Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal

Hussain Aldawood *hussain.aldawood@uon.edu.au*
School of Electrical Engineering and Computing
University of Newcastle
Newcastle, 2308, Australia

Geoffrey Skinner *geoff.skinner@newcastle.edu.au*
School of Electrical Engineering and Computing
University of Newcastle
Newcastle, 2308, Australia

Abstract

Social engineering is a major threat to organizations as more and more companies digitize operations and increase connectivity through the internet. After defining social engineering and the problems it presents, this study offers a critical review of existing protection measures, tools, and policies for organizations to combat cyber security social engineering. Through a systematic review of recent studies published on the subject, our analysis identifies the need to provide training for employees to ensure they understand the risks of social engineering and how best to avoid becoming a victim. Protection measures include awareness programs, training of non-technical staff members, new security networks, software usage, and security protocols to address social engineering threats.

Keywords: Social Engineering Threats, Social Engineering Measures, Security Policies, Social Engineering Tools, Social Engineering Solutions.

1. INTRODUCTION

This paper is an extension of work originally presented in the 26th International Conference on Systems Engineering (ICSEng 2018), which took place in Sydney, Australia on December 18, 2018 [1]. The cyber world today plays a major role in increasing connectivity among people from across the globe. With this ubiquity of the internet, there are inevitable threats that have also grown over time. Crime related to the internet and the cyber world is categorized as ‘cybercrime.’ Cybercrime poses a threat to economies, as well as individual safety and has been identified as the primary medium of terrorism [2]. The extent of organized threats from cybercrime is assessed by many recent studies and reports. An example provided in [3] addresses the convergence of cyber and terrorism. The rate of cybercrime is accelerating rapidly and has surpassed the rate of traditional crimes in certain countries of the European Union (EU). Some recent reports also link cyber menace to other forms of terrorism such as human trafficking.

The definition of a socially engineered attack as stated by [4] is “a psychological exploitation which scammers use to skillfully manipulate human weaknesses and carry out emotional attacks on innocent people.” Social engineering goes beyond the technical vulnerability of the users’ system. It is the act of deception in which victim users are manipulated into revealing information to a perpetrator who then performs tasks pretending to be the target user. The breached computer is then used without their knowledge for acts that may be viewed as an abuse of the authorized use [4, 5]. The kinds of threats that users are exposed to as a result of social engineering include phishing of confidential information and targeted attacks based on information gained. Such socially engineered cyber-attacks include the interruption or infection of complex information systems, transfer of unauthorized funds, and stealing of credentials [6, 7].

The methods of cyber-attacks today go beyond hardware and software tools. Recently, some of the fastest-growing corporate crime threats have steered away from exploiting systems or vulnerabilities on information security, and instead have focused on humans, a target considered to be the weakest link in every organization [8, 9].

This study aims to conduct a critical appraisal through a systematic review of contemporary policies, measures, and tools used to address social engineering. This study is developed based on identified expertise on the subject matter of social engineering through research, interviews, and industry conferences to critically evaluate the tools that help in the prevention of social engineered attacks in an organization.

Setting up controls for socially engineered attacks is essential in light of the damages these attacks can cause. One of the most notable incidents of social engineering includes the sabotage of manufacturing plants in Germany in December 2014. The hackers used the technique of targeted phishing emails that captured a user's credentials to gain access to the back office and production network, causing massive damage to the plant [10]. Another attack was that on the Ubiquiti Network, San Jose, a California-based networking equipment company where it lost approximately $46.7 million dollars to a spear phishing email attack of which only a fraction was recovered [11]. In both incidents, the attackers identified human flaws to induce cyber-harm.

With respect to social engineering attacks, organizations cannot be completely protected as there is a 'human factor' involved that can be influenced to facilitate or even initiate an attack [12]. However, organizations can ensure the containment of such attacks and impede their success by adopting security policies [13, 14]. Email security is among the primary security measures that can be adopted. Organizational policies should maintain email security gateways through tools such as Sender Policy Framework (SPF) to identify origins of emails, DomainKeys Identified Mail Policy (DIMP) with a cryptographic signature that ensures the validity of the email signature and non-modification of in transit [14], [15]. The most advanced version of email security is the Domain-based Message Authentication Reporting and Conformance (DMARC) which uses SPF and DIMP to restrict any unidentified email [14].

Real-time blocking on the basis of hostname and server IP for identifying a malicious email is another measure against social engineering. The security policies of organizations should further have in place an attachment type restriction blocking the file types that would be considered as risky such as, ".386", ".perl", and ".ws" formats among others. Apart from email security, endpoint security measures such as updating antiviruses, anti-malwares, host-based intrusion detection system (HIDS) are other popular methods to contain socially engineered attacks on firms [15].

However, even with such technologies, studies indicate that organizations still have to focus on training their employees to increase their preventive measures. Awodele et al. [16] suggest that a successful defense against social engineering activities has to have not only good policies but also security education for employees. The remainder of the paper is structured as follows: A methodology is provided in section 3, followed by the critical appraisal in section 4, the implications of the research detailed in section 5, and paper conclusion in section 6.

