International Journal of Computing and Digital Systems
2025, VOL. 17, NO.1, 1-13

http://dx.doi.org/10.12785/ijcds/1571048308

Development of Cyber Security Awareness and Education Framework

Amreen Ashraf M. Sharif[1] **and Jaflah Alammary**[2]

[12]*College of Information Technology, University of Bahrain, Zallaq, Bahrain.*

Received 12 March 2024, Revised 15 June 2024, Accepted 10 July 2024

Abstract: All barriers have been removed by the Internet, which has completely changed how we interact with one another, watch movies, make friends, work, play games, shop, pay bills, listen to music, and place food orders. Key services and infrastructures in our increasingly networked world are based on digital information [1]. There is no doubt about the benefits offered by the Internet, but with all these benefits, there are many disadvantages; one of them is cybercrime, which costs millions of dollars every year. User awareness is considered one of the most significant components when dealing with cyber-attacks. Although numerous efforts (such as emails, posters, in-class instruction, web seminars, and games) are made to raise awareness among people, these efforts often fail to achieve the purpose as these initiatives are often implemented without proper planning as there are no standard guidelines that can be followed when developing awareness initiatives. Thus, the goal of this study is to fill this gap of needing a structured approach to designing awareness programs. This study proposes a framework that can serve as a benchmark for providing guidance on successfully planning and implementing cybersecurity awareness campaigns/programs.

Keywords: Cybersecurity, Cybercrimes, User awareness, Awareness Programs

1. INTRODUCTION

Every day, more and more people are using the Internet, and as a result, society is rapidly transitioning into a "network society." The use of the Internet has skyrocketed globally during the last few decades. Millions of computers connected by an electrical network constitute the Internet. At the beginning of the twenty-first century, there were over 700 million Internet users worldwide [2].

People worldwide utilize the Internet these days to exchange thoughts, messages, opinions, and sentiments. Numerous social media sites, like Twitter, TikTok, Instagram, Facebook, and YouTube, offer users free memberships. Almost 2.7 billion individuals are connected by the borderless virtual environment known as the Internet [3]. These technologies are now necessary for everyone's daily life as well as for societal well-being, economic development, vital infrastructure, and national security [4]. While the Internet has many positive aspects, it also gives hackers and cyber terrorists equal access to the platform [3].

Roughly 143 million American consumers' personal and financial information was stolen in an Equifax hack [5]. According to estimates, cybercrimes cost the world economy over 450 billion dollars. In 2020, the average amount claimed for cyber insurance increased from 145,000 USD in 2019 to 359,000 USD. Hence, the need for improved cybersecurity procedures is increasing [6].

Security can be defined as the process of keeping something safe from harm, theft, illegal access, and loss while upholding strict confidentiality [7]. Every citizen now worries about cybersecurity [8].

Cybersecurity is not limited to technology; it also encompasses the individuals who use technology and are in charge of correctly installing and maintaining it. According to prior research, the majority of cybersecurity issues have been linked to human behavior and activities; as a result, in the people-process-technology cybersecurity triangle, "people" are considered the weakest link. Increasing people's cybersecurity awareness (CSA) is crucial, as it is the first step in managing human aspects [9].

Strong cybersecurity awareness and training programs are essential, given the ever-present threat scenario. These efforts play a critical role in creating a cyber hygiene culture in which Internet users adopt safe online habits and practices as second nature [10].

Developed nations such as Canada, the United States

E-mail address: 20147480@stu.uob.edu.bh, jalammari@uob.edu.bh

(US), and the United Kingdom (UK) have national cybersecurity strategies, action plans, and at least one major campaign launched to raise awareness of cybersecurity [11]. The National Initiative for Cybersecurity Education (NICE) in the United States (US) is an example of such campaigns [12].

A. Problem Statement

People are frequently regarded as the weakest link in the chain of cyber-security [13]. According to recent studies, human mistakes account for 95% of security breaches, as they affect all aspects of information security in businesses and are one of the main causes behind data breaches; hence, the technology-based safeguards are insufficient to guarantee a secure environment. For example, many Internet users still don't know how their gullible actions might jeopardize their computers [14]. User education is generally considered to be one of the most important and widely used tactics for preventing attacks [15]. A program for raising awareness and providing training is essential because it serves as a means of distributing knowledge that is needed by all users, including managers, consumers, and staff. It's the standard method for communicating security requirements and suitable conduct [16]. As a result, many cybersecurity awareness campaigns have been launched to increase awareness among young people to promote safe online surfing and counteract the hazards related to cybersecurity. The structure and material of the programs may differ from one another, but they all serve a similar goal, which is to raise awareness [17].

Although many positive results emerge from such security efforts, not all of them can persuade people to behave securely [17]. Research has cast doubt on the efficacy of these programs in educating the general public, even while they assist organizations in meeting compliance requirements of security standards like ISO and NIST. Typically, educational programs maintain track of the users who completed the training, including the number of attendees at awareness sessions, exam passers, and so on [18]. According to Bada and Sasse, the major goal of security awareness is to "influence the adoption of secure behaviors." Education campaigns are frequently set up as information transfers that ignore the reasons underlying people's actions [17]. Programs for cyber awareness have not produced the desired outcomes [19][20].

Cybersecurity awareness campaigns can fail for many reasons, and it's imperative to be aware of these issues to ensure the effectiveness of such initiatives. One of the common reasons is that they are often implemented without proper planning as there are no standards or guidelines that can be followed, as highlighted in this study, which emphasizes that currently, there are no established, generally recognized standards for educating users about cybersecurity on a societal level. This study raises the question of how a successful education campaign can be created and tailored to the needs of the entire society? [21]. Hence, there is a strong need for clear guidelines to lay the foundation for robust cybersecurity awareness initiatives. Therefore, this study aims to address this gap by providing a comprehensive framework to help understand how to systematically design successful awareness Campaigns or Programs.

B. Objective

The objective of this study is to develop a comprehensive Cybersecurity Awareness and Education framework.

C. Contribution to the Field

The research will contribute to the field of study by filling a major gap of not having a structured approach to designing awareness programs at the national level. The study proposes a standard framework which serves as a benchmark in guiding how to successfully plan and implement cybersecurity awareness campaigns/programs by identifying the key components that must be considered. Additionally, by providing an extensive framework for the execution of awareness campaigns from beginning to end, this framework can aid in the efficient distribution of resources by determining the focus areas of cyber awareness campaigns according to the general public's level of awareness.

The rest of the paper has been arranged as follows: In Section II. The fundamental ideas surrounding cyberspace, its effects, cybercrimes, and cybersecurity awareness and education have been explored. Section III covers the recent studies and the research gap. Section IV provides an overview of the Methodology used to create the conceptual framework. Section V provides an overview of the proposed framework and its components. Lastly, Section VI covers the Conclusion, Future work, Implications, and Limitations of this study.

