IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 17, 2021, accepted June 23, 2021, date of publication July 14, 2021, date of current version July 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3097144

Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review

SHADAB KALHORO, MOBASHAR REHMAN, (Senior Member, IEEE), VASAKI A/P PONNUSAMY, AND FARHAN BASHIR SHAIKH

Department of Information Systems, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Petaling Jaya, Perak 31900, Malaysia

Corresponding author: Mobashar Rehman (mobashar@utar.edu.my)

This work was supported by the Universiti Tunku Abdul Rahman, Kampar, Perak, Malaysia, under Grant IPSR/RMC/UTARRF/2020-C1/M04.

ABSTRACT The advent of new technologies and the rapid growth of internet users have given birth to the menace of cyber-crime. Unfortunately, it is increasing at an alarming pace. This situation calls for good cyber hygiene behavior to secure digital lives. Cyber hygiene behaviour holds a significant role in terms of cybersecurity across the globe. There is a dire need to understand better the user variations associated with good or bad cyber hygiene behaviour and an improved view of what users do to encourage good cyber hygiene. Cybersecurity attacks are rising due to recent advancements in ICT and the Industrial Revolution 4.0 (IR 4.0). Software development organizations are among the crucial sectors suffering from cybersecurity issues. These organizations are more vulnerable to cyber-attacks because they lack proper cybersecurity culture. Although many initiatives have been taken by academia and industry to address this rising issue, the problem still exists for Software development organizations because good cyber hygiene behaviour is not observed, which is a prerequisite to reduce cyber threats. This study performed a Systematic Literature Review (SLR) of research papers published during 2010 – 2020. The key factors influencing software engineers' cyber hygiene behaviour intention are extracted from the published literature. The study examined 35 research papers out of 5,270 found from IEEE Xplore, Emerald Insight, SpringerLink, and ScienceDirect databases. The study reviewed number of factors such as the role of personal, social, socio-cognitive, environmental, & technological factors that may individually or collectively influence software engineers' cyber hygiene behaviour. The positive and negative factors associated with the cyber hygiene behaviour of software engineers are also categorized. This study enriches the understanding of the potential factors related to software engineers' cyber hygiene behaviours. It provides valuable insights to researchers, software development organizations, governments, and individuals associated with the field of Software Engineering. This research will assist in changing the software engineers' behaviour towards cyber hygiene, which will ultimately lead to mitigate the issues of Cybersecurity.

INDEX TERMS Cybersecurity, cybersecurity awareness, cybersecurity behaviour, software development organizations, SME employees, software engineers, factors of cybersecurity behaviour.

I. INTRODUCTION

Securing information has become one of the biggest challenges of today's world. The advent of novel technologies, mainly related to information and communication technology, has profoundly affected how businesses run in an organization and how employees can perform duties. Cybercriminals are increasingly targeting the human factor in information security. Many efforts are being carried out to improve ''cyber hygiene'' —a term that could be taken for granted to create and maintain online security. Unfortunately, the meaning of the word ''cyber hygiene'' and associated

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

practices vary and contradict each other somehow; thus, it is challenging to protect information resources. Some organizations may assume security-related rules are sufficient in their internal policy (but no additional safety exercises are conducted).

Employees must be aware of the risks and differentiate the requirements for undesirable behaviour. We cannot implement best practices if we do not know about the risk and attacks. This is an especially challenging situation within the cybersecurity domain when the nature of attacks seems to be constantly changing. People sometimes rely on shortcuts that allow them to make quick decisions. The information alone is not enough to encourage behaviour change.

In [1], authors have shown that even the trained users with a high level of safety awareness, their behaviour is not significantly different from untrained users; in addition to awareness and training, poor cybersecurity practices continue. So, for a good predictor of cybersecurity practices, information awareness and employee behaviour change are necessary. Therefore, in practice, it may be fruitful to raise awareness regarding cyber hygiene and change the behaviour of employees.

Data privacy and data security will remain the highest security measures for any organization. Currently, we live in a world where the entire information is stored in digital or cyber form. Social networking websites provide a space where users can feel safe when interacting with family and friends. For home users, cybercriminals will continue to steal personal information on social media. A person should take all necessary security measures during online social networking and banking transactions. The workplace has changed as it has become more common for many employees to work from home (especially during COVID-19) or have unlimited access to the organization's resources in the workplace. New access to it is highly valuable worldwide; however, organizations must protect their data, such as employees' personal information and intellectual property. Humans are often recognized as a weak link in cybersecurity. Ideally, users would have a good quality of cyber hygiene. They will understand the need to update the software, and it may take some time to create different passwords.

On the other hand, many users have bad cyber hygiene; they are not educated and not trained about the basics of cyber hygiene. They freely share their passwords and quickly share their personal data on social networks. Small businesses are at risk of fraud due to sharing passwords and personal data because small companies do not have employees with security expertise or a large budget to invest in cybersecurity. Though, good cyber-hygiene could endorse safe behaviour and defend against threats [1]. In that case, they are more likely to be victims of cyber-attacks that could lead to business damage, including the possibility of closure. Cybersecurity breaches are widely reported; not only are organizations vulnerable to cyber-attacks, but users at the individual level are suffering huge losses from the security breach. End users understand that they are at risk but do not know how to access, use these settings, and follow the best practices to protect their passwords and personal information [2]–[6].

One of the areas of research in cybersecurity is how to improve cyber hygiene behaviour [48]. Authors in the study [27] reported linking human characteristics, such as risk-taking, decision-making styles, demographics, and personality traits for ethical cybersecurity purposes. In [88], authors said that gender was found to predict the strength of passwords; women generate weaker passwords than men. In [8], authors examined how important a factor gender is in terms of cybersecurity beliefs and behaviours among employees; authors identified gender differences based on computer skills, prior experience, security self-efficacy, and self-reported cybersecurity behaviour. Women in the study had slightly lower levels of computer skills and less security knowledge. Noted the greatest difference for self-efficacy, where the women showed significantly lower self-efficacy than men. Authors in [1] analyzed the cyber hygiene knowledge of concepts and threats and the behaviours of the end-users. In their analysis, they reported that men had more experiences and awareness than women. The authors also mentioned that users need more knowledge to improve cybersecurity and change their behaviour. It was also reported that 81% of participants had cyber hygiene security training, but it did not improve their behaviour or increase their knowledge. Researchers concluded that it should provide the most effective training to all users [51].

The primary motivation of this systematic literature review is to present a comprehensive and effective understanding of the factors of cyber hygiene behaviour among software engineers. This study aims to fill the research gap by recognizing the factors of cyber hygiene behaviour and to find out the relationship between identified factors and cyber hygiene. Factors of cyber hygiene include the positive and negative relationship of the last ten years (2010-2020). This study consists of a descriptive and graphical analysis of identified factors. This SLR will help apply effective cyber hygiene practices and encourage software engineers to have a detailed understanding of positive and negative cyber hygiene factors.

A. CYBER HYGIENE SECURITY BEHAVIOUR

Cyber hygiene consists of behaviours, such as, checking computer for viruses and use strong passwords to help with maintaining system security. Two types of security behaviours that have an impact on security are described below. These two types are cyber hygiene and threat response.

1) CYBER HYGIENE

significantly reduces the risk of keeping the system insecure. Examples of cyber-hygiene behaviour include virus scanning, data backup, updating, and using strong passwords.

2) RESPONSE TO A THREAT

is the capability to prevent an attack and the ability to stop a potential attack. Computer scanning after a virus alert or

an unusual computer operation and completing a recovery program to end an attack are examples of behavioural responses to threats.

Security behaviour requires knowledge that a person acquires about cybersecurity; it leads to better security behaviour. The users generally prevent themselves from threats and detect theft when they have a high level of computer knowledge. In [9], the authors found that the lack of user knowledge about cyber hygiene was one reason for users to be exposed to phishing threats. The authors in [10] recommend that users become more careful and informed when using the Internet when they have more information about the effects of online threats.

II. FORMATION AND OVERVIEW OF THIS STUDY

The flow chart in figure 1 describes steps that are followed in this SLR. This figure also provides a summary of the entire research paper.

A. LACK OF CYBER HYGIENE BEHAVIOUR LEADS TO CYBER THREATS AND ATTACKS

Software development organizations must adopt policies and practices to recognize the weakest connections and security issues. Very few software development organizations can effectively develop management systems that can build a cybersecurity culture that has a positive impact on the behaviour of their software employees [84].

Social engineering attacks are increasing rapidly in today's networks and are considered a major cybersecurity threat, weakening the cybersecurity chain. Their purpose is to manipulate individuals and companies to disclose valuable and important data. Social engineering attacks challenge all networks' security regardless of the strength of their firewalls, cryptography methods, intrusion detection systems, and anti-virus software programs. These attacks can be classified into two categories: Human-based, in which the attacker makes a personal attack by working with the target to collect the desired information. The other is software-based, in which attacks are carried out using devices such as computers or cell phones to obtain targeted information [85].

Some common types of cyber-attacks are phishing, spear phishing, malware attack (viruses, worms, Rootkit, Trojan horse, ransomware attacks), DDOS, etc. A cyber-attack called WannaCry Ransomware attack [35] occurred a few years back, attacking the Microsoft Windows operating system on a large scale, including windows 8, 2003, and XP users because many people in organizations had not updated their version of software security. In the banking and corporate sectors, computers with transaction databases have been severely affected by this cyber-attack. It shows unawareness of cyber-hygiene practices can lead to more cyber-attacks and cyber threats. If users had updated their software timely, they could have easily and efficiently avoided major attacks. In general, different kinds of cybersecurity threats are [86]:

1) BRING YOUR OWN DEVICE (BYOD) AS A THREAT

BYOD (Bring Your Own Device) means the workers use their own devices during their working hours. BYOD threats are exclusively based on the user's activity with employees' personal devices. Organizations get the benefit of increased productivity and reduced investment in ICT. SMEs tend to have greater problems with information system security (ISS) than larger companies. The threat agent in BYOD is the employee who brings some critical risks in which is an authorized employee uses a particular system or device of an organization. This action might create a threat to an organization because of employee unawareness and faults. BYOD problems can lead to the theft of sensitive legal data and viruses on personal devices, malware that could infect incorporate network, unintentionally recovering spam, and opening virus-infected email attachments on devices. To prevent all these problems, SMEs are encouraged to pursue policies to protect security; for example, to specify authorize personal devices and use security applications in BYOD devices [87].

2) SPEAR PHISHING

Spear phishing attacks refer to the theft of sensitive information targeted to specific individuals or groups making claims or communicating using their names. They need to gather information about the victim using available online data. When they attack a company from the inside, it is difficult to identify and distinguish them from legitimate users, which explains the high level of success of these attacks compared to other social engineering attacks [39].

3) DISTRIBUTED DENIAL-OF-SERVICE DDOS

The distributed denial service floods the network of attacking organizations with traffic and eventually shuts it down. In 2016, Distributed Denial of service (DDoS), including tens of millions of Internet Protocol (IP) addresses, were identified and attacked by a domain name system (DNS). Last year the size and growth of DDoS attacks had increased several times. In 2016 it had a significant growth in terms of volume [77].

4) RANSOMWARE ATTACK

Ransomware [79] is a cyber-malware that blocks data access and related information. Sometimes it requires a fee, which must be paid to access the affected data, and it will be launched through an email; when the user clicks on the given link, it activates through that email. It can also filter the system when the user visits certain websites or specific web pages [35]. This cyber malware encrypts itself, blocks internal files, and renders them inactive to the end-user. It also affects the server connected to that computer and sometimes locks the entire system network settings [80], [81].

5) MALWARE ATTACK

Malware is a general term for all types of malicious software. For computer security: ''Software used for the purpose of

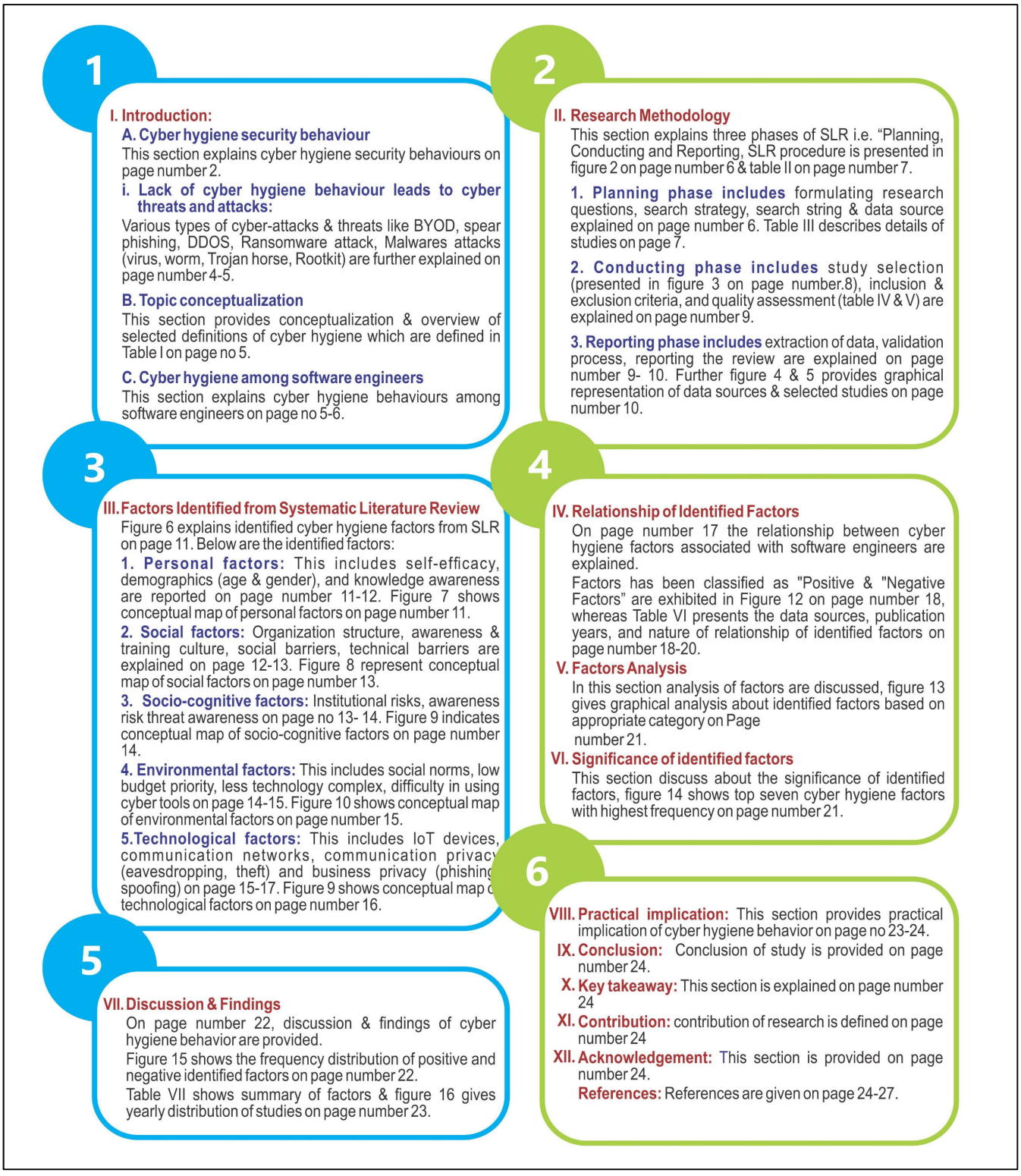

FIGURE 1. Flow chart of this study.