2. BACKGROUND

As the digital universe becomes progressively more integrated and complex with daily life, there are several methods in which cybercrime can affect people. Attacks towards organizations are unrelenting, and among the most prevalent attackers are cybercriminals who have the ability to accurately assess people or situations and exploit their weaknesses. These attackers employ social engineering as their dominant attack method [17]. Hackers have started to shift from automated exploit attacks to more personalized attacks that take advantage of flaws. Social engineering enables cybercriminals to induce victims to create vulnerabilities, infect systems, transfer funds, and steal credentials [8, 18].

Social engineering methods use psychological tricks to create deception. Social engineers prey on unsuspecting users and work towards gaining access to information. Broadhurst and Chantler [19] argued that employees are becoming primary targets for social engineers and cybercriminals. The authors indicated that gaining access to information is only the first step in any cyber-attack. As soon as the user-access information is available to the hackers, usually a secondary attack is then launched on the targeted organization's computer system. This is then turned into a tertiary attack on the main target of the system control program of the organization, where telecommunication, financial, or database information is exposed. In its tertiary attack, the 'access information' gained from the primary user allow attackers to bypass existing security measures. Attackers look for sensitive information sources including usernames and passwords, Personal Identification Numbers (PINs), and credit card and banking information. They even have the capabilities to modify, erase, or copy information to comply with the needs of their attack, once they have access to organizational system vulnerabilities.

Results of a survey by ICASA [17] display that a high number of respondents did not know about breaches they had experienced in the past. In terms of social engineering, employees are responsible for securing their organizational data. If staff do not protect their own information data, they could cause harm to the corporation for which they work. Employees can easily become exposed to advanced persistent threat (APT), especially if they have their cyber credentials stolen. The threat actors can then exploit their organization at advanced stages. These trends indicate the need for enterprises to create better monitoring systems and enhance their ability to track user behavior through better interpret logs. Additionally, organizations have a potential need for employee skills enhancement that helps them to identify and understand socially engineered attacks on their enterprise.

Social engineering attacks are not only becoming increasingly common but are also becoming progressively more sophisticated and complex. Hackers are coming up with ever-more-clever tricks for fooling individuals and employees into handing over valued and sensitive organizational data [20]. Under such circumstances, firms need contemporary and holistic cybersecurity social engineering solutions to stay ahead of cybercriminals. This study includes contemporary measures, policies, tools, and applications required to increase the level of awareness of staff and help them to better recognize social engineering techniques. These measures will further reinforce organizational preventive measures against socially engineered attacks and prevent them from succeeding.

3. METHODOLOGY

A systematic review of literature was done in this study to assess the current industry measures, polices, and tools to address social engineering threats. The analysis will further examine results attained by organizations after adopting the various efforts. The study used various literature-finding strategies and databases, along with criteria to determine the inclusion and exclusion of literature. The search strategy used was based on recommended measures, policies, and tools to tackle social engineering threats. The study used various databases in order to find literature that identify or present measures, policies, and tools adopted by industries to tackle social engineering threats. The databases used are Embase, EBSCO, Google Scholar, and IEEE Xplore. The search strategy used keyword patterns in order to search for relevant literature. The keywords used are 'social engineering', 'cyber threats', 'social engineering threats', 'social engineering measures', 'social engineering policy', 'social engineering tools', 'social engineering solutions', 'social engineering applications', 'software for social engineering threats', and 'tools and software for social engineering threats'. Literature or articles with one or multiple appearances of keywords were considered for eligibility criteria. A total of 2,973 relevant pieces of literature appeared against the keywords used. In order to segregate and filter out the studies, eligibility criteria of the literature were implemented to determine whether a book would be included or excluded for the study.

The exclusion criteria are:

- Literature with only abstract available or restricted access for reading
- Literature with incomplete information
- Literature published in foreign language and not English
- Literature published before year 2001

The inclusion criteria are:

- Literature with full access and complete information
- Literature published in English language only
- Literature with at least one of the keywords
- Literature published since 2001 in full text and until 2018
- Literature that only focuses on social engineering threats and strategies or solutions
- Literature may comprise of research papers, grey literature and PhD theses
- Literature that present tools as solutions and are used in general by organizations.

Tables 1 through 3 describe the characteristics of the studies included in the present systematic review to highlight the measures, policies, and tools that institutions have adopted. The present review includes thirty studies from the year 2001 to 2018 that show the evolution of technologies and techniques, which tend to prevent social engineering. 10 of each for measure, policy, and tools of social engineering were chosen to avoid biases of the studies. Total literature are the total count of articles for every keyword used in searching literature. The literature was already segregated for every systematic review for social engineering related measures, policies, and tools. The rejection of articles was based on the exclusion criteria.