2. Related Work

A. Cyberspace

The expansion of cyberspace is outpacing the growth of any other resource. Currently, there are about three billion individuals who use cyberspace to access the Internet; this number is expected to rise quickly to five billion users utilizing 50 billion devices [22]. The term "cyberspace" is frequently used and has many different meanings [23]. F. D. Kramer claims that the term "cyberspace" has 28 distinct definitions [24].

Over time, there have been several definitions of cyberspace. It is defined as the interconnected network of information technology infrastructures comprising computer systems, embedded processors and controllers, telecommunications networks, and the Internet, which constitutes a global domain inside the information environment. The human element is absent as this definition only discusses the hardware aspect of technology; software and data are also implied from definition [25]. Cyberspace is characterized by decentralization and the interaction of various interests, constituencies, and actors and is made possible by

institutional organization. All things considered, cyberspace can be summed up as a place where people and processes are predominant. It is constructed in layers, with physical components enabling a logical framework of interconnection that allows the augmentation, manipulation, processing, exploitation, and interaction of people and information [26]. Since access to technology and information is a prevalent feature of cyberspace, it can also be defined as a domain that uses electronics and the electromagnetic spectrum to edit, store, and exchange data via networked systems [27].

1) Impacts of cyberspace

It is reported that there were over 3 billion Internet users [28]; this enormous user base can be attributed in large part to the Internet's widely accessible nature and affordability. The Internet has enabled a vast worldwide network that generates billions of dollars annually [29].

Virtually every traditional activity has a digital equivalent these days due to the increasing relevance of cyberspace in ensuring national security, maintaining economic growth, promoting general prosperity, and providing citizen governance. In addition to paying bills and trading online, we can now conduct banking operations, play games, and correspond with companies, people, and governments. Furthermore, individuals can hold workshops, seminars, and conferences online, work together and share resources, and receive education online by utilizing online infrastructure [26].

Cyberspace is quickly displacing more conventional forms of communication, if not outpacing them. We post electronic messages on bulletin boards instead of attaching slips of paper to wooden notice boards and send emails rather than letters on paper. Letters, books, and other tangible items used in traditional communication are becoming outdated in favor of electronic items [27].

The Internet offers us numerous advantages in our daily lives, but it also has certain drawbacks. Vulnerabilities, hazards, and risks are ever-present in cyberspace, creating opportunities for collusion, exploitation, and conflict. An increasing number of unforeseen vulnerabilities, dangers, and risks are being exposed by the interdependence of people, processes, and technology [26].

B. Cybercrimes

The term "cybercrime" refers to crimes when a computer is used to commit theft or other crimes. In layman's terms, cybercrimes are sometimes defined as crimes performed with a computer and the Internet to steal identity, interfere with operations using harmful software, and stalking. The definition of cybercrime has been expanded by the US Department of Justice to include any act, including the use of a device to store evidence. The growing list of cybercrimes encompasses both computer-based versions of well-known crimes like stalking, stealing, and intimidation as well as computer crimes like the propagation of computer viruses and network intrusions [30]. Cybercrimes are simple to commit since they are easy to learn [27]. Millions of people worldwide are impacted by cybercrime each year. The risk of cybercrime involving computers and/or the Internet exists for individuals, businesses, governments, and international organizations [31].

Cybercriminals persist in leveraging the anonymity and convenience of virtual spaces to orchestrate worldwide attacks, frequently navigating jurisdictional boundaries with great ease. Individuals, businesses, governments, and vital infrastructure are among the victims [32]. Cybercrimes have been on the rise globally despite the efforts to control them. 40% of firms globally have fallen victim to cybercrime, according to the 2019 Cybersecurity Breaches Survey. New and sophisticated methods for committing cybercrimes are constantly being developed by cybercriminals, which has led to an increase in their number [33]. Other figures that highlight the growing detrimental impact of cybercrimes in recent years demonstrate the relevance of these issues. As per IBM 2022a, the average global cost of a cyber event in 2022 was 4.35 million USD, which signifies a 24.29% rise from 3.5 million USD in 2014 [34]. According to official reports, during the first half of 2021 alone, there were over 305 million ransomware assaults worldwide, with over 228 million of those attacks taking place in the United States [35].

Cyberattacks can have major, all-encompassing risks and consequences that impact many aspects of our lives, including risks to national security, disruption of operations, loss of intellectual property, reputational harm, legal and regulatory repercussions, and psychological and emotional repercussions [36].

1) Types of Cybercrimes

The list of cybercrimes is continually growing [37]; they cover a wide range of crimes such as hardware, software, and the human factor [38]. Some of the common cyberattacks have been defined below:

Cyberstalking (CS)

Intimidating a victim through GPS devices, spyware, or hidden cameras, as well as spying on or manipulating their behavior, is known as cyberstalking [39]. Stalking can also be defined as a criminal act that instills in the victim feelings of worry, panic, tension, or fear. Any unsolicited electronic communications that are persistent in nature have the potential to be intimidating, coercive, or threatening [40]. The increase in the use of Internet-enabled devices and services globally, particularly the unrestricted use of social media sites, channels, and apps, has contributed to the rise in cyberstalking [41]. The victim's sense of security is weakened by the stalker's ability to reach them at any time and from any distance, which can cause the victim to live in continual fear. The victim of cyberstalking may experience a loss of control over their own life due to the recurring nature of the stalker's contacts and appearances, as they never know when they will resurface [40].

Cyber Pornography

Depicting or demonstrating sexual acts in order to induce sexual excitement through books, films, etc. is called "pornography". This includes pornographic websites, computer-generated pornographic content, and the downloading and sharing of pornographic images, videos, texts, and other content via the Internet. Today, there are about 420 million distinct pornographic websites. One regrettable aspect of the Internet is the presence of child pornography. Abusers use the Internet extensively to reach and sexually abuse youngsters all over the world [42].

Phishing

Cybercriminals employ phishing, a deceitful approach, to trick users into giving over private information, such as passwords or credit card details [43]. Since phishing targets a large number of Internet users, it has become one of the main problems. In this type of social engineering attack, a hacker uses a public or reliable organization to deceive users into divulging sensitive information to them. The goal is to get the victim to trust the message and provide the attacker access to their personal information by using an automated pattern. Phishers employ social engineering techniques to trick people into visiting malicious websites when they click on an embedded link in an email they received [44]. Phishing differs from previous cyberattacks in part because deception methods are used in its conception, implementation, and ultimate success. There are four steps involved in phishing, and they are as follows: Acquiring Trust, Guidance, Information, and Implementation [45].

Spamming

Electronic spamming is the practice of sending unsolicited bulk communications (spam), particularly advertisements, randomly over electronic messaging networks [46]. It generally has to do with repeatedly delivering the same messages to the same individuals or groups in order to promote something or carry out phishing attacks [47].

Identity Theft

For as long as there have been people and crimes, identity theft has existed [48]. Identity theft is the act of getting private information about another individual without that person's knowledge and exploiting it for fraudulent purposes. This attack allows the attackers to trick the victims into thinking that they are giving sensitive personal information to a reputable company; occasionally, this happens in the form of an application for a job that is fraudulently posted online or a response to an email requesting an update to membership or billing details. Cybercriminals now have the means to acquire such data from the databases of susceptible firms [49].