violating computer security policy''. The term ''software'' here refers to the use of malicious code, scripts, etc. Malicious software programs can detect your sensitive information without your knowledge until they alert you [86]. Malware includes Worm, virus, Trojan horse, Rootkit, etc. Although many activities have been carried out in the Malware area,

no separate classification distinguishes a different type of Malware and defines each of them carefully [33].

a: WORM

The worm is one of the most dangerous malicious software with an independent structure. It circulates from one computer to another by replicating automatically without using infected files and human activities. Worms have self-replicating and self-contained properties. Self-replication means that it can copy itself, and the self-contained means algorithm can execute without attaching to another program [33]. The worm can be very harmful to computers on the network, i.e., it consumes too much computer memory; because of this, many applications may stop responding [38].

b: VIRUS

A virus is a computer program that moves from one computer to another by associating with another program. There are several ways in which the virus can be transmitted to other computers, such as sending infected files via email or by embedding copies of infected files on removable media like CDs, DVDs, or USB drives. Through these drives, chances of spreading viruses to other computers may increase and can infect a network file system or a file system of computers [35].

c: ROOTKIT

A Rootkit is an automated software package that hackers can use to hide access and to gain administrative (''root'') privileges on a computer or computer network. Alternatively, we can say that Rootkit is a set of tools for many purposes, such as collecting information about the system and its environment through network sniffers to provide a backdoor to the system that enables hackers to access the system over time concealing the fact that the system is corrupted. Rootkit usually includes a host that can delete audit records and other Rootkit records [33]. The important thing to note is that it does not access the infected computer to hide existing access by malicious resources and other usable techniques. Other malware such as worms and Trojans use the Rootkit to conceal their presence on the infected computer for a long time [35].

d: TROJAN HORSE

Trojan horse is malicious software that can hide on an infected computer. Unlike worms and viruses, Trojans do not have their onboard duplication and transmission capability. So, it is better to say that the Trojan horse is a virus that cannot be replicated. Trojans use many ways to infect the computers, such as downloading from a remote location, but recently Trojans used worms and viruses to infect victims' computers. A special type of Trojan can be controlled remotely and receive commands from attackers [33].

B. TOPIC CONCEPTUALISATION

The conceptualization of the topic provides detailed information on the subject under the study. Thinking about the topic conceptualization is necessary to **get "a broader understanding of what is known about a topic"** [11]. Table 1 exhibits the working definitions of Cyber Hygiene proposed by various authors.

TABLE 1. An Overview of the Selected Definitions of Cyber Hygiene.

Definations of Cyber Hygiene	Source
"Cyber hygiene is knowledge of concepts, the knowledge of threats, and the behaviours of end-users in an extensive and updated approach that will include topics of security software, authentication, phishing scams, social networking, web browsing, Wi-Fi hotspot usage, and USB drive use."	[2]
"Cyber Hygiene practices internet users need to follow to safeguard their devices and their personal information online."	[17]
"Cyber hygiene is the adaptive knowledge and behaviour to mitigate risky online activities that put an individual's social, financial, and personal information at risk."	[18]
"Implementing and enforcing data security and privacy policies, procedures, and controls to help minimize potential damages and reduce the chances of a data security breach."	[19]
"Cyber' hygiene' that trains an educated workforce to guard against errors or transgressions that can lead to cyber intrusion."	[20]
"Cyber hygiene" as a cybersecurity role of each employee with a computer, equal with employee responsibility to safeguard his or her door keys or access codes (comparison to the physical world)."	[21]

C. CYBER HYGIENE AMONG SOFTWARE ENGINEERS

Information technology is changing the way we do business and communicate. Organizations are increasingly using information technology to get better products and quality of service. Information is considered very important, and it is regarded as an asset of a given organization [12]. Protecting data is essential to ensure the integrity and confidentiality of the organization. It is difficult to protect personal and organizational data as it can be stolen at any time in many ways. The first requirement for users to protect their data is to know what to do and how to do it; in other words, they should have the necessary knowledge and skills. Sharing information of all kinds improves the security of the entire organization and creates trust among software engineers.

The small organization keeps a mailing service to communicate with employees, clients, and stakeholders. Malicious emails could damage the status of an organization. Such an attack is called phishing scams when an attacker sends unsolicited emails to employees in an organization that pretends to be authentic. It is a challenging situation for a software engineer to decide whether to click on a link or not. These decisions can be supported by appropriate training

regarding information security awareness. It is necessary that training be provided to all software engineers within the organization [13]. On the other hand, software engineers are at the forefront to defend the organization from the network and the most significant threats. The negligence of software engineers can cost and damage the organization in terms of money and the form of losing important information.

Therefore, it is essential to identify the knowledge awareness that a software engineer has regarding cyber threats and attacks. Organizations should also look at security awareness services, which could help both engineers and organizations understand the network vulnerabilities. In many cases, cyber-attacks occur in the organization's network due to a lack of information among software engineers.

Most organizations provide necessary training to software engineers. Security awareness training is beneficial, giving the user more insight into the cyber threat. To protect sensitive information with user safety practices contributes to security awareness.

Cybersecurity culture can also improve the security of software engineers. Culture operating on cyber-security is essential to prevent security breaches caused by engineers' non-compliance with the organization's security policies. It is well-known that awareness of security is a critical factor in reducing security information risk in organizations. In this dynamic environment, sharing cybersecurity practices increases awareness as an effective means and reduces cyber threats and attacks [14]. Creating a cybersecurity culture within the organization will minimize software engineers' negative interaction and reduce the risk of misconduct when in contact with organizational assets. Numerous studies show that user attitudes and a lack of security awareness are the main contributors to online safety incidents [15]. Such findings support the need to incorporate a cybersecurity culture that helps to contribute to the engineers' safety behaviour in organizations.

III. RESEARCH METHODOLOGY

The Systematic Literature Review (SLR) has been used to review the studies published from 2010 to 2020. SLR mainly consists of three phases, including "Planning", "Conducting" and "Reporting" reviews [89]. This methodological research strictly followed the guidelines suggested by Kitchenham for a systematic literature review [15]. The SLR design is composed of series of steps exhibited in Figure 2. Systematic literature study guidelines are structured into three phases, as presented in Table 2.

A. PHASE 1: PLANNING THE REVIEW

The research questions for this study have been formulated in line with the aims and objectives of the current study.

1) FORMULATING RESEARCH QUESTIONS

Research Question.1:

What are the key factors that are associated with the Cyber Hygiene Behaviour of software engineers?

TABLE 2. Systematic Literature Review Procedure.

SLR Phases	SLR Actions
Planning	• Specifying Research Questions • Search Strategy • Defining keywords, search sting, Data Sources
Conducting	• Search the related literature review • Select Primary Studies • SettingInclusion/exclusion criteria • Quality Assesment of Studies • Extraction of Required Data
Reporting	• Synthesize Data • Results • Discussion • Conclusion

Aim: To take out all the key factors that may impact software engineers' cyber hygiene behaviour.

Research Question 2: What is the relationship of identified factors between intentions to perform cyber hygiene behaviour?

Aim: To observe the relationship between intention to perform cyber hygiene behaviour.

2) SEARCH STRATEGY

An electronic search space was pre-defined as search for relevant studies. The electronic databases ScienceDirect, Emerald Insight, SpringerLink, and IEEE Xplore were used for literature search. The inclusion and exclusion criteria from the studies were set to obtain relevant literature for this study. The dismissals were found after screening and mutual agreements eliminated among the authors. The obtained articles were further reviewed to assess & improve the quality of this study.

a: SEARCH STRING

The relevant keywords are pre-defined to cover the broader scope of this study. Boolean operators, i.e., "AND" & "OR," were used to minimize irrelevant studies' search. The study used the below search string:

"Cybersecurity" OR "Internet security" OR "Computer Security," AND "Cyber Hygiene" AND "cybersecurity awareness" OR "Cybersecurity knowledge," AND "Cybersecurity behaviour" OR "Cybersecurity conduct," OR "Cyber Security actions" AND "Cybersecurity culture," AND Software Engineer," AND "SME employees" OR "SME Staff" OR "SME worker," AND "factors" OR "techniques" OR "methods."

b: DATA SOURCES

The authors systematically began to search related studies by limited search strings and keywords to begin the

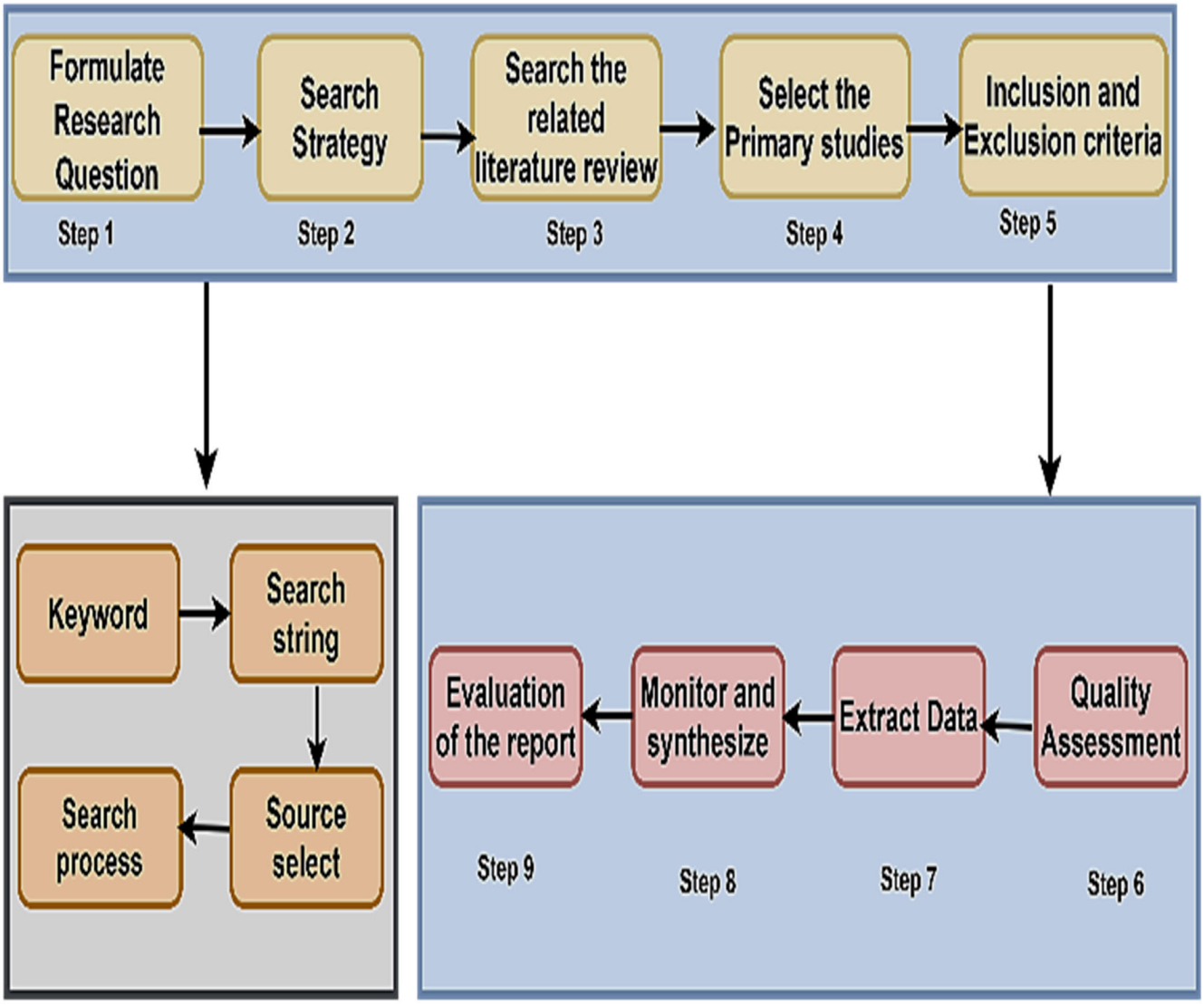

FIGURE 2. Systematic Literature Review Process followed in current study.

Systematic Literature Review. Advanced search in electronic databases was thoroughly performed. The most popular scientific databases were examined to determine the relevant literature for this systematic review. Data sources and the number of studies extracted (primarily) from each source of data (i.e., Emerald Insight, ScienceDirect, IEEE Xplore, and SpringerLink) are present in table 3.

B. PHASE 2: CONDUCTING REVIEW

Conducting review phase includes selecting studies, inclusion and exclusion criteria, and quality assessment.

These are described below:

1) STUDY SELECTION

Screening studies were conducted in accordance with the PRISMA framework and the emerging consensus among authors [22], [23], [90]. Research selection was based on a specific set of rules to improve the quality of existing study. The article screening process began with a verification system and identification of relevant studies, followed by the removal of duplicate studies from various data sources. Before the complete review of the text, abstract and introduction-based screening was also carried out. Later, studies were evaluated according to the inclusion and exclusion process. After a full-text review total 35 potential articles were finally observed. The step-by-step selection process is shown in figure 3. The PRISMA flowchart indicates the number of studies explored at each stage of the study.