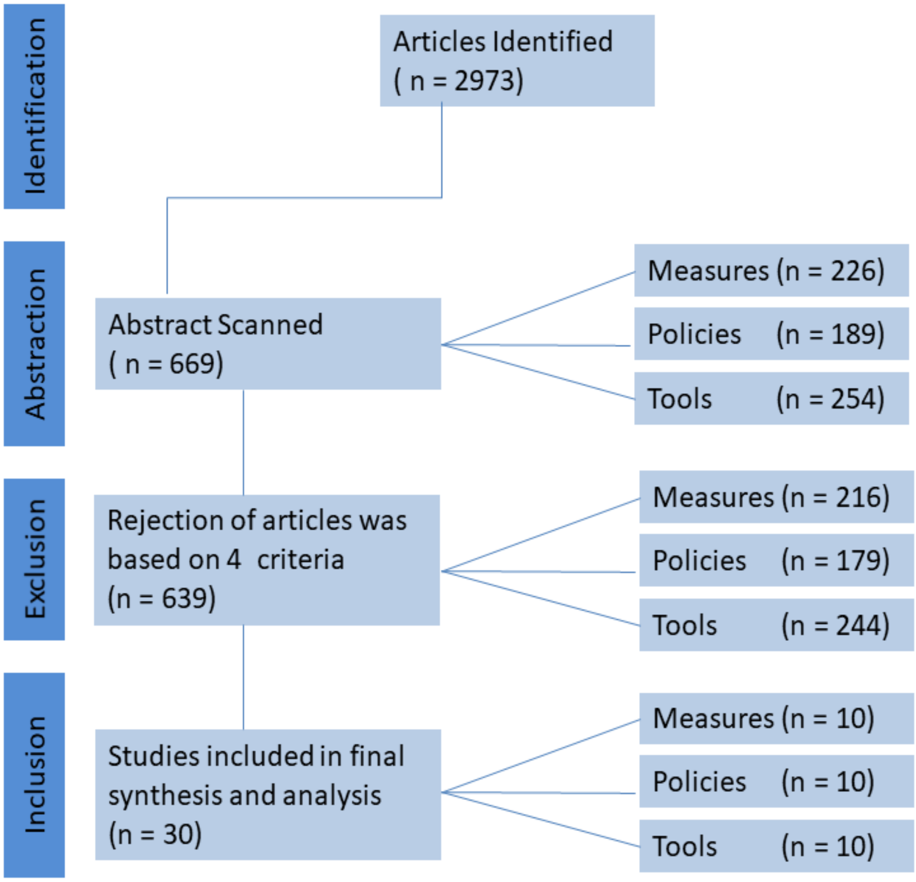

FIGURE 1: Inclusion & Exclusion of Studies.

4. CRITICAL APPRAISAL

4.1 Systematic Review of Knowledge Based Measures

Social engineers usually break into information systems of organizations by bypassing technical security tools such as firewalls. Measures or counter-measures for such socially engineered attacks include preventive habits that organizations need to improve in their own employees. The measures are designed to override the psychological stratagems of attackers and keep users' data such as security codes, usernames, and passwords safe [21, 22]. The primary measures to counter socially engineered attacks emphasize education, training, and development of awareness programs among staff [23].

End-users should be very careful with applications that attempt to gain unauthorized access to their operating systems. These attempts usually happen through the process of self-installation of software or applications which aim to extract user specific information at later stages. However, staff are unlikely to evade social engineering attacks without periodically reviewing the newly-used methods of social engineers to attack the human factor. Employees tend to trust others by nature and may give out sensitive information as a result. Companies need to educate staff about common manipulative methods used by hackers and constantly remind staff of how their vulnerability can cause harm to the organization [23]. Their enlightenment through the measure of education has the potential to diminish employees' vulnerability to hacking while performing online activities [24].

Measure	[R]	Method	Results	Conclusion	Limitation
Education	[25]	Teaching staff electronically	Enhanced behaviors	SE developed defense.	Qualities of staff
	[26]	Reminding personnel about social networking periodically	Driven staff to do self-study in their own time	Contemporary teaching plans for each education level	Staff naivety of threats.
	[27]	Teaching staff about SE common deceptive approaches	Conscious workforce to react positively	Avoiding SE attempts	Relying on human skills
	[21]	Teaching staff about best behavior during an attack	Alerted staff	Limiting expansions of incidents when taken place	Various qualities of human adaption to instructions
Training	[22]	General SE training	Efficient on protection strategies	Training staff to identify threats	Financial resources
	[28]	Penetration training	Prepared staff	Being prepared can stop being attacked	Funding
	[29]	Training on safe behaviors e.g. password safe keeping	Being perceptive of defensive procedures	Adopting preventive techniques in employees' behavior	Depends on the skill sets of individuals
Awareness Programs	[8]	Awareness programs on recognizing attack models	Being alert of recent SE methods	Raising overall awareness of threats	Staff negligence
	[19]	Awareness programs via posters	Improved knowledge to identify SE attacks	Increasing awareness on SE threats	Qualities of staff
	[30]	Awareness on categorizing sensitive data	Being able to classify confidential data	Preparing employees to catagorize information sensitivity	Depends on the level of persuasion of others

TABLE 1: Knowledge Based Measures against SE.

