, 2020, date of publication March 27, 2020, date of current version April 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983280

Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions

HUSSAIN ALDAWOOD, (Member, IEEE), AND GEOFFREY SKINNER, (Member, IEEE)
School of Electrical Engineering and Computing, University of Newcastle, Callaghan, NSW 2308, Australia

Corresponding author: Hussain Aldawood (hussain.aldawood@uon.edu.au)

ABSTRACT Social engineering is one of the biggest threats organizations face today, as more and more organizations are adopting digitalization. In the context of cyber security, social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal. For better implementation methods against social engineering, this qualitative study will attempt to provide measures against information security challenges faced by organizations. The analysis is then provided by the answers of interviewed experts in the field of cyber security and social engineering. The research herein focuses on the human element of cyber security threats, recognizing that hackers exploit the vulnerabilities and lack of awareness of staff. Then using these issues to create security loopholes and engineer cyber-attacks that include the interruption or infection of information systems, transfer of unauthorized funds, and stealing of credentials. The results of this qualitative study highlight that there is a positive relationship between social engineering and user awareness. The findings build upon the researchers' ongoing work, which postulates that as an increase in contextual social engineering knowledge leads to a decrease in being victims of social engineering and is, therefore, one of the most effective mechanisms for managing social engineering.

INDEX TERMS Cyber security social engineering, training and awareness programs, information security awareness programs.

I. INTRODUCTION

With the changing landscape in the operation of businesses, digitalization is a must for most sectors and nearly all organizations [1]. However, within such a digital environment, it is difficult to comprehend each aspect of operations and interactions that are taking place. The cyber-world and technological infrastructure are complex, spanning a network of custom-made tools and technology that may be on-premise within an organization, on the cloud or in a combination of internal and external data storage. While operating in the cyber world, organizations need to protect information and secure the privacy of their operations. The challenges of securing information today can be observed by the increase in the extent and nature of cyber-crimes [2]. Information systems today are more exposed to cyber-crimes than ever before.

The number of cyber-crimes against organizations has been increasing according to many scholars. Cyber-crimes include intrusion into organizations' computer networks and disseminating computer viruses [3]. Computer network-based attacks primarily exploit protected organizational information. Hackers usually start analyzing an entire network infrastructure of an organization to collect as much information as possible and exploit open ports or vulnerabilities. Network-based attacks also include unauthorized access to organizational resources [4], [5]. Information systems of modern organizations also face threats from viruses that are disseminated by hackers to access sensitive information, misuse data, or even send malicious information.

Cyber-attacks may target the technical part of a system, but other types of attacks are designed to target the human element and rely on personnel vulnerabilities. These attacks are considered socially engineered incidents. Humans are psychologically manipulated to perform a specific action that can potentially lead to leakage of confidential information [6]. Socially engineered attacks are designed for employees to leak classified information that can be used to damage an organization's resources or harm its reputation.

The nature of most social engineering attacks is spontaneous. Attackers select their targeted organizations on the

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

basis of ease of access to sensitive data in the due process. Organizations with information systems that have few security measures to secure their data appeal to and become great targets for social engineers [7].

II. THE RATIONALE FOR THE RESEARCH

The advancement of technology and the ubiquitous presence of digital devices have increased the need for cyber security. Frumento [8] listed statistics on social engineering attacks, estimating the number of cyber-attacks on private or government organizations. He highlighted that hackers are more inclined to use human vulnerabilities in an attempt to gain access to organizational systems than to focus on the lapses in a system's hardware or software. He also claimed that only 3% of the attacks target the technical infrastructures of organizations. On the other hand, 97% of malware attacks targeted users through social engineering hacking attempts. The motivation for this study is driven by professional experience, clearly identified contemporary issues in the research domain, and a very strong personal interest in the area. The rationale for the research derives from the key problem of numerous organizations worldwide seeking ways to address overall employee lack of awareness of cyber security social engineering vulnerabilities.

The first author was working professionally as an information and cyber security professional at Saudi Aramco, the largest oil-producing company in the world, for eight years, which gave him a solid experience in the field. During his professional life, the world witnessed the worst hack ever seen in history. Saudi Aramco was hit with an extensive cyber-attack back in August 2012. Officials later confirmed that the virus's goal was to shut down oil and gas distribution to regional and international markets. The final investigation report was released stating that the virus (Shamoon-1) was behind the attack. In a matter of hours, 35,000 computers were partially wiped or totally destroyed. This particular incident gave him clear insight into why such huge corporations need to secure their data. Managing supplies, shipping, and contracts with governments and business partners during the crisis was forced to happen manually on paper. The company confirmed at a later stage that one of the main causes of this particular incident was the lack of staff information and security awareness. He was part of the IT and security recovery teams during this crisis and it took them a significant amount of time to recover all the systems. Until the information systems were completely recovered, the cost was extremely high, especially as the production and distribution of oil to international markets was disrupted for almost two weeks. Recognizing employees' lack of information security awareness pushed him to seek to conduct further research on the subject. The researchers of this project opted to interview professional information security experts about their deep experience in the field and present it in an academic setting in order to find new methods to address the issue.