2) INCLUSION CRITERIA

The inclusion and exclusion criteria were devised and strictly followed by authors to select primary studies. The inclusion criteria finalized for current research is as under:

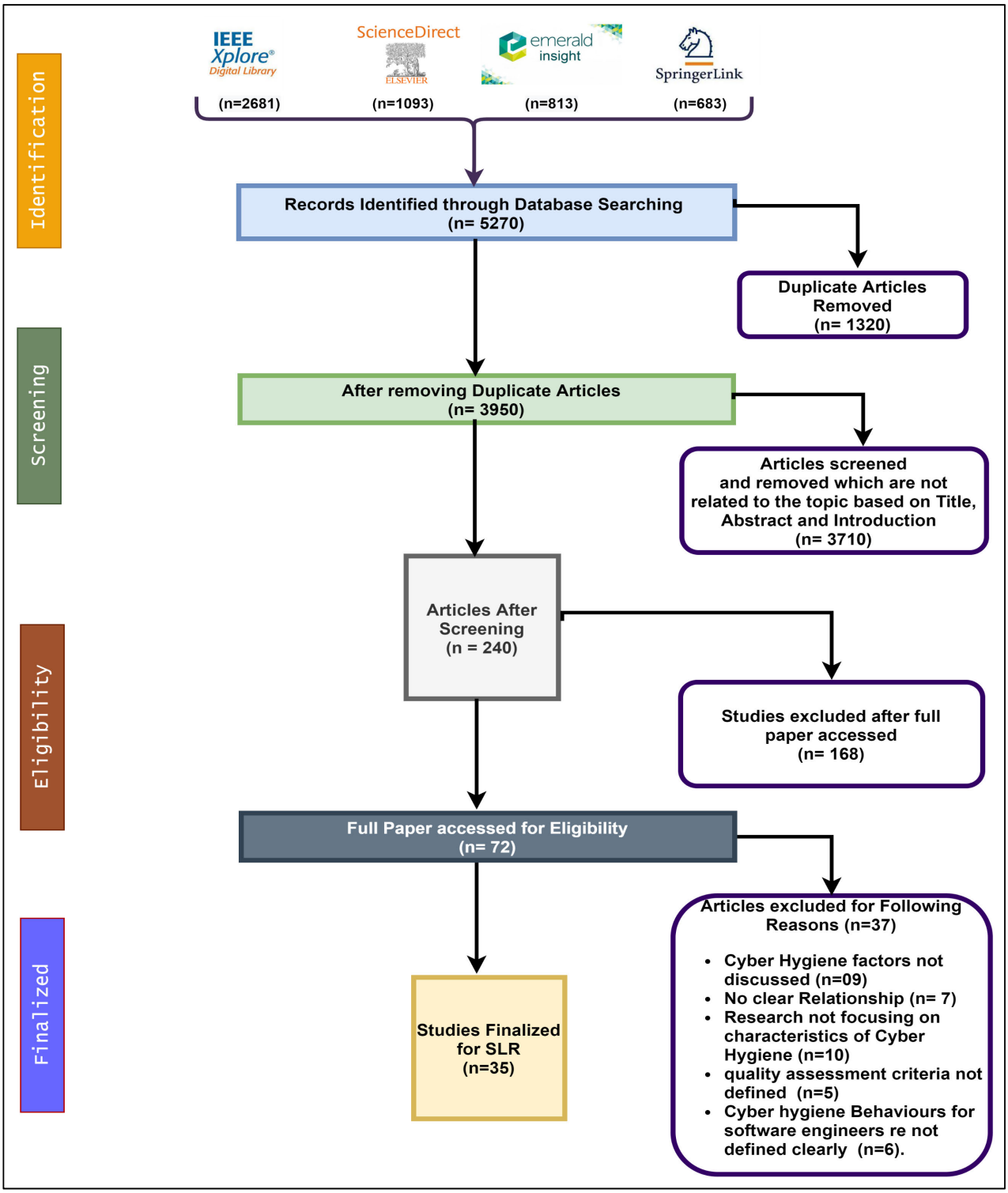

FIGURE 3. Study Selection Process in accordance with PRISMA guidelines [23, 92].

IC-1: Studies must be published in a journal.
IC-2: Studies written in the English language only.
IC-3: Studies must be published between 2010 and 2020.
IC-4: Studies focused on cyber hygiene behaviour of software engineers.

3) EXCLUSION CRITERIA

The following exclusion criteria was set:

EC-1: Newspaper articles, conference papers, online blogs, book chapters, short paper summaries, abstracts, and preliminary studies.

TABLE 3. Details of studies found.

Data Sources (2010-2020)	No. of Publications
Emerald Insight	813
ScienceDirect	1,093
IEEE Xplore	2,681
SpringerLink	683
Total	5,270

EC-2: Irrelevant and out-of-scope studies.

EC-3: Repeated/duplicated literature found from defined data sources.

EC-4: Studies not in the English language.

EC-5: Papers not matching quality assessment criterion.

4) QUALITY ASSESSMENT

The selected studies were evaluated following the procedure recommended by the Centre for Reviews and Dissemination (CDR) Database of Abstracts of Reviews of Effects (DARE), York University [16].

The quality assessment was based on four assessment questions presented in Table 4. The quality assessment questions were given one of the three values (0.0, 0.5, and 1.0).'No' for 0.0 values, 0.5 for 'partial' and 1.0 for 'yes'. Outcome-based studies favoring the quality assessment questions were marked with (1), studies showing some of the properties were marked with (0.5). In contrast, studies not related to the quality question were marked with (0). Table 5 shows the overall score of quality assessment for each paper. Each paper was screened against research questions, and finally, a complete review of the paper's quality was assessed [23]. The checklist for quality assessment questions is listed in Table 4.

C. PHASE 3: DOCUMENTATION REVIEW

The documentation review phase includes extraction of data, validation process, and reporting the review, which is described below:

1) EXTRACTION OF DATA

Thoroughly reviewed the studies extracted for this literature review to obtain the required information; the data acquired were duly noted as having a common opinion of all studies. The characteristics obtained in the perspective of this research are the title of the article, name of the researcher, year of publication, publisher & type of study, application of the analysis, methodology, and sector and security approach discussed. Data were recorded, including the conclusion provided by the authors.

TABLE 4. Quality Assessment Criteria Questions.

S. No.	Questions
QA-1	The study must be focusing mainly on cyber hygiene and its factors on software engineers.
QA-2	The framework of the study must be provided in sufficient detail to interpret the research accurately.
QA-3	Find out the accuracy of how the data were acquired, measured, and reported must be provided clearly.
QA-4	Contribution and credibility of the work based on the results of the study.

TABLE 5. Quality Evaluation of Studies.

Study (S)	Quality Assessment Questions				Total Score
	Q1	**Q2**	**Q3**	**Q4**	
Study-1	1.0	1.0	1.0	1.0	4.0
Study-2	1.0	1.0	1.0	1.0	4.0
Study-3	1.0	0.5	1.0	1.0	3.5
Study -4	1.0	1.0	0.5	1.0	3.5
Study -5	1.0	1.0	1.0	1.0	4.0
Study -6	1.0	0.5	1.0	0.5	3.0
Study -7	1.0	1.0	1.0	1.0	4.0
Study -8	1.0	1.0	0.5	1.0	3.5
Study -9	1.0	0.5	1.0	1.0	3.5
Study -10	1.0	1.0	1.0	0.5	3.5
Study -11	1.0	1.0	1.0	1.0	4.0
Study -12	1.0	1.0	1.0	1.0	4.0
Study-13	1.0	0.5	0.5	1.0	3.0
Study -14	1.0	1.0	1.0	0.5	3.5
Study -15	0.5	1.0	1.0	1.0	3.5
Study -16	1.0	1.0	1.0	1.0	4.0
Study -17	1.0	1.0	1.0	1.0	4.0
Study -18	1.0	0.5	1.0	1.0	3.5
Study -19	1.0	1.0	0.5	1.0	3.5
Study -20	1.0	1.0	1.0	1.0	4.0
Study -21	1.0	1.0	1.0	0.0	3.0
Study-22	1.0	1.0	1.0	1.0	3.0
Study -23	1.0	1.0	1.0	1.0	4.0
Study -24	1.0	1.0	1.0	0.0	3.0
Study -25	1.0	1.0	0.0	1.0	3.0
Study -26	1.0	1.0	1.0	1.0	4.0
Study -27	1.0	0.0	1.0	1.0	3.0
Study -28	1.0	1.0	1.0	1.0	4.0
Study -29	1.0	0.5	0.5	1.0	3.0
Study -30	0.5	1.0	1.0	1.0	3.5
Study -31	1.0	0.5	1.0	1.0	3.5
Study -32	1.0	0.0	1.0	1.0	3.0
Study -33	1.0	1.0	0.5	1.0	3.5
Study -34	1.0	1.0	1.0	1.0	4.0
Study -35	1.0	1.0	1.0	0.5	3.5

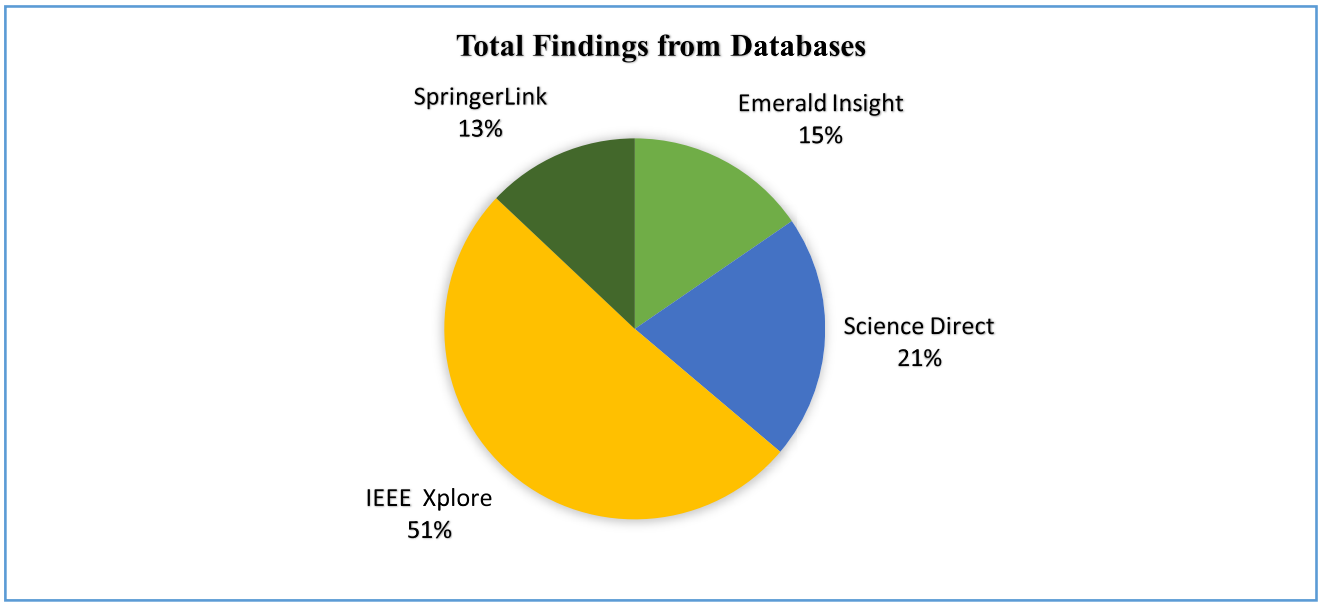

FIGURE 4. Data Source Publication Venues.

2) VALIDATION PROCESS

Kitchenham's recommendations [15] were accurately pursued to confirm the proper selection procedure and prevent inaccuracies in data extraction, research selection, and ''classification'' of articles. In general, uncertainty about the ''Validation Process'' particularly in ''research selection'', ''incorrect data extraction'', ''incorrect classification'', ''research method'' and ''Author Bias''. Therefore, in the present study included authors following the recommendations according to the proposed Kitchenham's. The authors participated in the classification and the studies were carefully discussed to avoid conflicts. The classification results were made on the basis of recommendations and with the mutual consent of the author.

3) REPORTING THE REVIEW

Figure 4 shows several studies found from the defined electronic database. The studies found were published from 2010 - 2020. The studies which have been finalized for systematic literature review from the total findings are exhibited in Figure 5. Table 6 summarises the selected studies and details of factors identified and their relationship (positive or negative relationship).

In figure 4, the pie chart shows the total number of studies found from a data source; 15% of publications were found from Emerald Insight, 21% from ScienceDirect, 51% of studies from IEEE Xplore, and 13% were found from the SpringerLink database.

Shortlisted studies (35) are shown in figure 5, twelve from the ScienceDirect database, ten studies were selected from Emerald Insight, from IEEE Xplore database nine studies were included, and four were selected from the SpringerLink database.

IV. FACTORS IDENTIFIED FROM SYSTEMATIC LITERATURE REVIEW

Research Question 1: What are the key factors associated with the Cyber Hygiene Behaviour of software engineers?

Factors that encourage software engineers in cyber hygiene behaviour have been extracted from the literature examined for this systematic review. These factors are divided into five main categories to improve the understanding and integration of identified factors. These are ''Personal Factors'', ''Social Factors'', ''Socio-cognitive Factors'' Environmental Factors,'' and ''Technological Factors''. Factors are categorized based on nature and relevance; the background of the factor discussed in the literature. A conceptual map of cyber hygiene factors influencing software engineers is shown in Figure 6. The figure shows the five main factors, and each factor is divided into other subfactors associated with software engineers.

A. PERSONAL FACTORS

Personal factors'' are related to people who have a significant influence on their behaviour. Personal factors have a profound effect on cyber hygiene behaviour and vary from person to person. Personal factors include self-efficacy, demographics (age and gender), and knowledge awareness [1]. Figure 7 shows the conceptual map of personal factors.

1) SELF-EFFICACY

Self-efficacy in cyber-security can be defined as a belief in one's ability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability for the businesses' benefits [82]. This parameter measures a user's confidence in

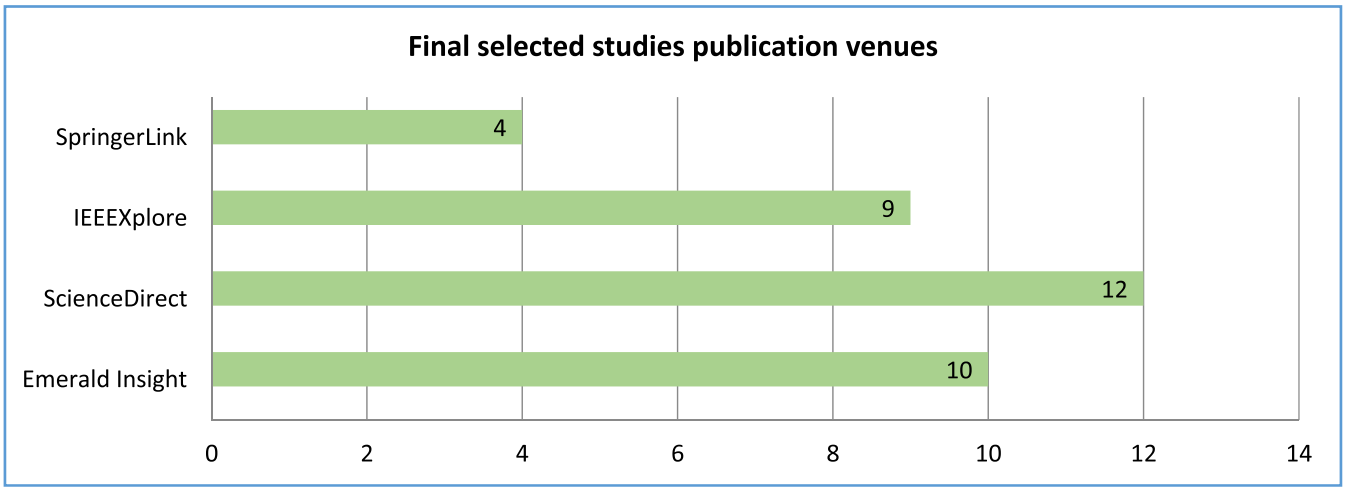

FIGURE 5. Final selected studies from the databases.