E-Mail Bombing

Email bombing is a harmful cyberattack that is becoming more common [50]. Email bombing is characterized by sending enormous volumes of email to a target address, resulting in the victim's email account or mail servers failing. The message is unnecessarily lengthy and pointless in order to use up network resources [51]. Because the emails frequently seem harmless, it is difficult for traditional spam filters to identify this kind of attack [50].

Unauthorized Access

Accessing a computer system, network, application software, data, or other resources without authorization is known as unauthorized access. When authorized users access a resource they are not permitted to use, it is also considered unauthorized access [52].

The prevalence of crimes involving smartphones and other personal devices in the modern world highlights how crucial cybersecurity is to protect the users [53]. Cybersecurity makes sure that the company survives and prospers in the digital environment by safeguarding user assets from online threats [54]. An overview of cybersecurity and its significance in our day-to-day lives is given in the section below.

C. Cybersecurity

The term "cybersecurity" refers to a grouping of resources that can be utilized to safeguard an organization's or an individual's online environment, including technology, risk management, best practices, policies, procedures, and education [55].

The topic of cybersecurity has gained significance and attention on a global scale. More than fifty countries have formally released a policy statement expressing their official positions on cybercrime, cybersecurity, and cyberspace [56]. In response to the steadily rising frequency of cyberattacks, cybersecurity has become a crucial sector requiring round-the-clock monitoring [57]. Any organizational or personal resources that are susceptible to cyberattacks and need to be protected against cyber threats are referred to as "assets" in the context of cyberspace. Cyberspace assets can contain a range of resources like networks, software, hardware, data resources, and utilities [58]. Cybersecurity helps to shield networks and devices from assaults and unwanted access by implementing the appropriate safeguards. The three pillars of confidentiality, integrity, and availability (CIA) form the foundation of cybersecurity [59].

1) Importance of cybersecurity

For those who routinely use the Internet on a variety of electronic devices, cybersecurity is essential to their safety. It helps in protecting extremely sensitive data, such as military assets and biotechnology, which are always under attack from hackers. In many spheres of life, particularly social media, higher education, and governmental institutions, misuse of the Internet has become a problem [60].

Cybersecurity is valued by institutions and enterprises in addition to private individuals and families. Because it offers suitable cyber defenses and data and information protection, cybersecurity is crucial. Additionally, cybersecurity guards against intrusions on networks and systems and safeguards

personal data. By using cybersecurity techniques, internet users are given the privacy they require and are entitled to. [61].

A safe electronic environment and controlled asset utilization are ensured by cyber-security, which includes rules, assurances, security ideas, policies, treatments, procedures, practices, training, and technologies. Network, computer, and software dangers can be addressed by cybersecurity through the detection of intrusions, prevention of viruses, blocking of access, facilitation of encrypted communications, and enforcement of authentication [62].

Nowadays, the majority of countries view cybersecurity as a component of national security. China, for example, views cybersecurity as being on par with national security. Since every state operates differently, it is often impossible to assign a single strategy to cybersecurity operations; yet, it is clear that cybersecurity is crucial for modern governments [61].

2) Cybersecurity is not all about technical security

Online fraud is thought to cost businesses £193 billion, according to recent research from the Office of National Statistics. Technological solutions like biometric devices, firewalls, and anomaly detection systems offer some genuine defense against a range of threats to improve network security [63]. A technology-centric perspective is typically taken when approaching cybersecurity, with little to no understanding of end users' demands, motivations, and cognitive processes. To combat possible cyber-attacks, corporations place a high priority on technology solutions (such as firewalls, antivirus software, and intrusion detection systems), whereas according to recent cybersecurity research, combating cyberattacks requires a comprehensive strategy rather than just technological fixes [64]. According to one survey, the biggest security flaw is people (86%), followed by technology (63%). Human mistakes in cybersecurity were identified as a major detriment to the national security in national cybersecurity policy of the United States and the United Kingdom. It is well known that over 80% of all ransomware, cyberattack, and data breach incidents are caused by human error. However, the majority of businesses have not been successful in putting procedures in place to address human issues in cybersecurity [65]. The main problem with humans in cybersecurity is that users are not aware of cyber threats [66]. Stated differently, the majority of security incidents stem from human faults, which can include purposeful and inadvertent misbehavior [67].

3) Cybersecurity Awareness

Cybersecurity awareness can be defined as the extent to which users comprehend the value of information security and their obligations to exercise appropriate information control to safeguard the company's networks and data [68]. One of the fundamental causes of the success of cyberattacks is the human factor: cyber criminals utilize social engineering to target the least educated computer user as their weakest link. The implementation of formal cybersecurity awareness is required to stop attackers from exploiting human vulnerabilities [69].

A secure environment for an organization's digital assets cannot be ensured by technology measures alone since human error accounts for the majority of security breaches. For example, a lot of Internet users still don't know how their gullible actions can jeopardize their computers. As a result, users keep making weak passwords or sharing them with others; these individuals keep visiting dubious websites, clicking on links in emails from senders they don't know, and exposing private information via various forms of social engineering [14].

4) User Awareness and Education

The literature made a distinction between the functions of awareness, training and education: Awareness entails drawing the attention of every other employee to security, enabling them to abstain from actions that could jeopardize data security. Security experts integrate their skills and competencies into a shared body of knowledge for information security design and implementation through education [70].

The information that guides acceptable security behavior is known as user awareness. It's essential to comprehend how secure personal data is [71]. All users of IT systems and services must have a basic understanding of cybersecurity in order to safeguard themselves from danger and minimize risk. But even after years of employing a wider range of technologies, this knowledge is frequently found to be either completely inadequate or falling behind. It is especially pertinent in an organizational context, where a large number of incidents and breaches are caused by staff members' ignorance of security protocols and lack of compliance with them [72].

An awareness and training program is essential, as it is the means of disseminating knowledge that managers, employees, and other users (i.e., residents, customers, and workers) require. According to the authors, this is the most popular way to communicate security needs and proper behavior in the context of an information technology (IT) security program [19]. According to the study, the end-user online behavior and security awareness are greatly enhanced by cybersecurity awareness training programs. Researchers have demonstrated that the dissemination of cybersecurity best practices directly results from Internet end users taking part in cybersecurity awareness training [73]. Hence, frequent training is a recommended strategy for organizations to enhance cybersecurity knowledge and mitigate the negative effects of cyberattacks on corporate performance [74].

3. Recent Studies

The research [75] proposed a framework for cybersecurity education and training that would aid enterprises in assessing and measuring the cybersecurity expertise of their staff. This study proposed a CAT framework consisting of three main modules. Each level has its own set

of threshold values: beginner–50 percent; medium: 51–80 percent; and advanced: 81–100 percent. Employees are categorized based on their IQ level. By helping companies identify cybersecurity system vulnerabilities and evaluating employees' readiness for cyberattacks, threats, and incident response, this study aims to raise employee awareness.