Security awareness in any organization should be implemented with a formalized plan. It is important for employees to be periodically educated and tested through internal certification programs about their knowledge of commonly-used social engineering tactics by hackers. This training should address their malicious intention to exploit the human weaknesses. Many scholars including [18, 21] confirm that it is critical to keep staff prepared to practice their duties and behave safely in the workplace. Although firms use a number of technical security tools including intrusion detection systems, social engineers are still more likely to be capable of divulging sensitive information by manipulating human knowledge. Firms can address the root cause of employee-based weakness through an I-E model, where ‘I’ represents human’s internal nature and ‘E’ refers to the external influence they are subjected to. Organizations can also use subjective defense measures of educating their personnel through training awareness programs and models meant to detect human emotions. These training awareness programs help employees to become more aware of their weaknesses to ensure they are not deceived by hackers in real attacks [22].

An important part of the protection process against social engineering attacks requires organizations to train their new hires before they are given access to organizational information systems. Including an introductory information security awareness program as part of the orientation for new hires can help an organization avoid being victim to socially engineered attacks. The education of new hires should be arranged frequently through different means to increase their security knowledge base [12]. Effectiveness of learning can be enhanced through the use of interactive videos. Interactive videos allow management to pass information security announcements to their employees in an effective, fast, and economic way. Training staff through information security videos enhances learners’ engagement to better understand the mechanism of social engineering attacks. This training method also gives employees flexibility in accessing the training materials, so they can learn at their own speed by replaying some segments or even skip the parts they already know [31].

All measures for countering socially engineered attacks are organization-specific and are developed as user interventions. Through formal workshops, lectures, and internet-based learning tools, organizations inculcate employees on interventions or precautions that are necessary to identify an attack before it takes place. Employees also need to be more aware of how to identify and verify if the person they are dealing with is a social engineer. This process of being able to recognize a social engineer can be developed through well-designed awareness programs. As the internet world is dynamic, these countermeasures ensure that employees are updated on recent types of attacks. Educating employees with the help of social engineering penetration testing can also make employees ready for a real life scenario. Furthermore, implementing penetration testing can help management monitor and measure the effectiveness of their current security education and awareness programs. Raising the level of employees’ awareness creates a human firewall ensuring that users are self-reflective in recognizing they have been attacked or are a part of an elaborate social engineering hack experiment [24]. Table 1 presents popular measures adopted by organizations universally against social engineering.

4.2 Policies

Organizations use policy statements to enhance their information security measures against social engineering attacks. The policy statement outlines the desired personnel behaviors. The policy statements further define the direct consequences of not following organizational policies countering a social engineering attack. Firms develop policies to counter socially engineering attacks on the basis of creating a safe working culture. Additionally, a policy is formulated on the basis of expected behavior from employees that the organizational management aims to maintain within the business. Policy statements are needed to determine the difference between day-to-day functioning and the expected behavior from each employee within the firm [32].

Instituting comprehensive cyber security policies and procedures for all staff, vendors, and partners in an organization is one of the best security measures against social engineering attacks [33]. Specifically defining precise social engineering policies is also becoming important to safeguard companies' intellectual properties. These security rules and policies are usually developed for organizational benefits to help employees in both detection and prevention phases from social engineers' recent deceiving methods. Further, instituting preventive measures through policy statements allows staff to be aware of the guidelines and enables them to assess whether they are facing a legitimate request from authorized people or are facing social engineers. Policy approaches as a defense mechanism, such as setting clear desk policies, will protect sensitive information including passwords. Another example is the use of paper shredders, which will prevent information from being leaked through dumpster diving. Contemporary security policy statements may also implement caller ID for authorized personnel to identify themselves through the latest technology tools. This policy decreases the chances of being a victim and improves the mitigation rate against social engineering attacks [2, 12].

Policy initiatives may also include guidelines defining sensitive information and its usage in the enterprise. Policies stating access and authorization control with data classification and security strategies will prepare employees to encounter socially engineered attacks and face them while under attack [5, 26].

Periodic auditing and monitoring of the implementation of security policies improve the overall safety of an organization. Active auditing helps organizations to increase the chances of identifying and recognizing a real social engineering attack at an early stage. This monitoring routine strengthens the organizational data protection plans against social engineering manipulation methods. Monitoring the implementation of security policies also helps organizations to notify staff members in case of a potential problem. This early detection procedure helps reduce the total time required to address any violation to existing policies. Furthermore, auditing helps in defining the threats to and vulnerabilities in information systems. Conducting internal and external reviews enhances the overall auditing applicability of policy intervention in firms. Internal audit reports are usually examined by a firm's security council and designed to suit employees' needs and requirements in protecting against social engineering attacks. On the other hand, external audits increase overall security by pointing out glitches unnoticed by internal auditors [34].