Additionally, it has been confirmed in literature that various techniques of social engineering cause issues of cyber security threats in diverse environments [5]. As social engineering manipulation techniques are evolving with the evolution of cyber technologies, this research is critical in highlighting social engineering threats to organizations. Today, those threats are becoming the mainstream method of attacking dedicated organizational cyber systems across the globe. This study is imperative as it also sheds light on hackers' ability to attack organizational security design at various complex levels by exploiting their human layer of security [9]–[11]. This study will further lead to an exploration of measures and solutions that help organizations mitigate such cyber-attacks and highlight susceptible patches that organizations need to address on their human resource level.

The study will also investigate the significance of employees' information security awareness in determining the efficiency of safeguards established by organizations. It will highlight that as the efficiency of socially engineered attacks is dependent on the person or virtual psychological manipulations of employees, their containment measures should also be developmental in nature such as user-specific interventions. Furthermore, for better implementation methods against social engineering, this study will attempt to provide measures against challenges faced by organizations [12]–[14].

III. METHODOLOGY

A. THE OBJECTIVE OF THE ONLINE INTERVIEW QUESTIONNAIRE

Qualitative research approach was used to obtain subjective views on understanding human behavior related to cyber security and more specifically to social engineering awareness. This research performs a qualitative analysis of recognized cyber security professionals' responses to formulated interview questions in the context of social engineering awareness. Additionally, the aim of this study is to find the best working tools to mitigate social engineering threats besides awareness programs and then provide reliable solutions to create such a safe work environment. The researchers sought participants from senior information security professionals in organizations that have substantive business processes dependent on information and communication technology (ICT) systems to share their experiences of the latest practical solutions to protect from social engineering threats.

B. HYPOTHESES

A. Cyber security professionals rate social engineering as one of the highest contemporary security threats.
B. Cyber security professionals endorse and advocate user awareness programs as the most effective countermeasure for addressing cyber security social engineering threats.

C. RESEARCH DESIGN AND DATA COLLECTION PROCESS

Semi-structured online questions in this research were guided by the use of a pre-constructed thematic theoretical framework based on a literature search along with the

component-model of cyber security. Questions were structured regarding different scenarios in which users experience security demands in their organizations, primary and secondary causes of social engineering threats and then best measures used to mitigate these threats.

Experts in the field were identified by conducting an Internet search (using Google, Google Scholar, LinkedIn, Twitter) of individuals with strong expertise in cyber security. Their contact information was known from their personal websites, publications, Twitter or LinkedIn pages.

Identified experts were sent email invitations along with the information statement of the project. Those who agreed to participate by replying in the affirmative to the email were sent a second email containing a URL Hyperlink and a 6-digit code to complete an anonymous online questionnaire. The 6-digit code was only used to gain authorized (not authenticated) access to the questionnaire and was the same non-identifiable code for all participants. The questions were based around one's insights, opinions and experiences regarding the most up-to-date measures, tools and solutions against social engineering threats. We were particularly interested to know if the theoretical solutions, which we investigated from the literature, correlate with industrial and commercial solutions used to mitigate social engineering threats. We anticipated their responses that were formulated on their professional experience as it pertains to cyber security. All questions were factual and as such, no sensitive or personal information was to be collected in the questionnaire.

D. POPULATION AND SAMPLE

The researchers sought to have 10 to 20 participants from all of the stakeholder groups combined. As this study would be conducting thematic analysis, more interviews than the minimum number will improve the overall quality of the research. Also, a number of participants between 10-20 is more commonly seen in semi-structured studies in information systems domain i.e. human-computer interaction (HCI) [15]. The researchers ended up receiving 21 full participants that can be used for this study.

E. PARTICIPANTS' CHARACTERISTICS

As mentioned earlier that twenty one cyber security experts completed the online questionnaire successfully. Regarding the highest level of educational qualification, eleven participants had a master's degree and ten had a Ph.D. The majority of the security experts had more than fifteen years of experience in cyber security. All security experts were full-time employees. Table 1 summarizes the participants' profiles. Figure I categorizes the industry type that our participants belong to while figure 2 shows their education qualifications.

F. QUESTIONS

The researchers used eight questions in the online questionnaire, which are included in Table 2.

TABLE 1. Participants' characteristics.