The research [76] highlighted how many South African businesses, especially SMMEs, need to learn more about cybersecurity because they are currently ill-prepared to stop cybercrimes. A cybersecurity awareness framework has been presented based on the findings of a thorough literature research. The model consists of the Strategic, Tactical, Preparation, Delivery, and Monitoring layers. This study utilized a previously proposed model and added organizationally relevant components to modify it to match organizational needs.

The research [77] establishes a framework for raising awareness among users about social engineering attacks. The framework is divided into 3 phases: Awareness, Reporting, and Training. Each phase has sub-activities that must be achieved before moving to the next phase. The proposed learning and awareness training's first phase aims to improve employee familiarity with taxonomy-derived reference resources. To test the knowledge, an online assessment is conducted. In the second stage, employees are divided into three groups according to how well-informed and knowledgeable they are about social engineering risks. In phase three, employees undergo continuous testing, which is supplemented by frequent email reminders on the methods social engineers deploy and how to avoid falling for their tricks.

The research [78] suggested a theoretical framework for developing and enhancing cyber safety awareness to improve internet user safety by including cyber safety education in the South African school curriculum.

This research [79] examined the weaknesses in the current initiatives for raising employee awareness of cybersecurity and suggested a new model. To fill in the gaps in awareness training that currently exists, the authors suggest a paradigm for awareness training. To provide training to several businesses, the Cybersecurity Awareness Training Model (CATRAM) was developed. The authors emphasized the significance of more studies in the future directed at creating novel strategies to sustain cybersecurity awareness as they concluded their analysis.

This study [80] covers current and future features of cybersecurity awareness (CSA) programs. First, it offers strategies recommended by a plethora of prior research involving CSA. Secondly, it suggests using machine learning (ML) and artificial intelligence (AI) to create and provide CSA program viewers with a more individualized experience. The study divides the framework into three phases, each with different activities. First is the Pre-implementation phase (Team Setup, establishing goals and Objectives, Resources Preparation), Second is the Implementation phase (Pilot test, Message delivery, Lesson Learned), and third is the Post-implementation Phase (Evaluation Activities, Adjustment).

The research [81] covers a paradigm of cybersecurity awareness for senior citizens. The Security Awareness Model, Information Security Awareness Program (ISAPM) General Model, Information Security Awareness Capability Model (ISACM), and Peer Education Model have all been incorporated into the development of a cybersecurity awareness model for older people based on the mapping results. The models proposed consist of several factors that must be considered, such as identifying the organizations' security goals for the elderly, measuring the awareness level, designing, developing, implementing and reviewing the security awareness program for elderly.

The research [11] proposed a framework for enhancing cybersecurity awareness culture and education. Strategic, tactical, preparation and delivery, and monitoring are the five layers that make up the framework. Each layer is composed of different components: The strategic layer is made up of elements such as the strategic plan, responsible units, and national cybersecurity. The Tactical Layer includes awareness campaigns and partnerships, while the Preparation Layer includes elements such as tools, content, topic, and medium. The Delivery Layer includes elements like the Target Audience and Key Role Players, while the Monitoring Layer concentrates on evaluation through various methods like establishing benchmarks, success indicators, and periodic status reports.

The research [82] emphasized that university employees and do not know how to secure their data and do not have the requisite skills. As a result, a thorough awareness and education model for the adoption of safety measures for universities has been proposed. The framework is divided into 4 parts: the first is called Program Plan Design (this part includes several activities such as need assessment, funding, functional roles and responsibilities, success indicators, and delivery method); second is Develop Awareness and Education Material; third is Implementation; and fourth is Evaluation, and Feedback Technique.

The research [83] aims to improve graduates' cybersecurity awareness at any academic institution by proposing a conceptual framework for cybersecurity awareness. This framework includes components intended to continuously enhance the integration, creation, delivery, and assessment of cybersecurity knowledge into university curricula across disciplines and majors; as a result, all university graduates, who will make up the future workforce, would be more aware of this. This framework consists of three phases.

The research [84] emphasized the need for a structured approach to teaching parents about Internet safety concerns. It also presents a framework for increasing awareness. The framework identifies numerous areas that need to be

prioritized such as governance, required resources, safety topics, and delivery. A Cyber Safety Information Needs Assessment Instrument was developed to customize these features for a specific school. This framework also strongly emphasizes the classification of currently available cybersecurity information.

The research [85] emphasizes that the workers who deal with EHR systems must receive training on the dangers related to data protection. This study emphasizes how little research has been done on training program effectiveness and proposes a framework. The study highlights a few aspects that must be considered, such as Common information security issues, training content, selecting security topics, information security policy, targeted audience profile, training success factors, common training delivery methods for information security, Implementation, and Evaluation, etc.

A. Research Gap

Numerous researches have been undertaken to emphasize the need to establish a standard cyber awareness and education framework, and many frameworks have been recommended in various studies; nevertheless, most of the studies have either focused on organizations [75][79][76][85][82][83] or parents [84]. Few studies have provided a national framework for cyber awareness from the perspective of the public, such as this study [11]. However, its shortcoming is that the framework was specifically created for South Africa, which is still in the early phases of building cybersecurity. As a result, this study aims to fill this research gap by providing a holistic framework that can be utilized to develop cyber awareness campaigns/programs at the national level for public.

4. Research Methodology

Research methodology can be defined as a methodical approach to problem-solving [86]. The paradigm that directs the research activity—more precisely, the knowledge hypothesis that guides the research, the methods by which knowledge may be acquired, and views on the nature of reality and humankind (ontology) determine the choice of research methodology [87]. As the main goal of this study is to develop a cybersecurity awareness and education framework, a thorough literature analysis was conducted to create the conceptual framework in order to accomplish the aforementioned goal. This process consisted of several steps such as database selection, search strategy, inclusion/exclusion criteria, data extraction, data analysis, and finally, development of the framework. The first step was to identify all the recent studies that have proposed cybersecurity awareness and education framework; for this purpose, a variety of academic databases were selected, like Google Scholar, Semantic Scholar, and IEEE Xplore, which helped in getting a diverse range of resources like conference papers, journal papers, and reports. The keywords used to search the studies were “Cyber awareness”, “awareness education”, and the most frequently used word for searching resources was “Cyber awareness and education framework”. Although various studies have approached cyber awareness in different ways and different frameworks have been proposed, the common goal for the studies is the same, which is to enhance cybersecurity awareness among people. Previous studies were analyzed, and data was collected to construct the conceptual framework. The framework incorporates all the main factors identified by these studies.

5. Framework Development

The proposed framework consists of 5 layers, with each layer containing important components. The first layer is called Planning; the second is called Designing; the third layer is Development; the fourth is called Implementation; and the fifth is called Evaluation. These layers constitute all the components which have been identified by different studies to provide comprehensive guidelines on how to design and implement successful awareness initiatives/programs. The important components with layers have been summarized in the TABLE I.