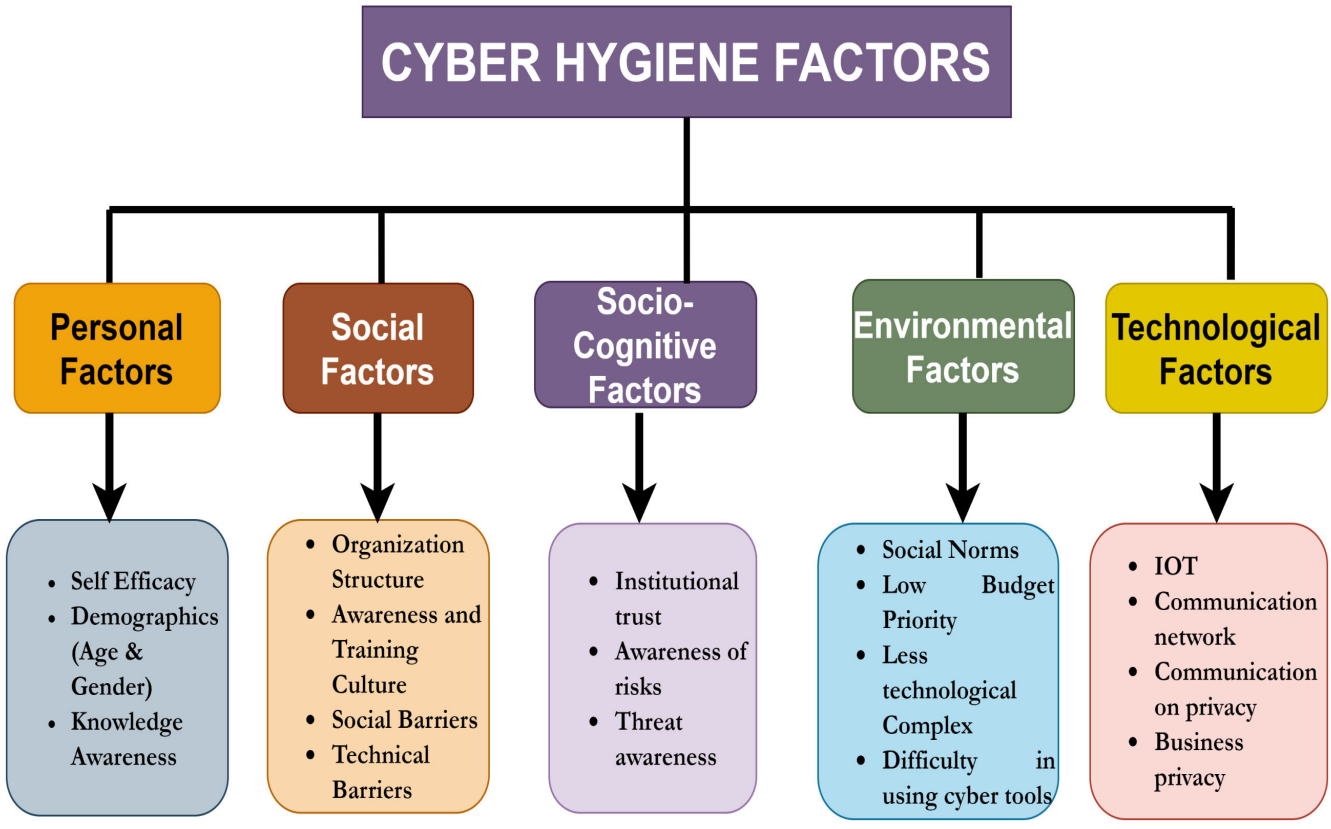

FIGURE 6. Conceptual map of Cyber Hygiene Factors.

the ability to mitigate cybersecurity threats [45], [46], [49]. In studies [50] and [66], authors demonstrate that cybersecurity self-efficacy can influence individuals' intentions to strengthen their cyber hygiene practices. In cyber hygiene, self-efficacy is a part of the appraisal in which a significant predictor of security behaviour is linked to the individual's confidence in performing the security behaviour [83] and [68]. Many studies have found that the stronger the self-efficacy, the more likely a person will undertake a task [8]. People avoid work when self-efficacy is low and self-sufficient [44], [62].

2) DEMOGRAPHICS

The most learned personality traits in cyber hygiene behaviour for employees are age and gender. In research [44]

TABLE 6. Summary of Selected Studies, associated factors, and nature of relationship.

Study Reference	Year	Publisher	Factors	Relationship
43	2020	IEEE Xplore	IOT devices	Positive
			Eavesdropping	Negative
			Phishing	Negative
			Spoofing	Negative
			Knowledge awareness	Positive
44	2020	Science Direct	Phishing	Negative
			Risk awareness	Positive
46	2020	Science Direct	Demographic	Positive
			Phishing	Negative
			Spoofing	Negative
			Self-efficacy	Positive
			Risk awareness	Positive
47	2020	Science Direct	Demographic	Positive
			IOT	Positive
			Training awareness & culture	Positive
			Risk awareness	Positive
48	2020	IEEE Xplore	Demographic	Positive
			Risk awareness	Positive
			Threat awareness	Positive
			IOT devices	Positive
			Social norm	Positive
			Less technology complex	Positive
49	2020	Emerald Insight	Social norm	Positive
			Demographic	Positive
			Organizational structure	Positive
			Technical Barrier	Negative
			Difficulty in using cyber tools	Negative
61	2020	ScienceDirect	Awareness & training culture	Positive
			IOT Devices	Positive
			Organizational Structure	Positive
			Awareness of risk	Positive
65	2020	Emerald Insight	Phishing	Negative
			Spoofing	Negative
			Demographic	Positive
			Self-efficacy	Positive
			Social Norm	Positive
			Social Barrier	Negative
69	2020	ScienceDirect	IOT Devices	Positive
			Difficulty in using cyber tools	Negative
			Awareness of risk	Positive
72	2020	IEEE Xplore	Awareness and Training	Positive
			Risk awareness	Positive
			Threat awareness	Positive
73	2020	SpringerLink	Risk Awareness	Positive
			Technical Barrier	Negative
			IOT	Positive
42	2019	IEEE Xplore	IOT devices	Positive
			Theft	Negative
45	2019	ScienceDirect	Self-efficacy	Positive
			Threat Awareness	Positive
			Awareness of training culture	Positive
			Organizational structure	Positive
50	2019	Emerald Insight	Training and awareness	Positive
			Organization structure	Positive
			Social Barrier	Negative
			Technical Barrier	Negative
			Spoofing	Negative
56	2019	Emerald Insight	Organization structure	Positive
			Low budget	Negative
			Awareness of training	Positive

TABLE 6. *(Continued.)* **Summary of Selected Studies, associated factors, and nature of relationship.**

			Awareness of risk	Positive
67	2019	Emerald Insight	Self-efficacy	Positive
			Social Barrier	Negative
			Social Norm	Positive
			Technical Barrier	Negative
			Low budget	Negative
68	2019	SpringerLink	IOT devices	Positive
			Technical Barriers	Negative
			Less technology complex	Positive
			Theft	Negative
62	2019	IEEE Xplore	Awareness & training culture	Positive
			Threat awareness	Positive
			Awareness of risk	Positive
			Social Barrier	Negative
			Technical Barrier	Negative
			Eavesdropping	Negative
			Phishing	Negative
1	2018	Science Direct	Demographic	Positive
			Knowledge awareness	Positive
27	2018	ScienceDirect	Demographic	Positive
			Risk awareness	Positive
			Awareness of training culture	Positive
			Institutional trust	Positive
			Social norm	Positive
78	2018	IEEE Xplore	Awareness & training culture	Positive
			Threat Awareness	Positive
66	2018	Emerald Insight	Awareness of risk	Positive
			Threat Awareness	Positive
			Institutional trust	Positive
			Awareness & training	Positive
70	2018	IEEE Xplore	IOT devices	Positive
			Technical barrier	Negative
			Less technology complex	Positive
75	2018	SpringerLink	Phishing	Negative
			Theft	Negative
			Spoofing	Negative
63	2018	Emerald Insight	Phishing	Negative
			Theft	Negative
			Spoofing	Negative
			Eavesdropping	Negative
			Technical Barrier	Negative
			Less technology complex	Positive
			IOT devices	Positive
57	2017	ScienceDirect	Self-efficacy	Positive
			Demographic	Positive
			Social barrier	Negative
			Low budget	Negative
58	2017	ScienceDirect	Institutional trust	Positive
			Awareness to risk	Positive
			Phishing	Negative
74	2017	SpringerLink	Awareness and Training	Positive
			IOT Devices	Positive
			Threat Awareness	Positive
14	2016	Science Direct	Demographic	Positive
			Social Norm	Positive
			Organization structure	Positive
			Threat awareness	Positive
			Institutional trust	Positive
59	2016	IEEE Xplore	Awareness & training culture	Positive
			Awareness risk	Positive
			Threat Awareness	Positive

TABLE 6. *(Continued.)* **Summary of Selected Studies, associated factors, and nature of relationship.**

55	2015	Emerald Insight	Risk awareness	Positive
60	2014	Emerald Insight	IOT devices	Positive
			Organizational structure	Positive
			Awareness & training culture	Positive
			Awareness risk	Positive
64.	2014	Emerald Insight	Awareness of risk	Positive
			Social Norm	Positive
			Low budget	Negative
			Social Barrier	Negative
54	2014	ScienceDirect	Phishing	Negative
			Less technology complex	Positive
			IOT Devices	Positive
71	2010	IEEE Xplore	Phishing	Negative
			Spoofing	Negative
			Theft	Negative
			Eavesdropping	Negative
			Technical Barrier	Negative

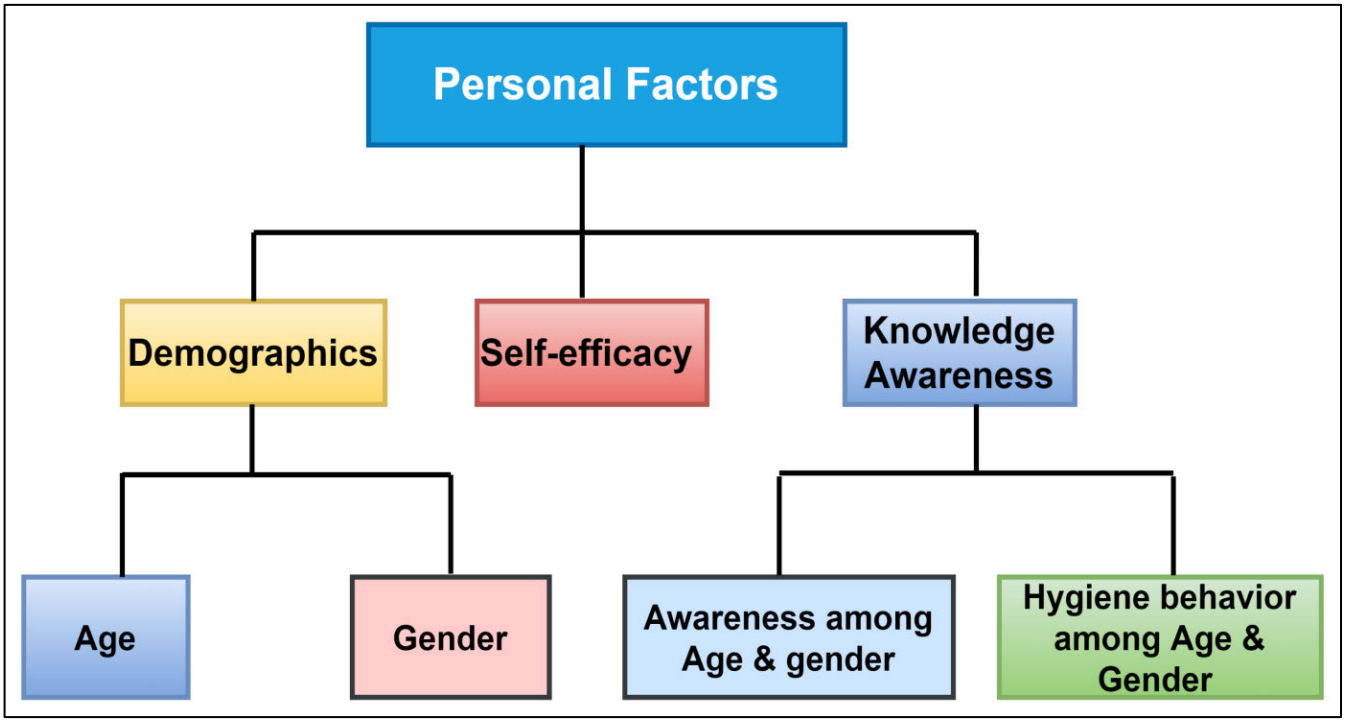

FIGURE 7. Conceptual map of Personal Factors [1].

authors observed that both age and gender profoundly affect cyber hygiene behaviour.

a: GENDER

There are individual differences among men and women's cyber hygiene habits. The authors in [1] also explained that women had been found to create weaker passwords and updated software less often than males; it is also given that males had more knowledge about cyber hygiene than females [27], [50].

b: AGE

Old age is a significant predictor of non-compliance with advanced cyber hygiene practices [24], [25], [46]. Most users, young and old age, share detailed personal information such as their address and phone number on social media, most of whom do not see their privacy settings [47]–[49]. In [1] and [55], the authors found a difference between behaviours showing older groups (45 to 55 & older) had significantly protective behaviours than the youngest group (18 to 24). The authors also concluded that no dissimilarities were found

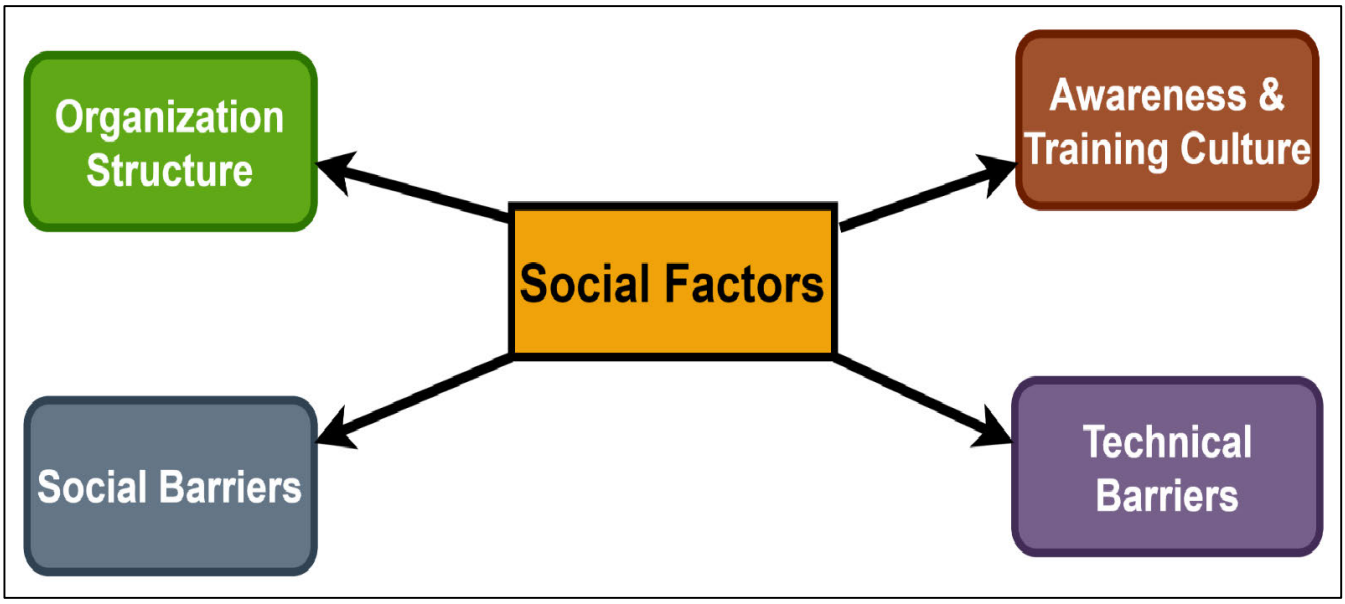

FIGURE 8. Conceptual map of social factors [28].

among behaviours of the other age groups compared [8], [51], [52], [62].