No	Level of Education	Years of Experience	Type of Industry	Role
P1	PhD	30+	Education	Professor of Practice in information security risk mgmt.
P2	PhD	25+	Education	Associate Professor in information security
P3	PhD	15+	Education	Senior Lecturer in information security
P4	PhD	10+	Education	Postdoctoral Research Associate in information security and privacy
P5	Master	10+	Banking	Risk Assessment Manager
P6	Master	15+	Government	Information Security Monitoring and Incident Response Manager
P7	PhD	20+	Training	Cyber Security Trainer
P8	Master	20+	Telecom.	Cyber Security Manager
P9	Master	25+	Government	Information Security Manager
P10	Master	10+	Oil & Gas	Senior Information Security Analyst
P11	PhD	20+	Consulting	Information Security Consultant
P12	PhD	15+	Consulting	Information Security Consultant
P13	Master	20+	Government & Research	Chief Information Security Officer
P14	Master	20+	Oil & Gas	Cyber Security Manager
P15	Master	15+	Software services	Software Security Specialist
P16	Master	10+	ICT	Information Technology Manager
P17	Master	15+	ICT	Cyber Security Analyst
P18	PhD	15+	Research	Cyber Security Researcher
P19	PhD	10+	Research	Cyber Security Researcher
P20	Master	10+	Banking	Information Security Specialist
P21	PhD	15+	Government	Cyber Security Consultant

G. METHOD OF DATA ANALYSIS

The received information was analyzed statistically as a qualitative approach was followed. Theoretical thematic analysis was used to analyze and interpret the data because of its flexibility to be utilized across a range of epistemological and theoretical approaches, its ability to identify emergent themes to aid improvement of the theoretical frameworks, as well as its ability to reinforce existing components of the framework [16]. After the targeted number of participants was reached, their data were coded into categories, themes, and concepts [16]–[18]. Thematic analysis is defined as 'a method for systematically identifying, organizing, and offering insight into patterns of meaning (themes) across a dataset' [16].

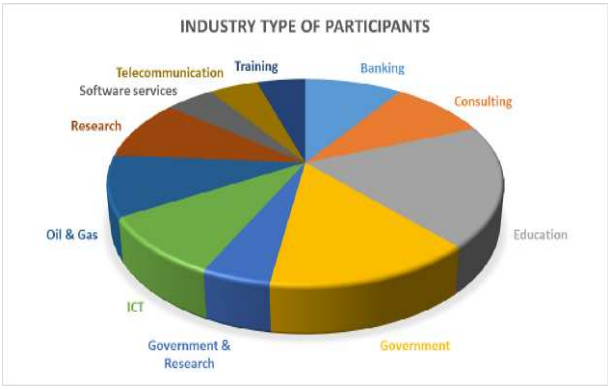

FIGURE 1. Industry types of participants.

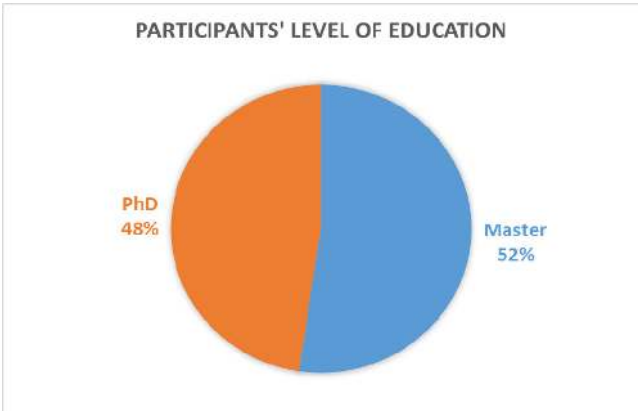

FIGURE 2. Participants' level of education.

H. CODING AND SEARCHING FOR TERMS TO IDENTIFY THEMES

Themes were identified and elaborated, as shown in Table 3.

IV. RESULTS AND DISCUSSION

A. CURRENT SOCIAL ENGINEERING IMPACT

In the last five years, there have been several cyber security issues and threats with advancements in technology. With the expansion of data use, there is a massive breach of data, and as a result, selling of personal data on the dark web has become a very normal practice. According to most of the respondents of our interview questions, the biggest threats of cyber security include ransomware, phishing attacks, botnets, computer viruses, worms, and leakage of data. While one of the respondents cited in the interview that ''Information security threats can be divided into technical cyber-attacks and social engineering attacks,'' one of the critical reasons for social engineering is the lack of awareness of end-users. This deficiency of awareness has made social engineering very easy for attackers. In the field of cyber security, social engineering plays a significant role. However, this type of threat can be avoided by providing proper awareness programs. Through the interviews, participants elucidated that the majority of individuals and organizations invest a lot of time, money and efforts in securing the technical tools and ignore the most important factor, which is developing the human knowledge. One of the respondents stated in the interview that, ''Without investing time, money and efforts in the social engineering attacks, we are not secure.'' The same respondent also stated ''Phishing and pretexting combined account for 98% of social engineering attacks. Personally, I believe that the risk of social engineering is higher than any other cyber attacks since there is no button that we can click to enable the human firewall.'' Interview participants also indicated that the victims are usually not aware of the consequences of replying to or clicking a link to update some sensitive information. For other respondents, phishing emails were the biggest threat causing damage to the infrastructures of information systems. Furthermore, respondents pointed out that the major cyber security incidents include the incidents which took place in Stuxnet, Target Sony, Facebook and subsidiary Instagram security and privacy malpractices and leaks, Uber database leak, Adobe leak, Careem, Yahoo mail credentials leak, Equifax, NetEase, LinkedIn, Anthem, RS, spyware, DDOS attack, and Cambridge Analytica.