1) Framework Description

Planning

The first layer of the framework is called Planning. Cybersecurity awareness initiatives can fail for a variety of reasons, and being aware of these challenges is critical to ensuring their efficacy. One of the most important elements is the lack of planning, as it provides a base for designing, implementing, and evaluating awareness initiatives highlighted in this research. In order for awareness initiatives to be successful, they should have a proper plan [88]. The planning layer includes components such as the needs assessment, cybersecurity threats, target audience, awareness level measurement, and program objective definition. The need assessment for cyber awareness campaigns in this framework include two crucial aspects: The first step is to identify the most recent cybersecurity threats that the country is experiencing and then assess peoples’ awareness levels; this will help us determine how aware people are of each sort of threat and where we should focus.

Because risks are always evolving [89], educating people about them without first identifying the most relevant dangers and their impact might diminish the effectiveness of cyber awareness campaigns. Measuring awareness level of the people can help to understand how much knowledge people have about evolving threats and which area to focus on.

TABLE I. Key Components identified from different Studies

Name of the Component	References
Planning	[82], [90]
Needs Assessment	[82], [90], [84], [91], [92]
Cyber Security threats	[83], [92], [85], [80]
Measure Awareness level	[75], [90], [81]
Target Audience	[11], [76], [90], [82]
Awareness Program Objective	[90], [91], [80]
Designing	[75], [90], [91], [81]
Key Role players	[93], [82]
Topics	[93], [11], [84], [76], [90], [83], [85], [80]
Delivery Methods	[82], [76], [90], [85], [80]
Medium	[75], [11], [76]
Development	[75], [91], [94], [81]
Partnerships	[11], [76]
Development of the Material	[82], [93], [91], [94]
Implementation	[75], [82], [90], [91], [85], [80]
Roles and Responsibilities	[11], [82], [76]
Implement the Awareness program	[75], [82], [81]
Evaluation	[75], [11], [82], [90], [76], [91], [85], [80]
Success Indicator	[11], [82], [76] , [85], [80]
Periodic Status Reports	[11], [76]

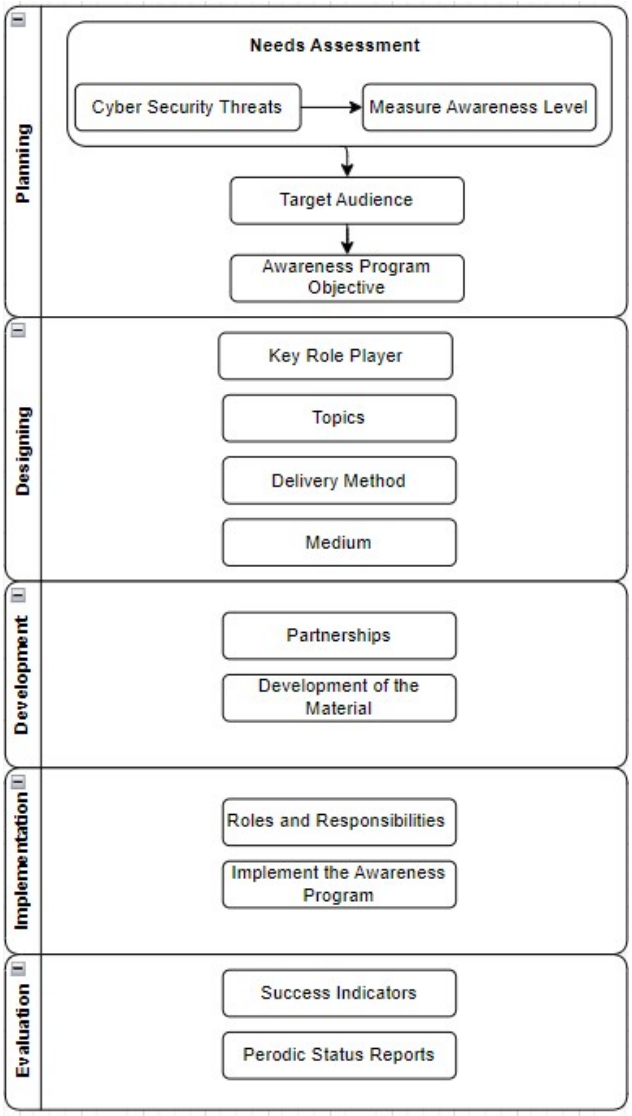

Figure 1. Proposed Conceptual Framework

When the need assessment is completed, it will help to understand which population segment needs. According to this study, if the demographic and psychographic features of each target segment are not properly specified, it may result in creation of content that will fail to achieve the desired result [95]. Once the target audience is clearly defined, the next step should be setting the campaign objective. It's important to understand what you want to achieve. According to Goldstein and Ford, identifying training needs and creating goals to meet them is the first stage for effective awareness training programs [96].

Designing

The design layer takes into account all of the important components that must considered when developing awareness campaigns. It consists of components including determining the key players who must be involved, selecting the right medium and delivery method, and choosing topics to be covered, etc. When training programs are inadequately designed, they may not succeed. This includes out-of-date resources, ineffective teaching strategies, and irrelevant information.

The first step in designing an awareness initiative is to identify important role players who can help you better understand the targeted audience. For example, if the target audience is children, the role players would be teachers, schools, and parents. If the target audience is the government sector employees, their supervisors can be approached for more information. According to this study, role players need to be recognized and understand their responsibilities [84].

Topics are a crucial component of any cyber safety program [93]. The topic should only cover one security vulnerability at a time. It can be difficult and confusing for the audience to focus on multiple topics at once [97].

While covering the right topics is critical, a security awareness program must carefully consider the delivery methods to use. Like any program, the awareness program's effectiveness will be greatly influenced by the manner in which the awareness material is delivered [98]. To reach the intended audience, a message must be sent through the appropriate media channel and medium. Most frequently, radio, newspapers, magazines, television, and the Internet are used as a medium to deliver the message [95].

Development

For the designated target audiences, the content development layer oversees creating persuasive collateral and materials related to cybersecurity awareness [94]. The development layer in this framework constitutes two components: first, developing partnerships and second is development of the material. For developing cyber awareness material, one does not always have the needed expertise as highlighted in this study where the researcher emphasized that, it is crucial to include essential public and private sector stakeholders in the planning and execution of the awareness-raising initiative [99]. Partnerships can include companies who currently invest in creating cyber awareness training for their staff [95]. These partnerships help ensure that the right expertise is available to develop awareness material for the targeted audience.

Implementation

Once the development of the material is complete, the next stage is the implementation of the designed program/campaign. The implementation layer in this framework consist of assigning roles and responsibilities and implementing the awareness program. Assigning roles and responsibilities is crucial for the successful implementation of the awareness initiatives. According to this study, role players must be acknowledged and comprehend their responsibilities [84]. The research suggests that a coordinated strategy for responsibility sharing is necessary and that numerous role players can or should be included, and every role player should be made aware of their duties [100].