3) KNOWLEDGE AWARENESS

Knowledge awareness is divided into two parts; one is awareness among age and gender, and the second is hygiene behaviour among age and gender. These two types are described below.

a: KNOWLEDGE AWARENESS AMONG AGE & GENDER

There are no dissimilarities in the knowledge of cyber-hygiene between age groups. When it comes to cyber-hygiene, older users familiar with less technology are more likely to be at risk. They are most likely to be attacked. The authors tested cyber hygiene knowledge between different age groups, but no differences were found between the inside and age on security awareness and behaviour. The authors also explored cyber hygiene knowledge among genders and found significant differences [1], [2].

On the other hand, it is found from [26], [47] that men have more knowledge awareness about cyber hygiene than women. However, [27] shows that males did not vary than females' cyber-hygiene behaviour despite having additional awareness.

b: HYGIENE BEHAVIOUR AMONG AGE & GENDER

In [1], researchers concluded that there are no differences between age and behaviours. Still, the survey shows that women's cyber hygiene behaviour does not differ from that of men despite much knowledge. It is widely believed that age contributes to cyber hygiene behaviour [25].

B. SOCIAL FACTORS

The study of an effective information security management system is incomplete if the system does not consider human and social factors. The social factor is divided into four sub-factors shown in figure 8. Below is the conceptual framework of social factors.

1) ORGANIZATION STRUCTURE

Responsibility for organization and communication structure is critical in predicting data security. According to [26], organizational information about cybersecurity and cyber hygiene practices plays a key role in making decisions. An organization's cyber hygiene practices are the measurement of the organization's capability to remain secure [61]. The organizational structure has a significant function in implementing cyber hygiene. The effectiveness of the entire information security framework is calculated and regulated to adjust to the changing circumstances [27]. Cyber hygiene in an organization should be viewed as personal hygiene [49]. Once properly integrated into an organization, it will be simple in daily routines, good behaviours, and occasional checkups to ensure the organization's online health is in optimum condition [62]. Authors in [45], [52], and [53] observed the literature about awareness of cyber hygiene practices and should communicate these practices to all unit managers; in addition to these critical actions are assigned to the responsible officer so that awareness regarding cyber hygiene practices is always informed to all employees of organization [54], [55], [58].

2) AWARENESS AND TRAINING CULTURE

In [28], [49], and [51], it is reported that a culture of awareness and training is also essential and should not

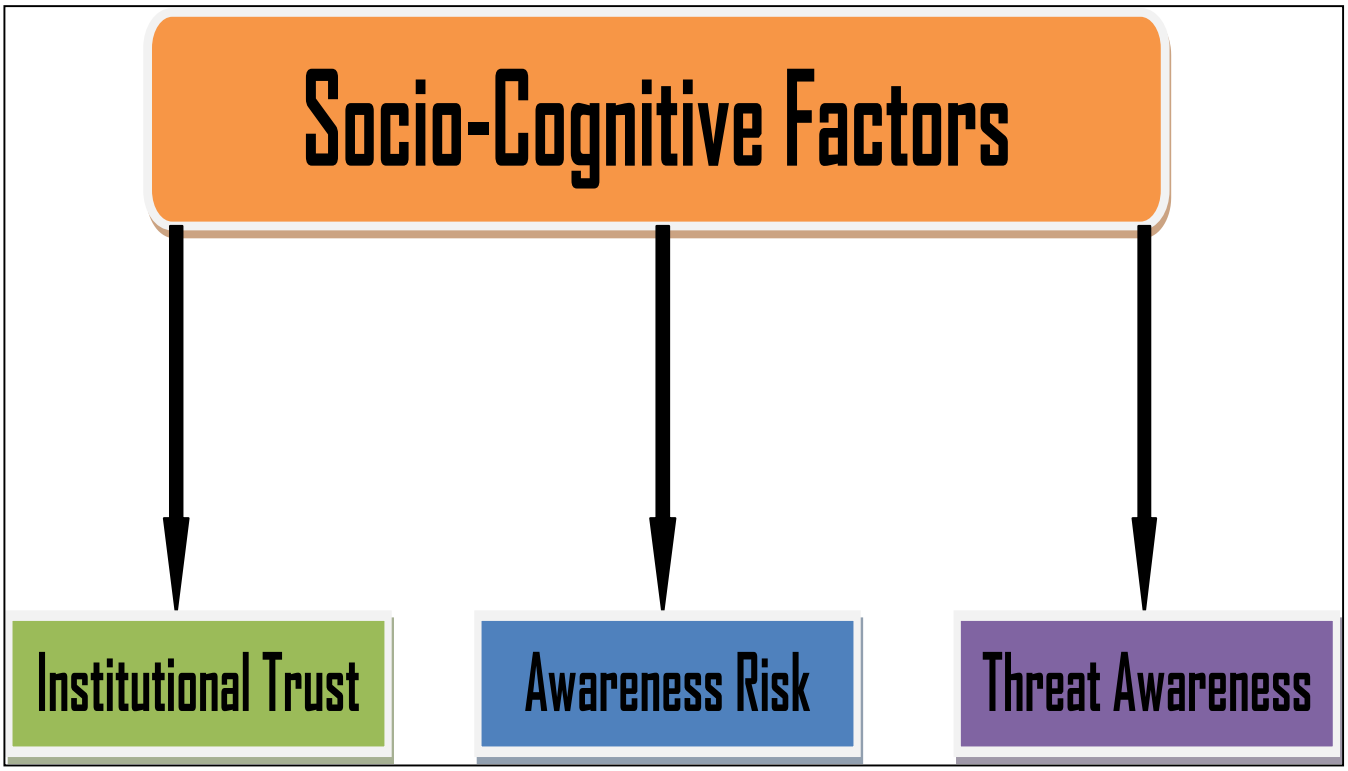

FIGURE 9. Conceptual map of Socio-Cognitive Factors [30].

be overlooked. Cybersecurity awareness and cyber hygiene information are mandatory for all employees [45], [47], [50]. Cyber hygiene detection and security awareness are done in the same way and are done legally [53], [58], [63]. In [27], [55], [57], [59], [60], and [67], the authors suggested that the employees should receive ongoing training in cybersecurity awareness to identify unwanted and suspicious activities in the organization so that users can secure their information.

3) SOCIAL BARRIERS

Social barrier refers to lack of dedication and attention from management, the lack of management awareness, and a lack of security awareness between employees [29]. Government guidelines on cyber hygiene behaviour and security awareness are not well defined [8], [44], [50], [53]. Organizational employees do not have time to start a security process [59], [61], [63]. The social barrier demands to balance the needs so that employees should meet their business objectives and maintain security [65], [68].

4) TECHNICAL BARRIERS

The technical barriers in cybersecurity are limited to the budget [27], [53]. The critical problems for the effective exchange of information for coordinating cyber-attack responses still exist due to legal and technical barriers and lack of interest from cybersecurity stakeholders regarding information sharing [50], [59], [63], [69]. The fast and rapid change in information technology and the nature of cyber-attacks are also the cause of these barriers [64], [71], [72].

C. SOCIO-COGNITIVE FACTORS

Very few studies focused on social behaviour and understanding the user's cyber hygiene practices and security behaviour [29]. The study [30] found a complicated relationship between risk, threat, and vulnerability awareness. This study also found that vulnerability awareness is the product of risk and threat awareness on a socio-cognitive level. Figure 9 shows the conceptual map of socio-cognitive factors.

1) INSTITUTIONAL TRUST

Institutional trust in cyber hygiene is one of the factors that contribute to social thinking [28]. The user trusts that online application stores only keep softwares that follows cyber hygiene practices; safe for the user and has no problems and malicious code [29]. The researchers believe that trust in cyber hygiene is rooted in a social structure, which builds on how people develop their beliefs with confidence, often referred to as institutionalized trust [27], [51], [54], [55]. Institutional trust also relates to smart devices or software that are reliable and trustworthy to the system operator. In cyber hygiene, the institution's trust will focus on the applicant's trust [56], [59], [63], [67].

2) AWARENESS OF RISK

The studies [29], [65], [70] reported the amount of awareness a person has regarding cyber-security. Employees should be aware of unauthorized emails [44], [57], [58], [67], text messages, and know that an unauthorized person can access their personal and financial information. [27], [48], [51], [73], [74]. Most of the research focuses on employee information about sensitive documents, browsing the Internet through illegal websites [44], [59]–[61], [63].

3) THREAT AWARENESS

Threat awareness is the amount of knowledge about the threat and attacks an employee has [28], [29]. As the threats become more intense, they become vulnerable, more numerous and significant impact on risk [45], [51]. With new technology, employees generally have no information on cybersecurity monitoring. Employees should have awareness of viruses, malware attacks, and network attacks and threats [57], [59].

D. ENVIRONMENTAL FACTOR

The findings show that four factors influence how organizations perceived cybersecurity. These are as follows: social norm, budget, IT complexity, and complicated cybersecurity tools.

1) SOCIAL NORMS

Social norms are the unwritten rules of behaviour considered acceptable in a group or a society [29]. It is worth noting that many powerful social norms, for example, that indicate what constitutes good software, have little or no legal standing, including laws and regulations to ensure basic cyber hygiene [30]. Besides, some cyber hygiene practices may be created by small groups or during closed departmental meetings that are not ready to increase their legitimacy [48], [49], [63]. Specific trends in cybersecurity and cyber norms, tend to focus on states as main factors [27], [52]. The organizations will sign co-operatives that strengthen the norms [60], [62], [73]. Social norms for cyber hygiene can change according to the environment, situation, and culture in which they are found [64]–[66].

2) LOW BUDGET PRIORITY

The budget is always identified as a barrier to adequate security measures by most stakeholders [30]. The small organization will not spend money on private security tests because they are costly; this is the reason that the organization prefers external testing, just because of the low budget [31]. Huge funds are required to implement the defense mechanism of systems and the respective processes [44], [58]. The limited budget available to SMEs makes it impossible for them to outsource firms' security tests that leave these organizations at high risk [65], [68].

3) COMPLEXITY OF TECHNOLOGY

SMEs often do not have complex legacy systems and assumed that they do not face security threats like large corporations [32], [33]. The organization will not become a target for cybercrime because of its size. Legacy systems have been identified as the source of security issues because a customized security code must always be written to maintain cybersecurity practices [27], [48], [53]. Small companies have fewer assets, and they think they will maintain cyber hygiene practices very easily [69]. In contrast, large companies have multiple legacy systems and require a lot of work to keep them safe [56], [60], [64].

4) DIFFICULTY IN USING CYBER TOOLS

While most SMEs authenticate that cost was one of the barriers to cyber-security and their practices [31], some organizations have adopted and are currently using cyber tools and strategies for cyber hygiene practices in their organizations [32]. They should be aware of how to use them to derive maximum benefit; the lack of IT experts (security experts) was a factor, although these can be inferred from the limited use of cybersecurity practice and the lack of confidence in security implementation within the SMEs [52]. The main challenge in terms of cyber hygiene is that SMEs had limited use of cybersecurity tools due to their complexity of using them efficiently [33]. There was a perception that cyber tools were difficult to implement and sustain and will not realize any value for cyber hygiene [49], [66], [70]. Environmental factors and their classifications are presented in figure 10.

E. TECHNOLOGICAL FACTORS

Technology factor includes IoT devices, communication networks, and communication privacy and business privacy. Figure 11 shows the conceptual map of technological factors.

1) IOT DEVICES

The Internet of Things has brought many distinguished and unique devices; it provides free access to various online services to employees [32]. IoT plays a significant role in developing and maintaining the benefits of the organization. IoT's cyber hygiene structure guarantees that devices are kept in a secure environment and that users can practice them securely [42]. The devices connected through IoT architectures might initiate from various developers and operating systems, leading to the possibility of the most important security breaches. Many IoT devices, as well as ''virtual assistants'' (including Amazon's Echo and Google's Home), can gather and investigate streams of sensitive personal data [43]. Cyber hygiene practices for IoT guarantees that IoT will develop a secure network for people, software/hardware, processes, and things. The more devices a user attaches, the greater the risk to the person and the network, and the higher the cybersecurity risk to the organization [59].