TABLE 2. Interview questions.

Interview Question	Purpose
What have been the biggest cyber security issues/threats/incidents in the last 5 years? What role or impact did social engineering have?	Current social engineering impact
What do you see as the biggest cyber security issues/threats/incidents in the next 5 years? What role or impact do you think social engineering will have?	Future role of social engineering
Do you feel that social engineering issues cannot be solved by purely technical solutions? If so what other methods/processes/tools/policies etc. do you deem most effective?	Mitigating the issue of social engineering
What role/impact do you think user awareness plays in managing or preventing cyber security incidents?	Impact of user awareness in managing cyber security incidents
Do you feel user awareness programs and training would be effective in combating social engineering threats and incidents?	Effectiveness of user awareness programs and training
What types of user awareness measures do you think are most effective in combating cyber security threats? What do you feel might work best in the context of social engineering threats?	Types of user awareness measures that are most effective in combating cyber security threats
Do you think cyber security and social engineering awareness training should be compulsory for all users/employees in an organization? If so, with what regularity should this type of training be conducted (for example: only at induction, weekly, monthly, annually, etc.)?	Cyber security and social engineering awareness training
Do you have any other specific comments in relation to social engineering and user awareness you would like to make?	Obtaining conclusive thoughts

TABLE 3. Searching for terms to identify themes.

Theme	Role
Present Social Engineering Impact	Social engineering attacks; Massive data breaches; Selling personal data in the dark; Ransomware, phishing attacks, botnets, computer viruses & worms. Hacking, Insider threat, Data leakage. Hacking, Insider threat; technical cyberattacks; SQL injection; Facebook and subsidiary Instagram security and privacy malpractices and leaks; using Gmail to spread a fake document that opens a google login screen look-a-like to steal user credentials and the phishing on a hotel chain reception employees that exposed guests credit card information; 1. Equifax 2. NetEase 3. LinkedIn 4. Anthem 5. RS; Spyware compromise systems and gain access to confidential user data; loss of confidential data, finances, intellectual property, and consumer credibility; security is the most important issue for business leadership; Cambridge Analytica.
Future Role of Social Engineering	Trading personal data; attackers will exploit various techniques and combine them together to gain access to personal data; Blockchain Hacking and Cryptojakcing, Machine Learning attacks, AI-based attacks, IoT based attacks etc; training to employees so they can recognize a phishing; Ransomware, Phishing, Data leakage, Hacking, Insider threat; phishing emails; Scanning & Enumeration; Cloud Security; targeting ICS system; Data breaches: 1. Phishing emails 2. Free WIFI 3. Social networks phishing 4. DDOS 5. Supply chain attack.
Effective Solutions for Social Engineering	Awareness; enhancing information security culture; Providing training to employees so they can recognize a phishing attempt; Employing a policy of least privilege for user accounts in your system; Using custom anti-phishing solutions to detect falsified emails; awareness and training; Educational organizations and schools; human factors perspective involving psychologists; mitigating risks
Impact of user awareness in managing cyber security incidents	Major role; Mitigating human mistakes; detecting threats; reporting; ensure compliance; training plan; User awareness; increase their level of experience; knowledge of dealing with security threats; improve employee skills and security skills; human factor is the weakest link in the cyber chain; Lack of knowledge and weak of awareness.
User Awareness programs and training in combating social engineering threats and incidents	Awareness programs; Ineffective; gamification and rewards; Reduces errors, Enhances security, Educated staff increases compliance, Can help to protect a company's reputation; Knowledge; process to measure their users' capabilities of dealing with security threats by doing fake threats scenarios frequently; defend against social engineering; significant improvement.
Effective user awareness measures in combating cyber security threats	Gamification and reward programs; awareness; face to face training online training; Effective Security Strategy; Defensive Practices; Tackle Human Error; Checking and updating Advance program; user awareness; Workshops, sessions, courses; Framework / Guideline (NIST /COBIT / ISO); Training; SETA (security, education, training, awareness) programs.
Cyber Security and Social Engineering Awareness Training	Awareness through gamification or reward systems for enjoyment; Awareness through quarterly or annually; a good security awareness program should educate employees; security culture; new employees with a refresher on an annual basis; compulsory and regular for all employees; depends on the user role and department; Upon violation, there should be a deduction in the points; Policy should be updated; gap analysis should be done to identify the baseline then start the training plan; individual security factors and information security awareness factors.
Social Engineering and User Awareness	Educate staff on the cyber threats; Raise awareness of the sensitivity of data; Reduce the number of data breaches; social engineering will be a hot security issue forever; many human factors/vulnerabilities that social engineers trigger/take advantage of; AWARENESS is the best solution to mitigate that risk; strong and solid security rule and actions; New solutions should be explored; relationship between social Engineering and User Awareness.