Evaluation

Evaluation aids in determining the awareness program's effectiveness. It highlights the awareness program's shortcomings and strengths and is a crucial component in understanding audience behavior. These are a few of the methods that can be applied, such as statistics on the level of awareness both before and after the campaign, which can assist in determining if program objectives and goals have been met or not [101]. The two components that make up the evaluation layer are Periodic Status Reports and Success Indicators.

Performance indicators are quantifiable statistics that show how well specific main goals have been achieved. Businesses and corporations frequently use these indicators to assess the effectiveness of employees, procedures, and the organization as a whole [91]. The practice of creating success indicators can be used to track and assess people's knowledge about cybersecurity. Following the launch of a security awareness campaign, creating regular status reports is a useful tool for monitoring and assessment [76].

6. Conclusions and Future Work

One of the most crucial aspects of cybersecurity is user awareness since humans are thought to be the weakest link in the chain. Many times, a lot of work is put into raising awareness, but most of the time, these efforts fail because of a lack of proper guidance. Therefore, this study proposed a framework that can be utilized as a benchmark when designing awareness programs. The proposed framework consists of five layers, namely Planning, Designing, Development, Implementation, and Evaluation. Further, each layer consists of several factors to enhance the success of awareness campaigns. This framework can serve as an educational tool by providing a holistic approach to how awareness initiatives should be approached from beginning to end and allocate the resources effectively by identifying focus areas of cyber awareness initiatives based on the awareness level among people.

A. Implications

This study contributes to the ongoing research by establishing a cybersecurity awareness and education framework. The suggested framework has the potential to significantly impact awareness campaign success because it is the first all-inclusive approach that emphasizes the significance of comprehending training needs before designing any awareness initiative. This study also highlights the necessity of creating training programs that are specifically tailored to the needs of individuals. A tailored training program can address the unique challenges faced by different people as awareness levels in people vary depending on education, age, and work experience. This will lead to more efficient use of resources and provide better outcomes than when awareness efforts are carried out without a thorough grasp of those demands. It also highlights how important it is to choose the most effective mediums and delivery techniques, as these factors can have a big impact on the success of awareness campaigns. Thus, it can be said that the suggested framework can appropriately direct the creation of effective awareness campaigns that can be utilized to inform the general public about online safety which will help in better protection from cyber attacks.

B. Future Work

Numerous studies have underlined that user awareness is the most crucial component in developing strategies to address the expanding threats posed by cyberspace. At the same time, studies have also highlighted the need to create successful campaigns to raise knowledge of cyberspace. This study offers a foundation for creating successful cyber awareness initiatives; further research would examine how applicable the suggested framework is. Moreover, the framework can be validated for its effectiveness among different user demographics which will contribute to further

improving the proposed framework, which in turn will lead to successful training programs. Furthermore, sector-specific adaptation of the framework may be the subject of future research, leading to a customized framework for several industries.

C. Limitation

The limitation of this study is the lack of implementation of the proposed framework.

References

[1] Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, and A. K. Jaiswal, "A systematic literature review on the cyber security," *International Journal of scientific research and management*, vol. 9, no. 12, pp. 669–710, 2021.

[2] A. Romaniello and A. Chircu, "A connected world: A systematic literature review of the internet effects on society." *Issues in Information Systems*, vol. 19, no. 3, 2018.

[3] A. Subhani, I. A. Khan, and U. Ahmad, "Importance of conducting cyber security awareness sessions among undergraduate students," *Journal of Advanced Research in Social Sciences and Humanities*, vol. 8, no. 2, pp. 59–68, 2023.

[4] R. Mokhtar and A. Rohaizat, "Cybercrimes and cyber security trends in the new normal," in *The New Normal and Its Impact on Society: Perspectives from ASEAN and the European Union*. Springer, 2024, pp. 41–60.

[5] H. Berkman, J. Jona, G. Lee, and N. Soderstrom, "Cybersecurity awareness and market valuations," *Journal of Accounting and Public Policy*, vol. 37, no. 6, pp. 508–526, 2018, special Issue on Cybersecurity and Accounting. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278425418302370

[6] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: a systematic review of data availability," *The Geneva papers on risk and insurance. Issues and practice*, vol. 47, no. 3, p. 698, 2022.

[7] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, pp. 65–88, 2015.

[8] R. Raju, N. H. Abd Rahman, and A. Ahmad, "Cyber security awareness in using digital platforms among students in a higher learning institution." *Asian Journal of University Education*, vol. 18, no. 3, pp. 756–766, 2022.

[9] S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity*, vol. 8, no. 1, p. tyac006, 2022.

[10] O. A. Popoola, M. O. Akinsanya, G. Nzeako, E. G. Chukwurah, and C. D. Okeke, "Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of african and us initiatives," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 5, pp. 819–827, 2024.

[11] N. Kortjan and R. Solms, "A conceptual framework for cyber security awareness and education in sa," *South African Computer Journal*, vol. 52, 06 2014.

[12] D. Pruitt-Mentle, "End your fomo: Ten ways to celebrate national cybersecurity career awareness week with nice," 2020.

[13] T. Rahman, R. Rohan, D. Pal, and P. Kanthamanon, "Human factors in cybersecurity: A scoping review," 07 2021.

[14] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, 2023.

[15] F. Aloul, "The need for effective information security awareness," *Journal of Advances in Information Technology*, vol. 3, pp. 176–183, 08 2012.

[16] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv preprint arXiv:1901.02672*, 2019.

[17] D. T. Smith and A. I. Ali, "You've been hacked: A technique for raising cyber security awareness." *Issues in Information Systems*, vol. 20, no. 1, 2019.

[18] F. A. Aloul, "The need for effective information security awareness," *Journal of advances in information technology*, vol. 3, no. 3, pp. 176–183, 2012.

[19] A. Alruwaili, "A review of the impact of training on cybersecurity awareness." *International Journal of Advanced Research in Computer Science*, vol. 10, no. 5, 2019.

[20] S. Chaudhary, "Driving behaviour change with cybersecurity awareness," *Computers Security*, vol. 142, p. 103858, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404824001597

[21] R. Reid and J. van Niekerk, "Towards an education campaign for fostering a societal, cyber security culture," 07 2014.

[22] L. P. Muller, "Cyber security capacity building in developing countries: challenges and opportunities," 2015.

[23] S. B. Richard McGregor, Carmen Reaiche and G. C. de Zubielqui, "Cyberspace and personal cyber insurance: A systematic review," *Journal of Computer Information Systems*, vol. 64, no. 1, pp. 157–171, 2024. [Online]. Available: https://doi.org/10.1080/08874417.2023.2185551

[24] M. Mayer, L. Martino, P. Mazurier, and G. Tzvetkova, "How would you define cyberspace," *First Draft Pisa*, vol. 19, p. 2014, 2014.

[25] R. Ottis and P. Lorents, "Cyberspace: Definition and implications," in *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2010, p. 267.

[26] U. Mbanaso and P. Dandaura, "The cyberspace: Redefining a new world," *Journal of Computer Engineering (IOSR-JCE*, vol. 17, pp. 2278–661, 06 2015.

[27] P. Bruce-Quaye, "Cyberspace-advantages and its disadvantages," 2016.