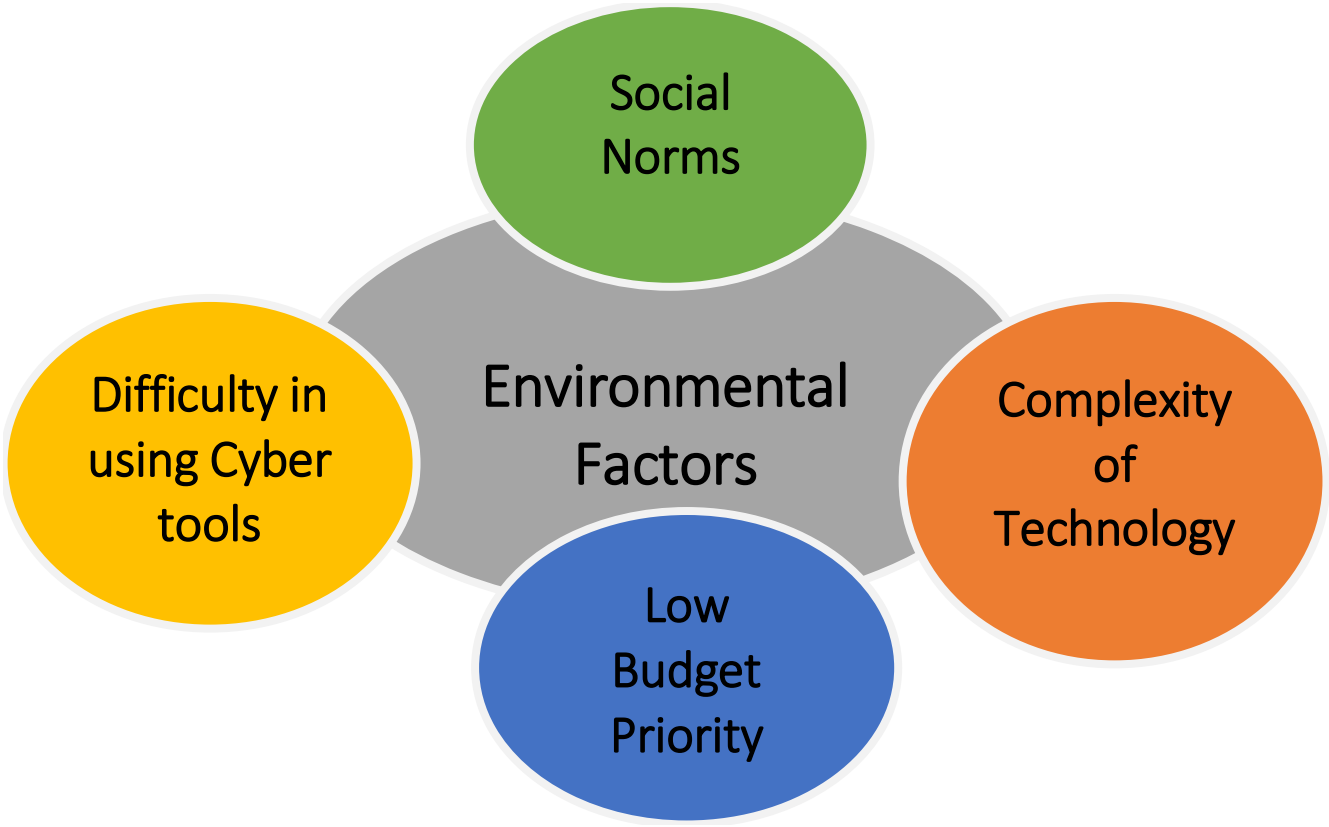

FIGURE 10. Conceptual map of Environmental Factors [31] and 34].

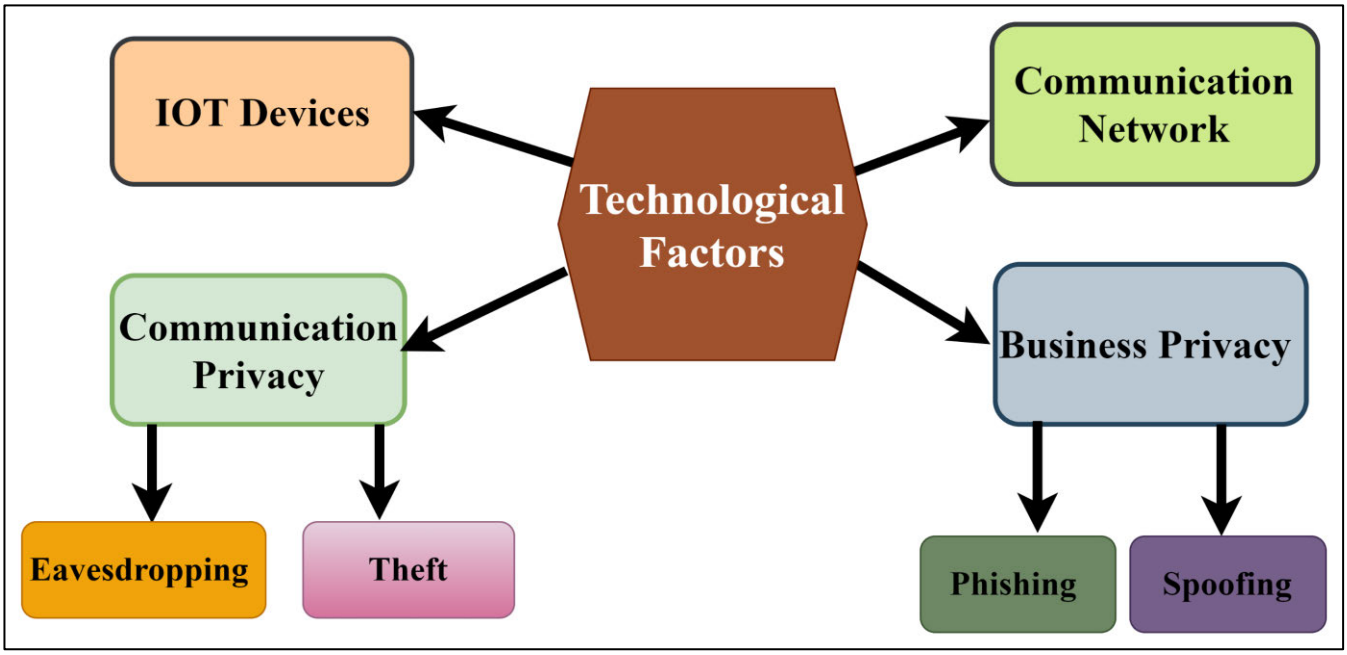

FIGURE 11. Conceptual map of Technological Factors [33].

2) COMMUNICATION NETWORKS

Using Wi-Fi, 4G, RFID, GSM, and many other communication networks, cyber-physical objects can be integrated into an organization. Each of them has some security issues that need to be addressed during the application and deployment of communication technologies to secure the data.

3) COMMUNICATION PRIVACY

Communication privacy is of two types, eavesdropping and theft, which are explained below.

a: EAVESDROPPING

Eavesdropping tools are used on a particular network to check the communication channels, capture network traffic behaviours, and locate the network map [29], [43], [47]. Eavesdropping is a dangerous threat that can lead to loss of employee integrity and confidentiality, leading to financial and personal failures of an organization [59], [63], [64], [72].

b: THEFT

Theft is defined as stealing sensitive data of organization, credentials, software keys; and stealing tangible items (handheld devices such as smartphones, laptops, and tablets) and electronic devices [29], [30], [46], [60]. It violates system access and confidentiality, resulting in financial instability and reputable leases [64], [65], [67], [72], and [76].

4) BUSINESS PRIVACY

Business privacy includes two types that are named phishing and spoofing and are described below.

a: PHISHING

Phishing of sensitive information is a big issue for businesses, governments, and technology. The outcome of phishing has devastating consequences [34], [35]. It is estimated that more than 80% of organizations experienced stealing sensitive information [36], [47], [48]. 83% of the respondents face the crime of phishing in 2018, and 76% in 2017. By the end of 2017, the average user received 16 emails of phishing scams per month. 30% of sensitive phishing messages were opened in 2016 - up from 23% in 2015 [50]. 49% of businesses worldwide reported being infected with viruses and malware, in 2017 an increase of 11% compared to the 2016 results [63], [64], [66]. These attacks resulted in the loss of billions of dollars each year [37], [56], [59]. While many resources have been brought to address this phishing problem, but it continues to grow [38]. Educate and train employees about phishing techniques is the way forward. Keeping current security with the latest patches and updates; install a safety net using other security measures [39], [53]. Employees should have believed that to stealing sensitive information is considered a threat in social engineering [72]. Additionally, employees should back up their data regularly by storing essential files on the drive or offline server. Email verification software can help prevent phishing emails from stealing sensitive information for an organization [62], [67], [76].

b: SPOOFING

In the computer world, spoofing means pretend to be another person or computer, often by giving false information. Spoofing could take many forms in the computer world, all of which involve misrepresenting information [40]. Certain spoofing types are IP spoofing, URL spoofing, Email spoofing, DNS spoofing, and MAC spoofing [41], [45]. As Internet access is now more extensively accessible, it is much easier for attackers to find multiple clients and capture and communicate with addresses and employ them to initiate attacks that are different from the network itself (routes and network services such as DNS) and continue other strangers and customers [47], [50], [53]. This can be surprising since sensitive websites are often protected using SSL or TLS protocols. Web spoofing attacks focus on the gap between user intentions and expectations and security's address and method specified by the browser on the web [64], [66]. Servers, clients, and routers cooperate and follow standard rules without factual errors [72], [76].

V. RELATIONSHIP OF IDENTIFIED FACTORS

This portion presents the results of the second research question of this study.

Research Question 2

What is the relationship between identified factors and intentions to perform cyber hygiene behaviour?

This research aims to find the relationship between cyber hygiene factors associated with software engineers. The study examines the relationship of factors on adopting cyber hygiene behaviour by software engineers. The relationship of cyber hygiene factors has been classified as positive or negative depending on ''Positive Factors'' and ''Negative Factors''. The positive factors are the factors having a positive association with good cyber hygiene behaviour. The negative factors are acting as barriers among software engineers and cyber hygiene. The conceptual map of frequently reported, ''Positive factors'' driving software engineers for cyber hygiene behaviour and repeatedly stated, ''Negative Factors'' that act as a barrier to the adopting cyber hygiene are exhibited in Figure 12. Moreover, table 6 presents the data source, publication year, and relationship of identified factors.

VI. FACTORS ANALYSIS

This study identified the factors that led software engineers to the adoption of cyber hygiene behaviour. This study's purpose was not limited to determining the factors; the scope also comprises finding the relationships among the associated factors and cyber hygiene. Therefore, this study identified the factors that push software engineers to cyber hygiene and detected the interaction of factors identified with cyber hygiene behaviour, i.e., ''Positive'' or ''Negative.'' The identified factors are divided into five main categories ''Personal Factors'', ''Social Factors'', ''Socio-Cognitive Factors'', ''Environmental Factors'', and ''Technological Factor.'' These categories are shown in Figure 6. The frequency among the included studies is divided into positive and negative factors. This study revealed that the technological factor category has the highest frequency of five, followed by social and environmental factors with four factors.

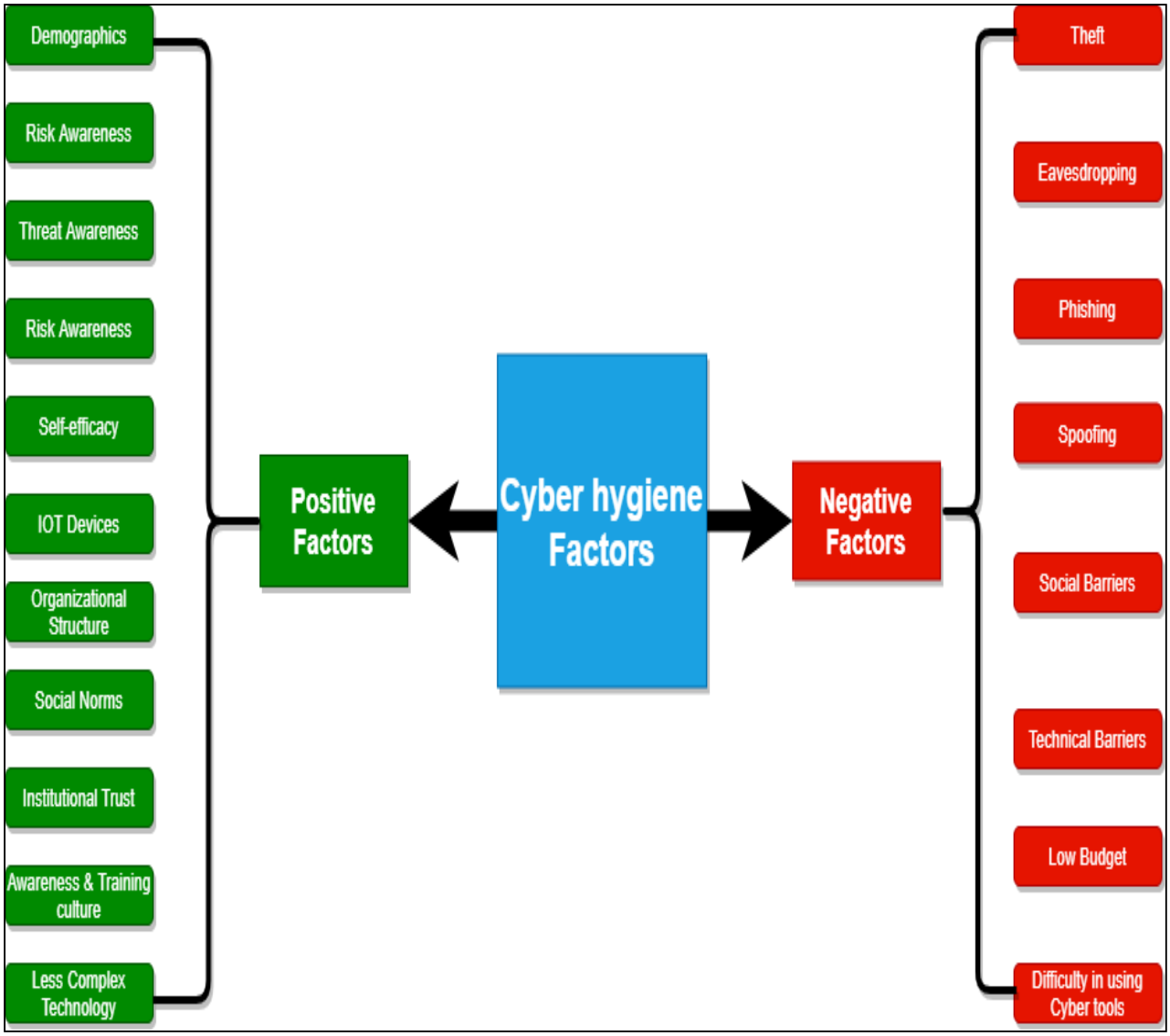

FIGURE 12. Factors having a positive and negative relationship with Cyber Hygiene Behaviour.

Each, personal and socio-cognitive category has three factors each as shown in figure 13.

VII. SIGNIFICANCE OF THE IDENTIFIED FACTORS

Software engineering employees might consider the identified factors by going through the list of cyber hygiene factors (positive & negative) and evaluating themselves against each factor to recognize their strengths and potential weaknesses. The outcomes of such analysis may suggest where organizational efforts and resources may be essential to enhance cyber hygiene behaviour among software engineering employees. A summary of all factors is presented in Table 7. Figure 14 shows factors that are the most cited. From the positive category ''Risk awareness'' appeared as the maximum cited factor (17 times), and the negative category ''phishing'' emerged as most cited factor (10 times). Special measures and steps may be taken to overcome the difficulties faced by software employees due to lack of cyber hygiene knowledge. The top seven reported factors associated with cyber hygiene behaviour among software industry employees are displayed in figure 14. However, figure 15 shows all identified factors of cyber hygiene that are associated with software industry employees.