Respondents confirmed that due to the unpredictable nature of social engineering threats, leading to the loss of confidential data, intellectual property, and consumer credibility could be an expected consequence. Conclusively, it was indicated that there is a need for individuals and organizations to be more mature in handling threats of social engineering. Comprehensively, social engineering plays a significant role in addressing the set of actions necessary to avoid such risks.

B. THE FUTURE ROLE OF SOCIAL ENGINEERING

It was observed from the interview that targeting the human knowledge will remain a significant threat in the next five years. Trading of personal data in the dark web and subsequent breach of the data will be the most significant issues of cyber security.

However, a few respondents were not clear about whether social engineering will continue to be the primary determinant as individuals are becoming more aware of those attacks. One respondent stated, ''One can predict that the attackers will exploit various techniques and combine them to gain access to personal data.'' New attacks which the industries must be aware of include the hacking of the blockchain, crypto hacking, machine learning attacks, and AI-based attacks, while in the current time, social engineering plays a major role. Henceforth, there is a need to provide training to staff so that they can better recognize these attacks.

There were also some other respondents who highlighted that phishing emails could be the next upcoming threat since the victims fail to identify the well-designed social engineering attacks. For example, one of the respondents manifested in the interview that, ''Social engineering needs to address numerous actions in order to handle sensitive data and ensure it is encrypted.'' However, from the interview, it was discerned that threats like ransomware, impersonation/pretexting, phishing, leakage of data, hacking and insider threat continue to be the major threats for companies. One of the interviewees also cited that, ''It will be the same thing given people like to pontificate about how great users can be while ignoring the systemic failings of their security programs.'' Additionally, organizations, which have insufficient controls and security procedures against revealing sensitive information will continue having their vital user data leaked. Furthermore, it was mentioned in the answers that companies must be aware of social engineering threats and hence must maintain a sufficient level of awareness of their users. Therefore, in order to identify such threats as responding to generous rewards or feeling pressured to act immediately to suspicious emails, one needs to be aware of the social engineering techniques.

It was also learned from the interview that some of the recent and trending threats included accessing free and public Wi-Fi and supply chain attacks. Very critically, one of the respondents elucidated in the interview that, ''Moving forward the element of deception is likely to be more

emphasized. My reasoning for this is that the major solution offered against social engineering is through education and awareness. I do not believe that these are successful. Instead, the criminals will play upon the established trust and confidence that users may gain through this education. A current example is the fake AV software. One might argue that education often makes people consider that they are in danger, without training them how to respond appropriately.''

Additionally, Internet of Things (IoT) is an ever-augmenting technology that is offering both economic and technological advantages. The primary reason for their increase is that more devices are becoming connected and hence creates more and more attack surfaces while the social engineering threat agents are becoming smarter as their methods and strategies are evolving. One of the interviewees also stated ''In addition to the diversity and simplicity of the techniques and forms that can be followed in social engineering, the human is the weakest link in cyber security so in my point of view it has an absolutely huge impact.''

C. MITIGATING THE ISSUES OF SOCIAL ENGINEERING

According to the majority of the respondents, technical solutions alone are not sufficient, although they are necessary. The respondents very clearly highlighted that raising awareness of end-users is one of the most effective methods of mitigating the threat. Overall, training and the enhancement of the information security culture are necessary in mitigating the threats of social engineering. One of the respondents mentioned a few useful counters to phishing emails and other social engineering attacks. One suggested countermeasure was staff training so employees can recognize phishing attempts. Respondents also included some other solutions to mitigate the overall issue with social engineering, suggesting having strong security policies in place and using custom anti-phishing solutions to detect suspicious emails that contain unknown links or requests for information from social engineers. Henceforth, according to the interviewed experts, there is a high need for the enforcement of policies. Raising awareness and training end-users with the sole purpose of understanding malicious intents is essential to maintain a reasonable level of awareness. On the other hand, updating the technical tools could also help in mitigating the threats and closing some of the gaps. For example, one of the respondents manifested in the interview that, ''In my opinion, social engineering plays an important role. However, some purely technical solutions will require another level of protection, such as encryption and encapsulation.''