[28] X. D. Hamidullayevna, T. B. Temirpulotovich, H. B. Sherboyevich, and S. D. Nematillayevna, "Features of the use of social networks by people with schizophrenia," *Journal of healthcare and life-science research*, vol. 3, no. 1, pp. 52–58, 2024.

[29] A. M. AL-Hawamleh, "Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures," *Interna-*

tional Journal of Advanced Computer Science and Applications, vol. 14, no. 2, 2023.

[30] K. Rajasekharaiah, C. S. Dule, and E. Sudarshan, "Cyber security challenges and its emerging trends on latest technologies," in *IOP Conference Series: Materials Science and Engineering*, vol. 981, no. 2. IOP Publishing, 2020, p. 022062.

[31] S. R. Biedron, "Cybercrime in the digital age," Ph.D. dissertation, University of Oxford, 2024.

[32] N. AllahRakha, "Transformation of crimes (cybercrimes) in digital age," *International Journal of Law and Policy*, vol. 2, no. 2, 2024.

[33] M. Alghamdi, M. Almushilah, and M. Alghamdi, "A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide," *International Journal of Engineering Research*, vol. 9, 01 2021.

[34] A. Kuzior, P. Brożek, O. Kuzmenko, H. Yarovenko, and T. Vasilyeva, "Countering cybercrime risks in financial institutions: Forecasting information trends," *Journal of Risk and Financial Management*, vol. 15, no. 12, p. 613, 2022.

[35] M. Haner, M. M. Sloan, A. Graham, J. T. Pickett, and F. T. Cullen, "Ransomware and the robin hood effect?: Experimental evidence on americans' willingness to support cyber-extortion," *Journal of Experimental Criminology*, vol. 19, no. 4, pp. 943–970, 2023.

[36] E. M. Kala, "The impact of cyber security on business: how to protect your business," *Open Journal of Safety Science and Technology*, vol. 13, no. 2, pp. 51–65, 2023.

[37] N. R. Gade and U. Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," 02 2014.

[38] U. Mbanaso and P. Dandaura, "The cyberspace: Redefining a new world," *Journal of Computer Engineering (IOSR-JCE*, vol. 17, pp. 2278–661, 06 2015.

[39] A. Bussu, M. Pulina, S.-A. Ashton, M. Mangiarulo, and E. Molloy, "Cyberbullying and cyberstalking victimisation among university students: A narrative systematic review," *International Review of Victimology*, p. 02697580241257217, 2024.

[40] S. D. Hazelwood and S. Koon-Magnin, "Cyber stalking and cyber harassment legislation in the united states: A qualitative analysis," *International Journal of Cyber Criminology*, vol. 7, no. 2, p. 155, 2013.

[41] A. Miftha, "The social, legal, and technical perspectives of cyberstalking in india," 2024.

[42] O. Goni, "Cyber crime and its classification," pp. 1–17, 05 2022.

[43] S. Kumar *et al.*, "Cyber crime: A review," *International Journal of Advanced Scientific Innovation*, vol. 5, no. 12, 2023.

[44] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, p. 563060, 2021.

[45] G. Varshney, R. Kumawat, V. Varadharajan, U. Tupakula, and C. Gupta, "Anti-phishing: A comprehensive perspective," *Expert Systems with Applications*, vol. 238, p. 122199, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095741742302701X

[46] B. M. E. Elnaim, "Cyber crime in kingdom of saudi arabia: The threat today and the expected future," in *Information and Knowledge Management*, vol. 3, no. 12, 2013, pp. 14–19.

[47] A. Marelino, "Understanding the types of cyber crime and its prevention," *Mathematical Statistician and Engineering Applications*, vol. 71, no. 1, pp. 108–112, 2022.

[48] A. Oloyede, I. Ajibade, A. Phillips, O. Shittu, E. Taiwo, S. Kizor-Akaraiwe *et al.*, "A review of cybersecurity as an effective tool for fighting identity theft across the united states," *A. Oloyede, I. Ajibade, C. Obunadike, A. Phillips, O. Shittu, E. Taiwo and S. Kizor-Akaraiwe (2023): A Review of Cybersecurity as an Effective Tool for Fighting Identity Theft across United States, International Journal on Cybernetics and Informatics (IJCI)*, vol. 12, no. 5, 2023.

[49] H. Jahankhani, A. Al-Nemrat, and A. Hosseinian-Far, *Cyber crime Classification and Characteristics*, 11 2014, pp. 149–164.

[50] S. Shukla, M. Misra, and G. Varshney, "Email bombing attack detection and mitigation using machine learning," *International Journal of Information Security*, pp. 1–11, 2024.

[51] O. Goni, "Cyber crime and its classification," *Int. J. of Electronics Engineering and Applications*, vol. 10, no. 1, p. 17, 2022.

[52] ——, "Cyber crime and its classification," pp. 1–17, 05 2022.

[53] J. N. Sales, R. Tiongco, S. Lu, M. J. Ruiz, J. Cruz, and M. Prudente, "Personal privacy and cyber security: Student attitudes, awareness, and perception on the use of social media," *International Journal of Curriculum and Instruction*, vol. 16, no. 1, pp. 175–190, 2024.

[54] A. Al-Hawamleh, A. Alorfi, J. Al-Gasawneh, and G. Al-Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," *Solid State Technology*, vol. 63, 12 2020.

[55] A. Papić, K. Knol Radoja, and D. Szombathelyi, "Cyber security awareness of croatian students and the personal data protection," in *11th international scientific symposium Region, Entrepreneurship, Development (RED 2022)*, 2022, pp. 563–574.

[56] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers Security*, vol. 38, pp. 97–102, 2013, cybercrime in the Digital Economy. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404813000801

[57] C. Aksoy, "Building a cyber security culture for resilient organizations against cyber attacks," *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, vol. 7, no. 1, pp. 96–110, 2024.

[58] V. Badadare, R. Patil, and D. V. Waghmare, "Cyber security need of digital era: A review," *International Journal of Computer Applications*, vol. Volume 182 – No. 22, pp. 9–12, 10 2018.

[59] M. N. Alenezi, H. Alabdulrazzaq, A. A. Alshaher, and M. M. Alkharang, "Evolution of malware threats and techniques: A review," *International journal of communication networks and information security*, vol. 12, no. 3, pp. 326–337, 2020.

[60] P. Lošonczi, "Importance of dealing with cybersecurity challenges and cybercrime in the senior population," *Security Dimensions*, vol. 26, pp. 173–186, 06 2018.

[61] A. Alasmari, "The role of cybersecurity to protect our information." *Multi-Knowledge Electronic Comprehensive Journal For Education & Science Publications (MECSJ)*, no. 32, 2020.

[62] J. A. Alkharman, S. A. A. Drawsheh, M. M. Al-Khataybeh, Z. B. BaniYounes, N. A. Hamid Darawsheh, and H. Alrashdan, "Cyber attacks and its implication to national security: The need for international law enforcement." *Pakistan Journal of Criminology*, vol. 16, no. 3, 2024.