VIII. DISCUSSION AND FINDINGS

The research on cyber hygiene behaviour has the emergence in the cyber hygiene occurrence. Researchers conceptualized cyber hygiene and surveyed it through questionnaires to get the experimental verification of various theories such as the theory of planned behaviour to know the effects of cyber hygiene behaviour. The present systematic literature review (SLR) examined these phenomena of cyber hygiene behaviour by analyzing previously published studies.

This study presented explanatory results about what users know about cyber hygiene and what they do for it. It is widely believed that age contributes to cyber hygiene behaviour.

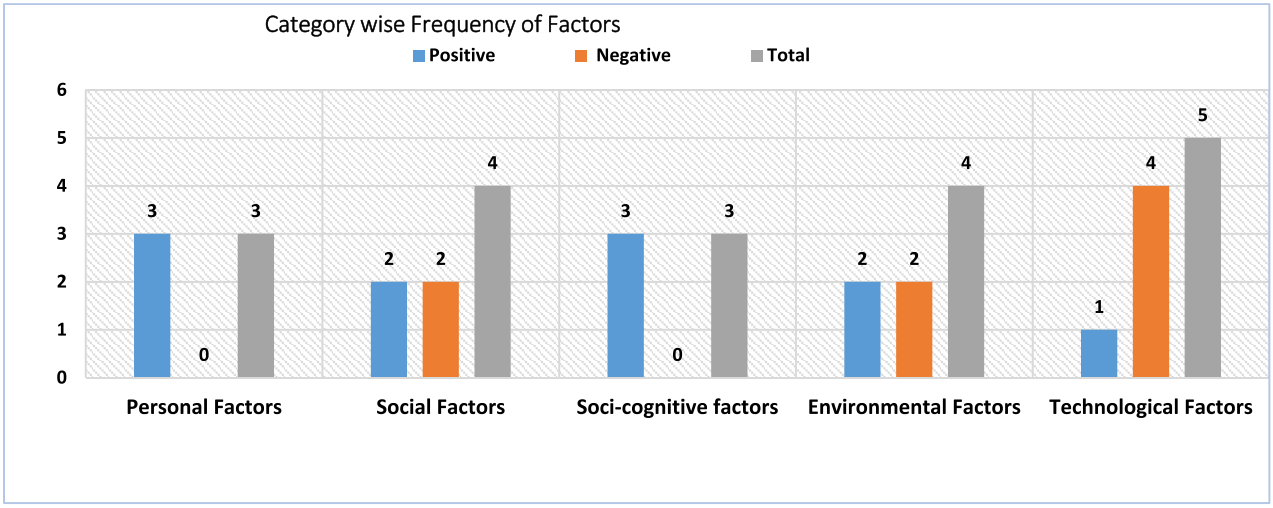

FIGURE 13. Frequency of factors.

TABLE 7. Summary of factors.

Positive Factors	Studies	Frequency
Personal Factors		
Self-Efficacy	[50], [69], [49], [71], [61]	5
Demographic	[50], [52], [53], [69], [2], [56], [61], [55]	8
Knowledge awareness	[47], [2]	2
Social Factors		
Organization Structure	[53], [65], [49], [54], [60], [55], [64]	7
Awareness & Training Culture	[51], [65], [76], [49], [54], [60], [66], [56], [70], [78], [63], [64]	12
Socio-Cognitive Factors		
Institution Trust	[56], [70], [62], [55]	4
Awareness Risk	[48], [50], [51], [52], [65], [73], [76], [77] , [60], [66], [56], [70], [62], [63], [59], [64], [68]	17
Threat Awareness	[52], [76], [49], [66], [57], [70], [78], [55], [63]	9
Environmental Factors		
Social Norm	[52], [53], [69], [71], [56], [55], [68]	7
Less Technological Complex	[52], [72], [74], [67], [58]	5
Technological Factors		
IOT devices	[47], [51], [52], [65], [73], [77], [46], [72], [74], [67], [78], [64], [58]	13
Negative Factors	Studies	Frequency
Social Factors		
Social Barrier	[69], [54], [71], [66], [61], [68]	6
Technical Barrier	[77], [54], [71], [72], [66], [74], [67], [75]	8
Environmental Factors		
Low Budget	[60], [71], [61], [68]	4
Difficulty in using cyber tools	[53], [73]	2
Technological Factors		
Eavesdropping	[47], [66], [67], [75]	4
Theft	[46], [72], [79], [67], [75]	5
Phishing	[47], [48], [50], [69], [66], [79], [67], [62], [58], [75]	10
Spoofing	[47], [50], [69], [54], [79], [67], [75]	7

The impact of age on knowledge and behaviour on cyber hygiene was examined in this study. The users of old age tend to act securely than young age users. These results are not contradictory since young age people are considered to have a lot of technical knowledge. And amazingly, there was no dissimilarity in the knowledge of cyber hygiene between age groups. When it comes to cyber hygiene, old age users, often illustrated as having less awareness of technology, are less likely to be at risk. From this research, it was observed that men knew more about cyber hygiene than women. It is also observed that although men have a lot of experience, they are not different from the cyber hygiene behaviour of women.

Given that females' self-efficacy performance is much lower than males', female self-efficacy can be the intervention's goal. Social norms and styles of understanding contribute to the divergence of risk perception. Social norms in various social environments profoundly affect how people will not perceive risk and how they will respond to that risk.

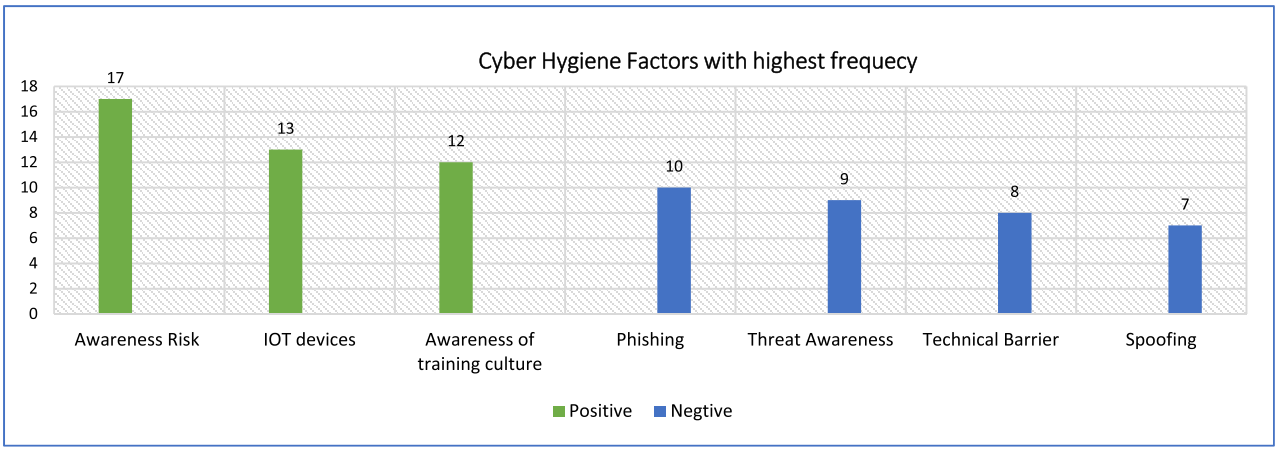

FIGURE 14. Top seven cyber hygiene factors associated with software industry employees.

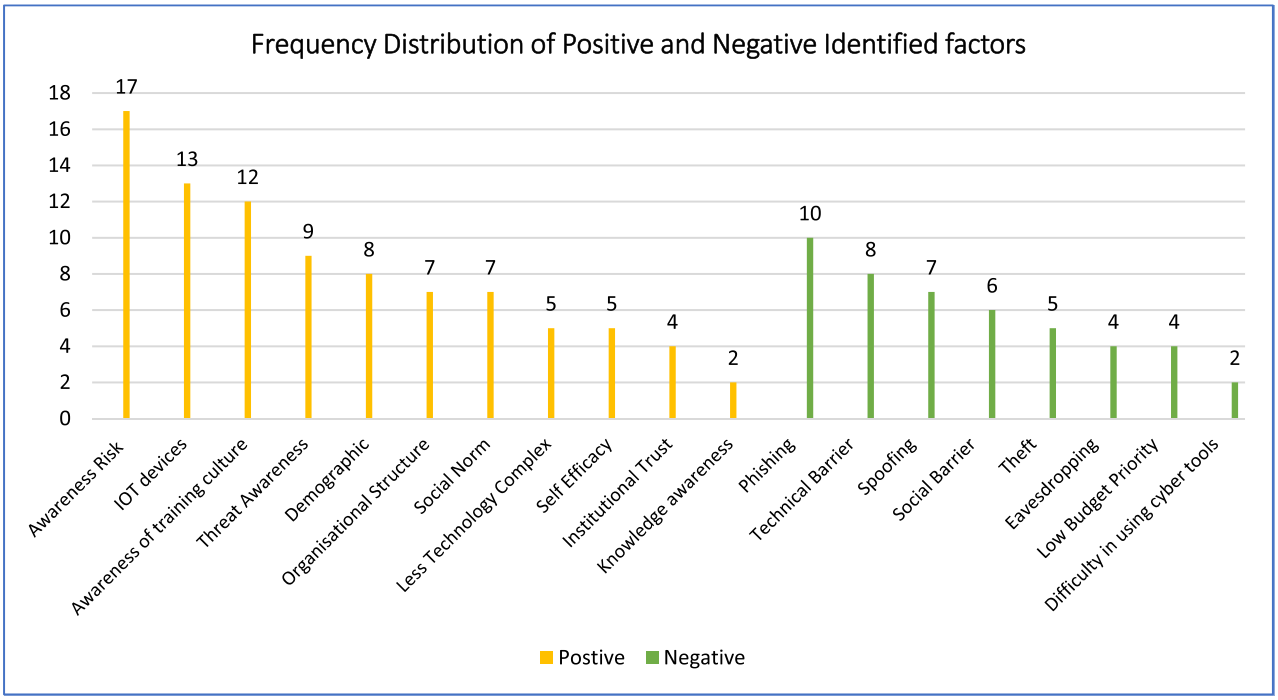

FIGURE 15. Frequency distribution of positive and negative factors.

The organizational structure is a similar construct to corporate culture, and research has shown a positive relationship. Organizations are also at risk of being targeted by social engineering attacks, i.e., phishing, eavesdropping, theft. Some people are more vulnerable to such attacks than others; this illustrates the organization's negative relationship. It is important to identify male and female safety practices and the similarities and dissimilarities in their safety practices to design cyber safety employee training programs [7]. Organizations need to raise awareness of employee safety and their ability to engage in secure cybersecurity practices because the cybersecurity practices of workers are influenced by many different psychological and social factors [8].

Figure 15 shows the frequency of all positive and negative identified factors of cyber hygiene behaviour. It is observed from the graph that the positive identified factor ''risk awareness'' has the highest count of seventeen, after that ''IOT devices'' which have a count of thirteen, the demographic factor has nine counts, awareness training culture have eight counts, organization and social norm have the same number of counts that is seven, count for threat awareness is six, self-efficacy and technology complex have a count of five and institutional trust count of four. From the negative identified factors, ''Phishing'' has the highest count of ten; technical barrier has the count of eight, spoofing has seven counts, six-count for the social barrier, five for theft, four for

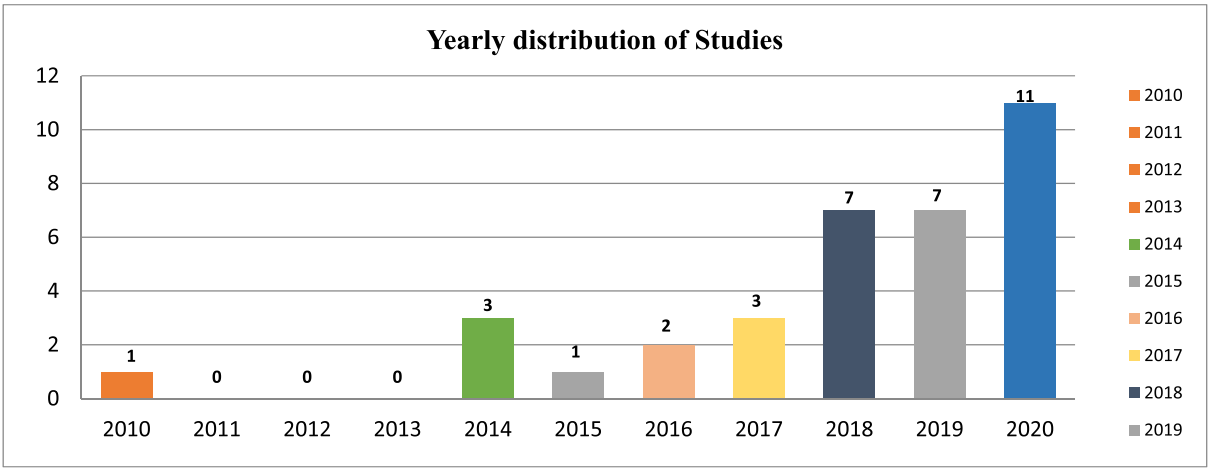

FIGURE 16. Yearly distribution of studies.

eavesdropping and low budget, and two for difficulty in using the cyber tool.

The given figure 16 illustrates the yearly distribution of selected studies. All the selected studies were published from 2010-2020. A total of thirty-five studies were selected according to cyber hygiene behaviour. The year 2020 have the highest peak which means more related research studies were found in this year, the year 2019 and 2018 have second highest, the year 2017 and 2014 have the same number of research studies, found two studies from the year 2016 and one from 2015 and 2010. However, found no studies in the year 2011, 2012, and 2013.

IX. IMPLICATION FOR PRACTICE

Cyber hygiene is a set of practices, whereas protection awareness is often linked to information security. Various solutions have been developed to secure information, but it remains a major challenge for many companies at a high level [73]. From several studies, it has been found that awareness of security has a significant impact that effectively influences organizations [74]. The identified cyber hygiene factors could serve as a guide to cyber hygiene behaviour among software Engineers. Software engineers can be targeted through malicious social engineering attacks, so it is better to inform employees about cybersecurity practices. By giving awareness and training of cybersecurity behaviour and cyber hygiene practices, employees can have a better understand and be better prepared for potential future social engineering attacks in their personal and professional lives. Organizations must establish clear authority, develop policies and procedures, and facilitate workshops and seminars, messages, educational campaigns to train the software engineers according to safety.

Human behaviour is also influenced to establish a safe information security environment. Despite trained employees having a higher level of security awareness, their behaviour does not vastly differ from untrained users [75]. Thus, it might be fruitful to implement practices that raise knowledge and awareness and change the behaviour of the employees.