Since social engineering is complicated, varied and comes from different platforms, technical solutions alone cannot resolve it. It was pointed out from the study that governments should step in to help regulate and enforce security laws to improve the desired actions against social engineering. There is also a need for educational organizations and schools to provide related training. With regards to this, one of the respondents stated, ''Educational organizations and schools provide the best way of educating Internet users about Internet security and Spyware awareness. These educational organizations could introduce nationwide programs that would provide information for their students through certain courses and materials about Internet security. These educational organizations can have much influence. The knowledge of students at educational institutions of awareness of Internet security issues has been increasing in recent years, as explained.'' Moreover, the same expert further pointed out that, ''Providers of antivirus and anti-spyware protection software should include easy understanding instructions with their software. The user interface of the software should be easy to use according to a user's level of experience. It is important that protection software is both easy to use and efficient in order to provide higher levels of protection against Internet attacks. A good and usable user interface will increase a user's confidence in operating the software and also their knowledge of Spyware and similar threats. A user will be more likely to use the software appropriately if it is not difficult to use, thereby leading to greater protection against malicious attacks.''

Conclusively, government awareness campaigns, educational institutions, corporate training programs, and social awareness events in improving user awareness levels play a major role in developing human knowledge. Subsequently, those types of programs and events provide examples of how to identify social engineering attempts.

D. IMPACT OF USER AWARENESS IN MANAGING CYBER SECURITY INCIDENTS

The results of the interview conducted highlighted important information. The majority of the respondents stated that user awareness plays a significant role in managing or preventing cyber security incidents. Primarily, it helps in the mitigation of human mistakes, and helps users detect threats and report them, especially in the realm of security. One of the interviewed experts stated, ''Security training allows organizations to influence behavior, mitigate risk, and ensure compliance. There are countless benefits of initiating security awareness training in your company.'' Respondents emphasized that keeping information safe is not only the responsibility of information security professionals but also the responsibility of everyone within the organization. Therefore, all users must be aware, not only of their roles and responsibilities in protecting information resources, but also how they can protect information and respond to any potential security threat or problem. One respondent shared that ''In my opinion, I believe that the responsibility of making the data of any organization secured is everybody's responsibility inside the organization. Absolutely, user awareness is essential to increase their level of knowledge of dealing with security threats.''

Awareness helps in reducing undesired mistakes made by end-users. Awareness is also the last defense line wherein all the technological solutions will fail when a social engineer invites others to click a link, install malware, or simply give away their credentials.

E. EFFECTIVENESS OF USER AWARENESS PROGRAMS AND TRAINING

It was found from the respondents that the current practices of user awareness programs could be improved by adopting modern awareness programs. Hence, there is a need for contemporary techniques that utilize gamification and rewards until cyber security protection becomes a social norm. These user awareness programs are primarily useful in offering benefits like reducing errors, enhancing security, increasing the level of awareness of staff, and overall protecting the company's intellectual properties. Additionally, the experts confirmed that in order to have a positive impact, training should be a continuous process because after a few months, the users will most likely go back to their original state. One of the respondents stated, ''I feel it is effective, in a way that if the users become aware . . . Humans are the weakest link! The more they become aware, the less the issues regarding social engineering become prevalent.'' Another respondent stated, ''User awareness programs have shown their effectiveness in the organization where I work and similar organizations. We have seen significant improvement in users being able to detect social engineering attempts and resisting the pressure.'' Additionally, organizations need to have a transparent process in measuring their user's capabilities of dealing with security threats by doing fake threats scenarios frequently. Conclusively, effective implementation of security awareness programs helps in the reduction of the risks of cyber threats targeted at exploiting people.

F. TYPES OF USER AWARENESS MEASURES THAT ARE MOST EFFECTIVE IN COMBATING CYBER SECURITY THREAT.

The primary role of awareness campaigns is to provide a suitable means of improving user awareness. Users must be introduced to the sensitivity of data and how revealing a small amount of sensitive information can lead to full-blown social engineering attacks. According to the interviewed experts, there are different types of user awareness programs that exist. The most common types of cyber security awareness are traditional programs and non-traditional programs. Traditional programs tend to be face-to-face trainings. Relatable measures include training workshops, gathering sessions, and courses. Non-traditional programs include simulations, gamification and reward programs, and online training. Primarily, the company should first develop an effective security strategy to ensure that every employee within the company understands the importance of cyber security and the far-reaching impact. Next, the company should keep defensive practices up-to-date, and subsequently should adopt modern non-traditional security awareness training. One of the respondents, while conducting the interview, cited that ''I feel the training and simulation of social engineering attacks internally would be fruitful to enhance the overall effectiveness of combating social engineering.'' One of the other respondents cited in the interview that ''Phishing campaign exercise time to time. Until culture changes I do not believe that the positive effects of current user awareness initiatives. It should be retained as is, but new techniques need to be explored to guide behavior''. Conclusively, SETA (Security, Education, Training, Awareness) is determined to be the most effective tool in combating cyber security threats.