[63] L. Hadlington, "The "human factor" in cybersecurity: Exploring the accidental insider," in *Research anthology on artificial intelligence applications in security*. IGI Global, 2021, pp. 1960–1977.

[64] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, and D. Guerri, "Leveraging human factors in cybersecurity: an integrated methodological approach," *Cognition, Technology & Work*, vol. 24, no. 2, pp. 371–390, 2022.

[65] C. Nobles, "Botching human factors in cybersecurity in business organizations," *HOLISTICA–Journal of Business and Public Administration*, vol. 9, no. 3, pp. 71–88, 2018.

[66] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of human vulnerabilities on cybersecurity." *Computer Systems Science & Engineering*, vol. 40, no. 3, 2022.

[67] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & security*, vol. 106, p. 102267, 2021.

[68] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022.

[69] V. H. U. Eze, C. N. Ugwu, and I. C. Ugwuanyi, "A study of cyber security threats, challenges in different fields and its prospective solutions: A review," *INOSR Journal of Scientific Research*, vol. 9, no. 1, pp. 13–24, 2023.

[70] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior," *IEEE access*, vol. 10, pp. 132 132–132 143, 2022.

[71] Y. Venugeetha, R. Rathod, and R. Kumar, "Social networking sites in daily life: benefits and threats," *Artificial Intelligence and Communication Technologies. New Delhi, India. Soft Computing Research Society*, 2022.

[72] I. Vasileiou and S. Furnell, *Cybersecurity education for awareness and compliance*. IGI Global, 2019.

[73] A. A. Al Shamsi, "Effectiveness of cyber security awareness program for young children: A case study in uae," 08 2019.

[74] H. Taherdoost, "A critical review on cybersecurity awareness frameworks and training models," *Procedia Computer Science*, vol. 235, pp. 1649–1663, 2024.

[75] M. Hijji and G. Alam, "Cybersecurity awareness and training (cat) framework for remote working employees," *Sensors*, vol. 22, no. 22, p. 8663, 2022.

[76] T. Lejaka, "A framework for cyber security awareness in small, medium and micro enterprises (smmes) in south africa," *University of South Africa*, 2021.

[77] H. A. Aldawood, "An awareness policy framework for cyber security social engineering threats," Ph.D. dissertation, The University of Newcastle, Australia, 2020.

[78] D. Scholtz, E. Kritzinger, and A. Botha, "Cyber safety awareness framework for south african schools to enhance cyber safety awareness," in *Applied Informatics and Cybernetics in Intelligent Systems: Proceedings of the 9th Computer Science On-line Conference 2020, Volume 3 9*. Springer, 2020, pp. 216–223.

[79] R. Sabillon, J. Serra-Ruiz, V. Cavaller *et al.*, "An effective cybersecurity training model to support an organizational awareness program: The cybersecurity awareness training model (catram). a case study in canada," in *Research anthology on artificial intelligence applications in security*. IGI Global, 2021, pp. 174–188.

[80] S. Chaudhary and V. Gkioulos, "Building a cybersecurity awareness program: Present and prospective aspects," in *International Workshop on Digital Sovereignty in Cyber Security: New Challenges in Future Vision*. Springer, 2022, pp. 149–160.

[81] A. G. Buja, S. D. M. Wahid, T. F. A. Rahman, N. A. Deraman, M. N. H. H. Jono, and A. A. Aziz, "Development of organization, social and individual cyber security awareness model (osicsam) for the elderly," *International Journal of Advanced Technology and Engineering Exploration*, vol. 8, no. 76, p. 511, 2021.

[82] B. Mutunhu, S. Dube, N. Ncube, and S. Sibanda, "Cyber security awareness and education framework for zimbabwe universities: A case of national university of science and technology," in *Proceedings of the International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria*, 2022, pp. 5–7.

[83] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, no. 10, p. 417, 2021.

[84] E. L. Paraiso, *Towards a cyber safety information framework for South African parents*. University of Pretoria (South Africa), 2019.

[85] A. Ghazvini and Z. Shukur, "A framework for an effective information security awareness program in healthcare," *Int. J. Adv. Comput. Sci. Appl*, vol. 8, no. 2, pp. 193–205, 2017.

[86] B. Dudhade, "Research methods and research methodology: Is there any difference?" 10 2012.

[87] F. Tuli, "The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological and methodological perspectives," *Ethiopian journal of education and sciences*, vol. 6, no. 1, 2010.

[88] *The Art of Planning an Impactful Awareness Campaign*, 2025 (accessed January 5 , 2025). [Online]. Available: https://aicontentfy.com/en/blog/art-of-planning-impactful-awareness-campaign#:~:text=Planning%20is%20a%20fundamental%20aspect,and%20objectives%20are%20effectively%20achieved

[89] W. Labuschagne, M. Eloff, N. Veerasamy, and M. Mujinga, "Design of a cyber security awareness campaign for internet cafés users in rural areas," 2011.

[90] I. Dlamini, B. Taute, and J. Radebe, *Framework for an African policy towards creating cyber security awareness*, 2011.

[91] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective

cybersecurity training frameworks: A delphi method-based study," *Computers & Security*, vol. 113, p. 102551, 2022.

[92] J. Rajamäki, J. Nevmerzhitskaya, and C. Virág, "Cybersecurity education and training in hospitals: Proactive resilience educational framework (prosilience ef)," in *2018 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2018, pp. 2042–2046.

[93] M. J. Z. De Barros and H. Lazarek, "A cyber safety model for schools in mozambique," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal*, 2018, pp. 22–24.

[94] Z. Yunos, R. S. Ab Hamid, and M. Ahmad, "Development of a cyber security awareness strategy using focus group discussion," in *2016 SAI Computing Conference (SAI)*. IEEE, 2016, pp. 1063–1067.

[95] C. Leppan, "Analysis of a south african cyber-security awareness campaign for schools using interdisciplinary communications frameworks," Ph.D. dissertation, Nelson Mandela Metropolitan University, 2017.

[96] J. E. Ejakait, "Effects of training needs assessment on employee performance in the postal corporation of kenya, bungoma county," *Research on humanities and social sciences*, vol. 6, no. 17, pp. 140–145, 2016.

[97] S. Chaudhary, S. Pape, M. Kompara, and V. Gkioulos, "Properties for cybersecurity awareness posters' design and quality assessment," 06 2022.

[98] A. Ghazvini and Z. Shukur, "Awareness training transfer and information security content development for healthcare industry," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 5, 2016.

[99] M. Bada, B. Von Solms, and I. Agrafiotis, "Reviewing national cybersecurity awareness in africa: An empirical study," 2019.

[100] N. Sonhera, E. Kritzinger, and M. Loock, "Roles and responsibilities for school role players in addressing cyber incidents in south africa," *Eurasian Journal of Social Sciences*, vol. 9, no. 3, pp. 123–137, 2021.

[101] S. Ashraf, "Organization need and everyone's responsibility information security awareness," *SANS Institute*, 2005.