Effective awareness, training of employees could be very effective for software engineers to exhibit good cyber security behaviour.

X. CONCLUSION

The main objective of this research was to extract the key factors of cyber hygiene behaviour and find the relationship between the factors (positive and negative relationship) for software engineers. For this purpose, a Systematic Literature Review (SLR) was conducted. The current SLR study was composed of empirical analyses of cyber hygiene behaviour published in the past ten years. A total of 35 studies were analyzed that were consistent with the well-defined inclusion, exclusion, and quality assessment criteria. Most of the included studies were conducted in 2010, 2014, and 2020, as shown in figure 12. From the findings of SLR, this research provides advantages by providing factors of cyber hygiene for software engineers; a total of 19 factors were identified and categorized in this research. The classification of factors using a conceptual map gives an image of positive and negative factors. This research could signal the organization to take a practical approach to improve cyber hygiene practices systematically. It is believed that this study can help to educate the software engineers and to understand the relationship between factors and cyber hygiene, which assist them in developing and maintaining an effective security system so that they protect themselves and behave more securely.

KEY TAKEAWAYS

- From this study, authors find out that practicing cyber hygiene will provide a better protection, better security, monitoring, and maintenance of the networks of software development organizations.
- The key point of this study is to raise the knowledge and awareness of cyber hygiene among software engineers through employee training programs. With

the help of such training, efficient & practical measures are defined to combat the effect of cyber-attacks like (Phishing, Viruses, Worms, Trojan horse, Malware attacks, BYOD, Ransomware attacks, Rootkits).

CONTRIBUTION

- The main contribution of this study is that the authors have done a Systematic Literature Review (SLR) of cyber hygiene behaviour among software engineers for the last ten years (2010-2020).
- This research has made a significant contribution by identifying and providing a comprehensive overview of cyber hygiene factors associated with software engineers.
- This research also contributes to identifying the factors of cyber hygiene and their relationship (i.e., positive, and negative); software engineers can maintain proper cyber-hygiene practices through these factors and relationships.
- Existing literature does not provide knowledge about cybersecurity behaviour, cyber hygiene practices, and the relationship of identified factors amongst software employees. But this study identified the behavioural gaps of cybersecurity and software engineers who are familiar with the practices of the organization's cyber hygiene policy.

REFERENCES

[1] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/j.jisa.2018.08.002.

[2] F. A. Aloul, "The need for effective information security awareness," *J. Adv. Inf. Technol.*, vol. 3, no. 3, Aug. 2012, doi: 10.4304/jait.3.3.176-183.

[3] L. Anderson and R. Agarwal, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Quart.*, vol. 34, no. 3, pp. 613–643, 2010.

[4] R. M. Long, "Using phishing to test social engineering awareness of financial employees," Tech. Rep., 2013.

[5] M. Pike, "The magazine for the IT professional. The charted institute for IT; British computer society," Tech. Rep., 2011.

[6] S. Seidenberger. (2016). *A New Role for Human Resource Managers: Social Engineering Defense*. [Online]. Available: https://core.ac.uk/download/pdf/78048634.pdf.

[7] S. Talib, N. L. Clarke, and S. M. Furnell, "An analysis of information security awareness within home and work environments," in *Proc. Int. Conf. Availability, Rel. Secur.*, Feb. 2010, pp. 196–203.

[8] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Hum. Behav.*, vol. 69, pp. 437–443, Apr. 2017.

[9] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Comput. Hum. Behav.*, vol. 38, pp. 304–312, Sep. 2014.

[10] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Hum. Behav.*, vol. 48, pp. 51–61, Jul. 2015.

[11] R. J. Torraco, "Writing integrative literature reviews: Guidelines and examples," *Hum. Resource Develop. Rev.*, vol. 4, no. 3, pp. 356–367, Sep. 2005.

[12] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, Jun. 2010.

[13] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour Inf. Technol.*, vol. 33, no. 3, pp. 237–248, Mar. 2014.

[14] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Comput. Hum. Behav.*, vol. 57, pp. 442–451, Apr. 2016.

[15] B. Kitchenham, "Systematic reviews," in *Procedures for Performing Systematic Reviews*, vol. 33. Keele, U.K.: Keele Univ., 2004, pp. 1–26.

[16] B. Kitchenham, R. Pretorius, D. Budgen, O. Pearl Brereton, M. Turner, M. Niazi, and S. Linkman, "Systematic literature reviews in software engineering—A tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, 2010.

[17] G. Laws, M. Nowatkowski, J. Heslen, and S. Vericella, *Guidelines for Cyber Hygiene in Online Education*. 2018, pp. 93–100.

[18] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, and G. M. Hancock, "Holistic cyber hygiene education: Accounting for the human factors," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101731.

[19] K. Kirkpatrick, "Cyber policies on the rise," *Commun. ACM*, vol. 58, no. 10, pp. 21–23, Sep. 2015.

[20] J. P. Farwell and R. Rohozinski, "The new reality of cyber war," *Survival*, vol. 54, no. 4, pp. 107–120, Sep. 2012.

[21] R. Dodge, C. Toregas, L. Hoffman, and D. Burley, "Cybersecurity workforce development directions," in *Proc. HAISA*, 2012, pp. 1–12.

[22] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep., 2004.

[23] F. B. Shaikh, M. Rehman, and A. Amin, "Cyberbullying: A systematic literature review to identify the factors impelling university students towards cyberbullying," *IEEE Access*, vol. 8, pp. 148031–148051, 2020.

[24] G. A. Grimes, M. G. Hough, E. Mazur, and M. L. Signorella, "Older Adults' knowledge of Internet hazards," *Educ. Gerontol.*, vol. 36, no. 3, pp. 173–192, Feb. 2010.

[25] M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual differences in cyber security behaviors: An examination of who is sharing passwords," *Cyberpsychol., Behav., Social Netw.*, vol. 18, no. 1, pp. 3–7, Jan. 2015.

[26] T. McGill and N. Thompson, "Old risks, new challenges: Exploring differences in security between home computer and mobile device use," *Behav. Inf. Technol.*, vol. 36, no. 11, pp. 1111–1124, Nov. 2017.

[27] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018.

[28] S. Dzazali, "Social factors influencing the information security maturity of Malaysian public service organisation: An empirical analysis," 2006.

[29] D.-L. Huang, P.-L.-P. Rau, and G. Salvendy, "Perception of information security," *Behav. Inf. Technol.*, vol. 29, no. 3, pp. 221–232, May 2010.

[30] J. P. Simpson Deb and K. Uddin, "Empirical analysis of socio-cognitive factors affecting security behaviours and practices of smartphone users," Tech. Rep., 2016.

[31] B. P. F. M. Van Horenbeeck, J. Kulesza, A. Paziuk, and A. Pisanty, *Cybersecurity Culture, Norms and Values*. IGF, 2018.

[32] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[33] A. AlDairi and L. Tawalbeh, "Cyber security attacks on smart cities and associated mobile technologies," *Procedia Comput. Sci.*, vol. 109, pp. 1086–1091, Jan. 2017.

[34] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *J. Organizational Comput. Electron. Commerce*, vol. 28, no. 3, pp. 269–282, Jul. 2018.

[35] J. E. Thomas, "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks," *Int. J. Bus. Manage.*, vol. 13, no. 6, p. 1, Apr. 2018.

[36] E. Derouet, "Fighting phishing and securing data with email authentication," *Comput. Fraud Secur.*, vol. 2016, no. 10, pp. 5–8, Oct. 2016.

[37] S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," *J. Assoc. Inf. Syst.*, vol. 18, no. 1, pp. 22–44, Jan. 2017.

[38] M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *J. Manage. Inf. Syst.*, vol. 34, no. 2, pp. 597–626, Apr. 2017.

[39] J. Greenwald. (2016). *Employers Face Growing Risk in Tax Season*. [Online]. Available: http://www.businessinsurance.com

[40] P. Ramesh, D. L. Bhaskari, and C. H. Satyanarayana, "A comprehensive analysis of spoofing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 1, no. 6, pp. 157–162, 2010.

[41] A. Herzberg and A. Jbara, "Security and identification indicators for browsers against spoofing and phishing attacks," *ACM Trans. Internet Technol.*, vol. 8, no. 4, pp. 1–36, Sep. 2008.

[42] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, "Cyber security threats detection in Internet of Things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[43] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: A systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[44] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, vol. 98, Nov. 2020, Art. no. 102003.

[45] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manage.*, vol. 45, pp. 13–24, Apr. 2019.

[46] A. Vishwanath, L. S. Neo, P. Goh, S. Lee, M. Khader, G. Ong, and J. Chin, "Cyber hygiene: The concept, its measure, and its initial tests," *Decis. Support Syst.*, vol. 128, Jan. 2020, Art. no. 113160.

[47] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, Jul. 2017, Art. no. e00346.

[48] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors related to cyber security behavior," *IEEE Access*, vol. 8, pp. 125140–125148, 2020.

[49] S. Kumar, B. Biswas, M. S. Bhatia, and M. Dora, "Antecedents for enhanced level of cyber-security in organisations," *J. Enterprise Inf. Manage.*, Oct. 2020.

[50] M. Malatji, S. Von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 233–272, Jun. 2019.

[51] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" 2019, *arXiv:1901.02672*. [Online]. Available: http://arxiv.org/abs/1901.02672

[52] H. Al-Mohannadi, I. Awan, J. Al Hamar, Y. Al Hamar, M. Shah, and A. Musa, "Understanding awareness of cyber security threat among IT employees," in *Proc. 6th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2018.

[53] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014.

[54] E. M. Falkner and M. R. W. Hiebl, "Risk management in SMEs: A systematic review of available evidence," *J. Risk Finance*, vol. 16, no. 2, pp. 122–144, Mar. 2015.

[55] M. Bada and J. R. C. Nurse, "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 393–410, Jul. 2019.

[56] E. J. Williams, A. Beardmore, and A. N. Joinson, "Individual differences in susceptibility to online influence: A theoretical review," *Comput. Hum. Behav.*, vol. 72, pp. 412–421, Jul. 2017.

[57] R. Ramirez and N. Choucri, "Improving interdisciplinary communication with standardized cyber security terminology: A literature review," *IEEE Access*, vol. 4, pp. 2216–2243, 2016.

[58] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review," *Manage. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, Nov. 2014.

[59] J. M. Such, P. Ciholas, A. Rashid, J. Vidler, and T. Seabrook, "Basic cyber hygiene: Does it work?" *Computer*, vol. 52, no. 4, pp. 21–31, Apr. 2019.

[60] Y. Raban and A. Hauptman, "Foresight of cyber security threat drivers and affecting technologies," *foresight*, vol. 20, no. 4, pp. 353–363, Oct. 2018.

[61] I. Atoum, A. Otoom, and A. Abu Ali, "A holistic cyber security implementation framework," *Inf. Manage. Comput. Secur.*, vol. 22, no. 3, pp. 251–264, Jul. 2014.

[62] N. Akdemir and C. J. Lawless, "Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach," *Internet Res.*, vol. 30, no. 6, pp. 1665–1687, Jun. 2020.

[63] M. Alohali, N. Clarke, F. Li, and S. Furnell, "Identifying and predicting the factors affecting end-users' risk-taking behavior," *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 306–326, Jul. 2018.

[64] U. D. Ani, H. He, and A. Tiwari, "Human factor security: Evaluating the cybersecurity capacity of the industrial workforce," *J. Syst. Inf. Technol.*, vol. 21, no. 1, pp. 2–35, Mar. 2019.

[65] A. Nieto and R. Rios, "Cybersecurity profiles based on human-centric IoT devices," *Human-centric Comput. Inf. Sci.*, vol. 9, no. 1, Dec. 2019.

[66] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.

[67] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[68] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst. Hum.*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[69] J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "Systematic approach to cyber resilience operationalization in SMEs," *IEEE Access*, vol. 8, pp. 174200–174221, 2020.

[70] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, p. 8, Dec. 2020.

[71] B.-H. Kim, K.-C. Kim, S.-E. Hong, and S.-Y. Oh, "Development of cyber information security education and training system," *Multimedia Tools Appl.*, vol. 76, no. 4, pp. 6051–6064, Feb. 2017.

[72] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, and T. Baker, "Security threats to critical infrastructure: The human factor," *J. Supercomput.*, vol. 74, no. 10, pp. 4986–5002, Oct. 2018.

[73] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, Apr. 2016.

[74] M. Kajzer, J. D'Arcy, C. R. Crowell, A. Striegel, and D. Van Bruggen, "An exploratory investigation of message-person congruence in information security awareness campaigns," *Comput. Secur.*, vol. 43, pp. 64–76, Jun. 2014.

[75] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018.

[76] PurpleSec. (Mar. 24, 2021). *Cyber Security Statistics Trends & Data*. Accessed: May 30, 2021. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/

[77] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 12, Dec. 2017, Art. no. 155014771774146.

[78] J. M. Ehrenfeld, "WannaCry, cybersecurity and health information technology: A time to act," *J. Med. Syst.*, vol. 41, no. 7, p. 104, Jul. 2017.

[79] N. A. Hassan, "Ransomware overview," in *Ransomware Revealed*. 2019, pp. 3–28.

[80] M. A. Rader and S. S. M. Rahman, "Phishing techniques and mitigating the associated security risks," *Int. J. Netw. Secur. Appl.*, vol. 5, no. 4, pp. 23–41, Jul. 2013.

[81] A. Aparajita, S. Swagatika, and D. Singh, "Comparative analysis of clustering techniques in cloud for effective load balancing," *Int. J. Eng. Technol.*, vol. 7, no. 3.4, p. 47, Jun. 2018.

[82] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, Nov. 2009.

[83] B. Hanus and Y. A. Wu, "Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective," *Inf. Syst. Manage.*, vol. 33, no. 1, pp. 2–16, 2015.

[84] A. Boiko, V. Shendryk, and O. Boiko, "Information systems for supply chain management: Uncertainties, risks and cyber security," *Procedia Comput. Sci.*, vol. 149, pp. 65–70, Jan. 2019.

[85] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019.

[86] D. Singh, N. P. Mohanty, S. Swagatika, and S. Kumar, "Cyber-hygiene: The key concept for cyber security in cyberspace," *Test Eng. Manage.*, vol. 83, pp. 8145–8152, May 2020.

[87] N. Amrin, "The impact of cyber security on SMEs," M.S. thesis, Univ. Twente, Enschede, The Netherlands, 2014.

[88] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014.

[89] R. Anwar, M. Rehman, K. S. Wang, and M. A. Hashmani, "Systematic literature review of knowledge sharing barriers and facilitators in global software development organizations using concept maps," *IEEE Access*, vol. 7, pp. 24231–24247, 2019.

[90] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, 2010.