Policies	[R]	Method	Results	Conclusion	Limitation
Desk Policies	[21]	Shredding printouts containing sensitive data	Clean desks sensitive information	Desk policies avoids dumpster diving	Different behavior of staff
Destruction	[35]	Better safekeeping classified information by shredders	Classified data couldn't be taken from recycle bins	Protection through retention and destruction policy	Different behavior of staff
Sensitive Data	[5]	Limiting accessibility to sensitive data to authorized personnel only	Data leakage threat is mitigated	Policy for managerial authorization to sensitive information	Dependent on staff compliance
Classifications	[36]	Guidelines for labeling the level of data classification	Data is categorized in groups e.g. (public, classified)	Classification policies increase the vigilance in the firm	Lack of clear policy statement classifying the roles
Security Audit	[37]	Auditing practices to test the level of staff awareness	A security culture is maintained due to reg. auditing	Auditing policies contain the spread of an attack	Dependent on staff capability of compliance
Plug-in Devices	[38]	Disallowing plug-in storage devices in organizational workstations	There is no backdoor of information being shared	Disallowing these devices prevents from unauthorized access	Increasing the hustle of data sharing in firms
Social Media	[39]	Minimizing the number of staff accessing social media websites	Threats of social media is reduced	Controlling the access of staff to social media avoids SE breaches	Employees' private devices to access these websites

New-Hire	[40]	Screening new hires before joining an organization	Having an insider threat is minimized	Hiring staff with a credible background prevents against SE	Inaccuracy of background checks
Physical Security	[41]	Adopting biometric for all staff to enter organizational locations	Illegal access to buildings is limited	Biometrics policies help against unauthorized access	Biometrics can be hacked
Compliance	[38]	Mandatory compliance monitoring system	A security culture is maintained	Compliance policy ensures the practice of security	Compliance monitoring is time intensive

TABLE 2: Policies to Prevent Social Engineering Attacks.

4.3 Tools

The most powerful tool that an attacker uses in a socially engineered attack is the access to knowledge pertaining to an organization as well as its users [21, 42]. Since social engineering hackers frequently use manipulation, a breach of a system of an organization can be controlled by preventive tools such as firewalls, network security tools, and incidental response handling tools. The studies shown in Table 3 reveal some of the tools that have been developed to counter the vulnerabilities existing in information systems. Tools to counter a socially engineered attack are developed by organizations on the basis of aggregate implementations that were available during the time [37, 38]. Additionally, as socially engineered attacks are developing with time, firms also need to work on the improvement and adoption of new tools that can prevent leakage of valuable information [41].

Tools	**[R]**	**Method**	**Results**	**Conclusion**	**Limitation**
Network Security Tools	[14]	Updating network tools e.g. content filtering via proxy setting	Developed network-based tools against SE threats	Enhancing firewalls stops attacks	Reliant on routine updates
	[13]	Network-based Intrusion Detection System (NIDS)	Recognizing spammers, fake profiles by NIDS	NIDS is practical in identifying SE threats	Skills of staff vary
Biometrics	[43]	Biometrics e.g. voice signature, face recognition & fingerprint	Illegitimate access is blocked	Biometrics confirms users identity	SE attacks are evolving over time
Artificial Intelligence (AI)	[44]	Introducing Artificial Intelligence to identify phishing attacks	Identifying a SE attack before launched	AI prevents SE attacks	Financial funding as it's still expensive
	[45]	Neuro-Fuzzy	Secure online transactions in real time	NF provides defense on user-behaviors	Technical knowledge of staff
Config. Tools	[15]	Restrictions on received email attachment, real-time blocking, geo-location blocking	Immediate protection in the event of contacting staff by social engineers	Pre-configured tools safeguard against SE before happening	Technical training is required for IT staff
tal Respo nse	[43]	Automatic reporting tool to information security response teams	Early detection tool of suspicious activities	Automatic reporting tool can expedite the containment of a threat	Requires well-timed scanning of data

	[46]	Host-based firewalls, isolation of machine or user account access as response tools	Spreading of threats is mitigated	Exposure of threats to the entire network is limited	Need for high tech staff
Patch Mgmt.	[47]	Keeping appropriate applications patches on regular updates	Up to date applications	Being updated helps creating a safe culture	Requires highly skilled IT staff
Penetration Testing	[38]	Conducting penetration testing (PT) regularly	Ready	PT ensures readiness	Incorrect tests may cause a damage

TABLE 3: Tools to Control Social Engineering Attacks.

As socially engineered attacks have become a profitable trade, organizations need contemporary tools to identify their vulnerabilities. Enforcing automatic proxy configurations such as firewall group controls, helps in restricting malicious network activities on the end-user side. Proxy configurations explicitly force any outbound network communications from an organization to be combed through a content filtering proxy. Applying automatic proxy configurations also helps control user access to the Internet through web browsers and provides safer network data trafficking. Forcing legitimate data traffic to be diverted through a proxy server and implementing Egress filtering can prevent malware from affecting organizational information systems. Furthermore, considering the fact that spam domains are not reputation-based, newly-born spam domains in nature can raise an issue. IPs under such newly-born spam are used to launch attacks within minutes of registering existing technologies, which are not always enough to address these issues. However, enhanced spam filtering against the newly-born host inspection trend will provide an additional layer of protection to firms. These contemporary filters are effective in identifying spam, advanced threats, phishing, and social engineering attacks. Additionally, using these filters in combination with fast real-time domain lookups using big data correlation techniques will address the issue of newly-born malicious domains [14].