G. CYBER SECURITY AND SOCIAL ENGINEERING AWARENESS TRAINING

Pertaining to whether cyber security and social engineering awareness training should be compulsory for all or not, critical answers and insights were observed during the course of interviewing the experts. One of the respondents critically replied to this by stating ''No! I believe that awareness programs should be designed in a way that they can sell themselves without the need to force individuals to adopt them. If they are designed using gamification or reward systems, individuals will adopt them as they find enjoyment in engaging with such programs.'' Respondents also weighed in on the frequency of training programs. Some of the respondents stated that training should be done on a monthly basis. Others think quarterly works better while some others argued that the cycle of awareness should take place once a year. Each group justified their answers. For example, one of the responses stated that ''Awareness programs should be compulsory on a monthly basis and if employees made a mistake or violated what has been demonstrated in training, they lose some points toward their yearly performance. On the other hand, another expert stated that ''I think it depends on the user role and department, some users have to be made aware of general things like viruses more frequently (quarterly), however, those who carry advanced security knowledge like IT and security staff should be reminded and updated once a year.'' In short, the most significant point was that these programs should be continuous in the process of having passive engagement, and then embed awareness into the process of securing sensitive data. Social engineering training should be a requirement for all staff including new hires with a refresher on a regular basis. Also, testing employees and training them through emailing them fake phishing scenarios can help keep employees conscious.

Regardless of frequency, a good security awareness program must have a clear objective of raising staff awareness on corporate security policies and procedures for working with information technology (IT) and the policies pertaining to the user awareness programs must be kept updated. Moreover, the interviews confirmed that the status of how well an organization is maintaining a reasonable awareness level can be measured by the number of incidents over time.

H. CONCLUSIVE THOUGHTS

The last question the experts were asked was if they want to add any comments regarding social engineering and user awareness. Most of them confirmed that social engineering does not require any technical background, and it is a very easy, cheap and effective way to gain unauthorized access

to sensitive information. As a result, investing in humans is the key, no matter what advanced technology one uses for protection. There is a need to raise staff awareness on cyber threats. Another point experts emphasized was the need to ensure that procedures and policies are followed correctly in organizations. As the complexity and sophistication of social engineering increases, so should the user awareness. It was observed from the experts' comments that by using and adopting these measures, the number of data breaches can be potentially reduced. Most of them also indicated that social engineering will be a hot security issue forever. Overall, awareness is by far the best solution for mitigating the risk. However, user awareness is only a partial solution. Henceforth, new solutions should be explored in complementing this necessary factor. With regard to this, one of the interviewees also stated "I believe cyber security awareness is everyone's responsibility. So, awareness should start at home as we have to make our children aware to know how to stay safe online and warn each other of any cyber security tips that could keep us secure." This battle of cyber security cannot be won with just one weapon, instead, integration of contemporary education and technology are all needed. Conclusively, there is a positive relationship between social engineering and user awareness as an increase in knowledge leads to a decrease in being victims of social engineering.

V. CONCLUSION

Today, organizations are greatly dependent on information systems. This reliance has led to vulnerability to information security threats that put data and people at risk. Furthermore, social engineering fraud has been increasing with advancements in technology. Social engineering is defined in several studies as manipulating and persuading people to disclose sensitive information through online networks or by granting access to restricted areas or systems. Criminals are getting more sophisticated in finding new ways to attack. As a result, organizations have been increasing their investments in cyber security initiatives to safeguard their data. Additionally, some governments such as Australia have started legislating different laws and regulations against cyber criminals to ensure the protection of citizens and organizations from social engineering attacks and other cyber-related crimes. However, keeping up with perpetrators is challenging.

Information security awareness is a crucial step towards having a secure cyber environment in which all types of computer users' (end-users, technical users, employees in different departments, etc.) skill aptitude levels can freely use technology to conduct positive and self-developing activities. This research aims to find the best working tools to mitigate social engineering threats and to find reliable solutions to create safe work environments. The researcher sought participants who are senior IT cyber security professionals in organizations that have substantive business processes dependent on information and communication technology (ICT) systems to share their experiences with the latest practical solutions to protect against social engineering threats. The results of this study highlight that there is a relationship between social engineering and user awareness. Based on the authors' ongoing research and coupled with Industry experts' responses provided in this paper, it is believed that an increase in targeted contextual social engineering awareness and cyber security organizational culture leads to a decrease in being victims of social engineering.

ACKNOWLEDGMENT

Hussain Aldawood would like to acknowledge the full scholarship from the Saudi Ministry of Education to study the Ph.D. degree with the Faculty of Engineering and Built Environment, University of Newcastle, Australia.

The authors would like to thank our colleagues in GulfNet Solutions (GNS) Company Limited, who provided expertise that greatly assisted the research. They have to express out appreciation to Mr. O. Aldulaijan, GNS General Manager, for sharing his pearls of wisdom with us during the course of this research.