Reliability of malware detection tools are code-dependent. For additional enhanced protection, biometrics are used to counter the issues for false positives in the identity verification systems. With up-to-date biometric tools such as face recognition, voice signature, and fingerprint, chances of illegal access are minimized. Biometric tools are also strongly linked to employees and their personal identity. Biometric traits cannot be easily duplicated or shared, which makes them more resistant and superior for prevention against socially engineered attacks than traditional methods of passwords alone. Biometric recognition requires users at the time of authentication, which prevents users from refutation false claim and checks attacks on user-level to prevent secondary and tertiary attacks. Furthermore, biometric tools counteract physical methods of safekeeping as authentication, which is not based on perceived identity of employees. Rather, it distinguishes authorized users based on their unique traits of biological nature [43, 48].

Organizations can also adopt neuro fuzzy inference systems using neural networks, for better protection against social engineering. Incorporating fuzzy inference systems, using artificial model are used for their self-learning ability. Logic can be designed to create self-predicting phishing detection approaches and use them for URL blacklists, to ensure hackers are unable to generalize it. Blacklisting sites can prevent attacks on human weakness [43, 48]. Some companies elect to utilize location-based intelligence for better verification of the exact location of authorized person transacting with organizational information systems. This information is usually gathered through devices of the employees and interactions can be verified across special channels. Enterprises further increase their security through Dynamic Security Questions, where firms require employees to keep one step authentication process on personal records, to predict socially engineered hacks [15].

5. ISSUES DERIVED FROM THE LITERATURE REVIEW

The issues related to social engineering, such as phishing, have been around for a long time, with the purpose of gaining access to victims' credentials. These credentials are then used as part of a scheme to infect an organization's database or information system with malicious viruses or malware. However, with the advancement of cyber technologies, emerging issues are becoming more personalized and targeted. The four key fields we have identified as problem areas in the current state of social engineering are Social Phishing, Spear Phishing Attacks, Brand Theft, and Email Fraud.

5.1 Social Phishing

Social phishing uses techniques involving social media accounts of employees on platforms such as Facebook and Twitter. The objective of such attacks is to gain access to the organizational network through social network personal accounts. Attacks are usually designed in the form of posts and links that redirect users to malicious websites. Mirroring of social media pages used by such unsuspecting employees is another access point that social engineers are increasingly using. Fake apps, and links posted by an attacker to attract employees pose a challenge to organizational safety against socially engineered attacks [49].

5.2 Spear Phishing Attacks

Spear-phishing is a preliminary stage in an Advanced Persistent Threat (APT) attack, which is done to create a point of entry into an information system. This type of attack targets a specific group of staff in an organization. Spear phishing is designed through combing social profiles, websites, and blogs of employees. Some phishing attacks may even contain malware such as Trojan, directed for the primary purpose of industrial spying. One of the main objectives of spear-phishing is committing financial frauds [46].

5.3 Brand Theft and Typosquatting

Hackers automate exploits such as brand theft to lure staff. In brand theft, employees are tricked into believing that they are interacting with legitimate services or websites. These socially engineered attacks use methods of typosquatting (URL hijacking) or registering their domain names with minor misspelling. The domains are typographically mangled to trick users who do not pay attention to email headers. Typosquatting leads to trademark infringement and loss of trust in the original organizations [50].

5.4 Email Fraud

Among all the techniques of socially engineered attacks, email frauds are the most dependent on the human factor to succeed. Social engineers use this technique to raise panic among employees. Examples include 'Lawyer's Call', 'job offer letters' or notices from the IRS (Internal Revenue Services). Organizations can be exposed to such attacks, in which the emails are designed to look like they are coming from internal higher management levels. This spoofing trend suggests that socially engineered attacks are adapting and adjusting to organizational efforts in the establishment of preventive measures [51].

However, the literature has clearly indicated paramount to all four of these issues, and the potential root cause for them, is lack of user, administrative, and organizational social engineering awareness. As such, the overarching focus of my research is in the specific context of social engineering awareness within the cyber security domain. More specifically, the current state of the research in this field indicates that social engineering awareness and effective countermeasures to address social engineering threats is severely lacking.

6. IMPLICATIONS OF THE RESEARCH

The reviewed studies point out some limitations that an organization may face while implementing countermeasures, policies, and tools for preventing social engineering attacks. First, a limitation in implementing measures of prevention arises from the capability, skill sets, education, and personality traits of personnel [25-27]. The differences among staff can cause a major challenge in the implementation process of preventive measures. Furthermore, the difference in training needs and level of awareness among employees also limits the success rate of these countermeasures [22, 29]. The techniques of hackers to gain organizational specific information are ever evolving. Safekeeping sensitive data is dependent on the ability of management to persuade and convince employees to change their behaviors toward exposing confidential information that can be used by hackers [19, 42].

An analysis of policy implementation reveals that human errors in following policies is a critical challenge that organizations encounter while handling preventive measures against socially engineered attacks [5, 12, 35]. Literature also suggests that a lack of clear policy statement prohibits employees' capability to understand their roles in the prevention process. Additionally, proactive prevention through surveillance is both time consuming and costly to businesses as it disturbs day-to-day operations [37-39, 52]. Lastly, a limitation in the process of a security policy implementation to control social engineering arises from the restraint of lacking of clarity of policies, and the fact that there are limited tools against such attacks [36, 52].

Our analysis of the preventive tools used by modern organizations against socially engineered attacks identified the limitations that come from new threats that are engineered every day. Tools such as malwares and firewalls also need to be updated regularly to ensure their timely protection of the firm [13, 14]. Additionally, tools such as biometrics offer challenges such as being vulnerable to attacks [44]. The tools of Artificial Intelligence (AI) are expensive to implement and also need a large knowledge base to ensure a holistic protection of information [45, 46]. The level of professionalism, capability, and comprehensibility of employees for using such tools as countermeasures have also been highlighted in literature as an important challenge that organizations encounter in the preventive process [15, 38, 47].

Among the three parameters of measures, policies, and tools to counter socially engineered attacks, the prominent challenge arises from the capability of employees to understand the new ways in which they can be a source of information leakage. Employees' capability to differentiate between confidential and non-confidential information ensures the safety of an organization from social engineering. The critical analyses of the reviewed studies highlighted that this limitation mitigates by increasing user awareness of social engineering attacks [16, 25, 26]. Enhanced information security awareness programs on password protection, non-sharing of any work-related information on social media and other gaming websites can all be included to raise their awareness about the real threats. By implementing these awareness programs, organizations can ensure that their employees are aware of all the latest socially engineering methods and techniques. Such awareness prevents employees from falling prey to attacks [29, 35, 38, 39, 42, 52].

7. CONCLUSION

The evaluation of the reviewed studies for this critical appraisal is analyzed on the parameter of methods employed, results of the study, and conclusions by researchers to identify the limitations posed by adopting measures, policies, and tools. Measures undertaken to control socially engineered attacks include education, training, and increasing awareness among employees. This review also presents an overview of how implementing information security education and awareness programs can be an effective way to increase user knowledge, thus reducing and eventually preventing cyber security social engineering attacks.

Developing and adopting evolving information security policies enhances an organization's overall security culture. Policies such as mandatory compliance, audits, disallowed plugins, and ways to treat and dispose of sensitive information reduce the chances of data breaches and leakage of organizational data. Routine training to fill the knowledge gap of employees about defined security policies will further enforce information security. In brief, for all listed measures suggested in this study, a focus on educating and training an organization's workforce about social engineering threats to raise their knowledge base and awareness is one of the best approaches discussed throughout the literature.

8. REFERENCES

[1] H. Aldawood and G. Skinner, "A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications," in *IEEE 26th International Conference on Systems Engineering*, Sydney, Australia, 2018.

[2] W. Lee *et al.*, "2017 Emerging Cyber Threats, Trends & Technologies Report," *Georgia Institute of Technology,* p. 28, 2018.

[3] E. Europol, "The Internet Organised Crime Threat Assessment (IOCTA) 2016," ed: Europol, 2016.

[4] B. Atkins and W. Huang, "A study of social engineering in online frauds," *Open Journal of Social Sciences,* vol. 1, no. 03, p. 23, 2013.

[5] D. P. Twitchell, "Social engineering in information assurance curricula," in *Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06*, 2007, pp. 191-193.

[6] R. Heartfield and D. Gan, "Social engineering in the internet of everything," *Cutter IT Journal,* Article vol. 29, no. 7, 2016.

[7] R. Lemos, "Expect a New Battle in Cyber Security: AI versus AI," *Symantec Publications,* 2017.

[8] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cyber security," in *em Conference: International Technology, Education and Development Conference*, 2017.

[9] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2018: IEEE, pp. 62-68.

[10] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Industrial Control Systems,* vol. 30, p. 62, 2014.

[11] R. Hackett, "Fraudsters duped this company into handing over $40 million," *Fortune Publication,* 2015.

[12] A. U. Zulkurnain, A. K. B. K. Hamidy, A. B. Husain, and H. Chizari, "Social Engineering Attack Mitigation," *International Journal of Mathematics and Computational Science,* vol. 1, no. 4, pp. 188-198, 2015.

[13] A. Sharifi, A. B. Noorollahi, and F. Farokhmanesh, "Intrusion detection and prevention systems (IDPS) and security issues," *International Journal of Computer Science and Network Security (IJCSNS),* vol. 14, no. 11, p. 80, 2014.

[14] R. Albert *et al.*, "The Future of Ransomware and Social Engineering," *U.S. Department of Homeland Security,* 2017.

[15] R. F. Rights, "Global Information Assurance Certification Paper," 2003.

[16] O. Awodele, E. E. Onuiri, and S. O. Okolie, "Vulnerabilities in Network Infrastructures and Prevention/Containment Measures," in *Proceedings of Informing Science & IT Education Conference (InSITE)*, 2012.

[17] ISACA. State of Cybersecurity: Implications for 2015 [Online] Available: https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[18] H. Aldawood and G. Skinner, "Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering," in *International Conferences on Cyber Security and Communication Systems*, Melbourne, Australia, 2018.

[19] A. N. Chantler and R. Broadhurst, "Social engineering and crime prevention in cyberspace," 2006.

[20] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society,* vol. 32, no. 3, pp. 183-196, 2010.