REFERENCES

[1] Z. L. Svehla, I. Sedinic, and L. Pauk, "Going white hat: Security check by hacking employees using social engineering techniques," in *Proc. 39th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2016, pp. 1419–1422, doi: 10.1109/MIPRO.2016.7522362.

[2] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cyber security," in *Proc. EM Conf., Int. Technol., Educ. Develop. Conf.*, 2017, pp. 1–8.

[3] G. N. Reddy and G. J. U. Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," 2014, *arXiv:1402.1842*. [Online]. Available: http://arxiv.org/abs/1402.1842

[4] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in *Proc. IEEE Int. Conf. Teach., Assessment, Learn. Eng. (TALE)*, Dec. 2018, pp. 62–68, doi: 10.1109/TALE.2018.8615162.

[5] H. Aldawood, T. Alashoor, and G. Skinner, "Does awareness of social engineering make employees more secure?" *Int. J. Comput. Appl.*, vol. 177, no. 38, pp. 45–49, Feb. 2020, doi: 10.5120/ijca2020919891.

[6] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proc. 28th Int. Conf. Hum. Factors Comput. Syst. (CHI)*, 2010, pp. 373–382.

[7] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: An analysis of students' individual factors," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 352–359, doi: 10.1109/Trustcom.2015.394.

[8] E. Frumento, R. Puricelli, F. Freschi, D. Ariu, N. Weiss, C. Dambra, I. Cotoi, P. Roccetti, M. Rodriguez, and L. Adrei. *The Role of Social Engineering in Evolution of Attacks*. [Online]. Available: https://www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf

[9] K. Thomas, A. Moscicki, D. Margolis, V. Paxson, E. Bursztein, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, and V. Eranti, "Data breaches, phishing, or malware?: Understanding the risks of stolen credentials," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2017, pp. 1421–1434.

[10] R. Heartfield, G. Loukas, and D. Gan, "An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks," in *Proc. IEEE 15th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, Jun. 2017, pp. 371–378.

[11] A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," *Comput. Secur.*, vol. 52, pp. 128–141, Jul. 2015.

[12] R. Alavi, S. Islam, H. Mouratidis, and S. Lee, "Managing social engineering attacks-considering human factors and security investment," in *Proc. HAISA*, 2015, pp. 161–171.

[13] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 145–149, doi: 10.1109/FiCloud.2016.28.
[14] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Secur. Privacy*, vol. 12, no. 1, pp. 28–38, Jan. 2014.
[15] A. Blandford, "Semi-structured qualitative studies," in *The Encyclopedia of Human-Computer Interaction*, M. Soegaard and R. F. Dam, Eds., 2nd ed. Aarhus, Denmark: The Interaction Design Foundation. 2013. [Online]. Available: http://www.interactiondesign.org/encyclopedia/semi-structured_qualitative_studies.html
[16] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Res. Psychol.*, vol. 3, no. 2, pp. 77–101, Jan. 2006.
[17] M. B. Miles, A. M. Huberman, M. A. Huberman, and M. Huberman, *Qualitative Data Analysis: A Methods Sourcebook*. Thousand Oaks, CA, USA: SAGE, 1994.
[18] B. L. Berg and H. Lune, *Qualitative Research Methods for the Social Sciences*. Harlow, U.K.: Pearson, 2012, p. 408.

HUSSAIN ALDAWOOD (Member, IEEE) received the B.S. degree in management information systems from The University of Arizona, Tucson, AZ, USA, in 2009, and the M.S. degree in business administration from Florida Atlantic University, Boca Raton, FL, USA, in 2015. He is currently pursuing the Ph.D. degree in information systems (cyber security) with the University of Newcastle, Callaghan, NSW, Australia.

From 2010 to 2018, he was an Information Security Professional with Saudi Arabian Oil Company (Saudi Aramco). Since January 2019, he has been a Casual Academic with the School of Electrical Engineering and Computing, University of Newcastle. He has also been the Director of Cyber Security in GulfNet Solutions Company (GNS), since December 2019. He is the author of several cyber security articles. His research interests include cyber security, social engineering threats and solutions, and information security awareness programs.

Mr. Aldawood became a member of ACM, in 2018. He is also a member of various committees and institutions on information security, cyber security engineering, and project management. He was a recipient of many prestigious and international honors and awards. He is also internationally and professionally certified by ISACA, ISO, PMI, PECB, CompTIA, EC-Council, including the following certifications: CISM, CISA, PMP, DRP, Security+, ISO27001, ISO27005, ECIH, and others. He is a Research Reviewer of several journals.

GEOFFREY SKINNER (Member, IEEE) received the B.E. degree in computer engineering from the University of Newcastle, Callaghan, NSW, Australia, and the Ph.D. degree from the Curtin University of Technology, Bentley, WA, Australia. Since 2006, he has been working as an Academic with the School of Electrical Engineering and Computing, University of Newcastle. His research interest includes cyber security, data security, security, software development, and information privacy.