[21] S. D. Applegate, "Social engineering: Hacking the wetware!," *Information Security Journal,* Article vol. 18, no. 1, pp. 40-46, 2009.

[22] W. Fan, L. Kevin, and R. Rong, "Social engineering: Ie based model of human weakness for attack and defense investigations," *IJ Computer Network and Information Security,* vol. 9, no. 1, pp. 1-11, 2017.

[23] V. Greavu-Serban and O. Serban, "Social engineering a general approach," *Informatica Economica,* vol. 18, no. 2, p. 5, 2014.

[24] D. Airehrour, N. Vasudevan Nair, and S. Madanian, "Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model," *Information,* vol. 9, no. 5, p. 110, 2018.

[25] T. R. Peltier, "Social engineering: Concepts and solutions," *Information Security Journal,* vol. 15, no. 5, p. 13, 2006.

[26] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," in *Internet technology and secured transactions (icitst), 2013 8th international conference for*, 2013: IEEE, pp. 508-515.

[27] W. R. Flores and M. Ekstedt, "Countermeasures for Social Engineering-based Malware Installation Attacks," in *CONF-IRM*, 2013, p. 23.

[28] M. Nohlberg and S. Kowalski, "The cycle of deception - A model of social engineering attacks, defences and victims," in *Proceedings of the 2nd International Symposium on Human Aspects of Information Security and Assurance, HAISA 2008*, 2008, pp. 1-11.

[29] T. Mataracioglu and S. Ozkan, "User awareness measurement through social engineering," *arXiv preprint arXiv:1108.2149,* 2011.

[30] A. Adewole, A. Durosinmi, and M. A. Polyetchnic, "Social Engineering Threats and Applicable Countermeasures," *African Journal of Computing & ICT,* vol. 8, no. 2, 2015.

[31] E. Alkhamis and K. Renaud, "The Design and Evaluation of an Interactive Social Engineering Training Programme," 2016.

[32] O. Buckley, J. R. Nurse, P. A. Legg, M. Goldsmith, and S. Creese, "Reflecting on the ability of enterprise security policy to address accidental insider threat," in *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on*, 2014: IEEE, pp. 8-15.

[33] H. Aldawood and G. Skinner, "An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions," in *2019 the 3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia 2019.

[34] I. Tovstukha and U. Laaneots, "Prevention Strategies For Social Engineering," 2013.

[35] A. Kumar, M. Chaudhary, and N. Kumar, "Social engineering threats and awareness: a survey," *European Journal of Advances in Engineering and Technology,* vol. 2, no. 11, pp. 15-19, 2015.

[36] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Information Systems Security,* Article vol. 16, no. 6, pp. 315-331, 2007.

[37] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," in *Computer and Network Security Essentials*, 2017, pp. 603-618.

[38] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers and Security,* Article vol. 59, pp. 186-209, 2016.

[39] H. Wilcox and M. Bhattacharya. *Countering social engineering through social media: An enterprise security perspective, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9330 LNCS, pp. 54-64, 2015.

[40] R. Gulati, "The threat of social engineering and your defense against it," *SANS Reading Room,* 2003.

[41] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications,* Article vol. 22, pp. 113-122, 2015.

[42] A. Smith, M. Papadaki, and S. M. Furnell. *Improving awareness of social engineering attacks, IFIP Advances in Information and Communication Technology*, vol. 406, pp. 249-256, 2013.

[43] J. D. Bustard, J. N. Carter, and M. S. Nixon, "Targeted biometric impersonation," in *Biometrics and Forensics (IWBF), 2013 International Workshop on*, 2013: IEEE, pp. 1-4.

[44] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *Journal of Network and Computer Applications,* vol. 36, no. 1, pp. 324-335, 2013.

[45] P. A. Barraclough, M. A. Hossain, M. Tahir, G. Sexton, and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions," *Expert Systems with Applications,* vol. 40, no. 11, pp. 4697-4706, 2013.

[46] M. Butavicius, K. Parsons, M. Pattinson, and A. McCormac, "Breaching the human firewall: Social engineering in phishing and spear-phishing emails," *arXiv preprint arXiv:1606.00887,* 2016.

[47] K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks," in *International Conference on Information Resources Management*, 2011: Centre for Information Technology, Organizations, and People, pp. 1-12.

[48] S. S. Mudholkar, P. M. Shende, and M. V. Sarode, "Biometrics authentication technique for intrusion detection systems using fingerprint recognition," *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* vol. 2, no. 1, pp. 57-65, 2012.

[49] A. Elyashar, "The Security of Organizations and Individuals in Online Social Networks," *arXiv preprint arXiv:1607.04775,* 2016.

[50] P. Piredda *et al.*, "Deepsquatting: Learning-based typosquatting detection at deeper domain levels," in *Conference of the Italian Association for Artificial Intelligence*, 2017: Springer, pp. 347-358.

[51] ProofPoint. The Human Factor: People-Centered threats define the Landscape [Online] Available: https://www.proofpoint.com/us/human-factor-2018

[52] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Computers and Security,* Article vol. 56, pp. 1-13, 2016.