JOIV : Int. J. Inform. Visualization, 9(1) - January 2025 137-145

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

A Comprehensive Review of Cyber Hygiene Practices in the Workplace for Enhanced Digital Security

Sheeba Armoogum [a], Vinaye Armoogum [b], Anurag Chandra [c], Deshinta Arrova Dewi [d,*], Tri Basuki Kurniawan [e], Soodeshna Bappoo [a], Mohd Zaki Mohd Salikon [f], Alde Alanda [g]

[a] *University of Mauritius, Reduit 80837, Mauritius*
[b] *University of Technology, Mauritius, Port Louis, Mauritius*
[c] *Defense & Aviation, New Delhi, India*
[d] *Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia*
[e] *Postgraduate Program, Universitas Bina Darma, Palembang, Indonesia*
[f] *Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor, Malaysia*
[g] *Department of Information Technology, Politeknik Negeri Padang, Padang, Indonesia*

Corresponding author: [*]deshinta.ad@newinti.edu.my

Abstract*—In today's digital age, cybercrime is increasing at an alarming rate, and it has become more critical than ever for organizations to prioritize adopting best practices in cyber hygiene to safeguard their personnel and resources from cyberattacks. As personal hygiene keeps one clean and healthy, cyber hygiene combines behaviors to enhance data privacy. This paper aims to explore the common cyber-attacks currently faced by organizations and how the different practices associated with good cyber hygiene can be used to mitigate those attacks. This paper also emphasizes the need for organizations to adopt good cyber hygiene techniques and, therefore, provides the top 10 effective cyber hygiene measures for organizations seeking to enhance their cybersecurity posture. To better evaluate the cyber hygiene techniques, a systematic literature approach was used, assessing the different models of cyber hygiene, thus distinguishing between good and bad cyber hygiene techniques and what are the cyber-attacks associated with bad cyber hygiene that can eventually affect any organization. Based on the case study and surveys done by the researchers, it has been deduced that good cyber hygiene techniques bring positive behavior among employees, thus contributing to a more secure organization. More importantly, it is the responsibility of both the organization and the employees to practice good cyber hygiene techniques. Suppose organizations fail to enforce good cyber hygiene techniques, such as a lack of security awareness programs. In that case, employees may have the misconception that it is not their responsibility to contribute to their security and that of the organization, which consequently opens doors to various cyber-attacks. There have not been many research papers on cyber hygiene, particularly when it comes to its application in the workplace, which is a fundamental aspect of our everyday life. This paper focuses on the cyber hygiene techniques that any small to larger organization should consider. It also highlights the existing challenges associated with the implementation of good cyber hygiene techniques and offers potential solutions to address them.

***Keywords*— Cyber hygiene; cyber-attacks; cybersecurity in the workplace; process innovation.**

Manuscript received 2 Feb. 2023; revised 8 Aug. 2024; accepted 22 Nov. 2024. Date of publication 31 Jan. 2025.

I. INTRODUCTION

In this digital era, data has become very valuable and at the same time, very vulnerable. The digital age has revolutionized business operations where the internet plays a crucial role in every aspect of our daily life. However, this advancement has also increased the risk of cyber-attacks and data breaches, putting individuals, business leaders, students, and small to bigger organizations at risk. It is estimated that the world economy lost $945 billion because of inadequate cyber security in 2020 [1] and according to the United Nations estimate, cybercrime has risen sharply since the COVID-19 pandemic with a reported 600% increase in malicious emails [2]. Phishing emails, brute force attacks, DDOS, malware, and other cyber threats will continue to evolve and will become more sophisticated. Hence organizations must employ strong cyber security measures to protect against these attacks. Recent studies underscore the importance of proactive cyber hygiene practices in mitigating such risks. For instance, a comprehensive review emphasizes the role of

vulnerability management systems (VMS) in identifying and addressing security flaws within organizational IT ecosystems. These systems leverage automated processes to detect vulnerabilities, assess their impact, and recommend timely interventions, thereby enhancing digital resilience [3]. Therefore, adopting strong cyber hygiene measures is not just essential but imperative for safeguarding digital assets in this increasingly interconnected world.

Cyber hygiene is a concept that is usually underestimated when it comes to implementing and maintaining security [4]. Personal hygiene keeps one clean and healthy, similarly, cyber hygiene is a combination of behaviors to enhance data privacy, prevent data loss, and protect from various cyber threats. Cyber hygiene is not a one-off measure that is established once by organizations but is a set of routines and repetitions to make good practice stay. It takes a more proactive approach and consistent measures when it comes to cyber security. This is particularly crucial in the healthcare sector, where [5] highlights the urgent threat of cyber-attacks, especially in the context of the COVID-19 pandemic.

COVID-19 has triggered a drastic change in the workplace and working from home has become increasingly typical for many employees. Technology was the fundamental enabler for this transition, but security has not always been a top focus in that environment [6]. Karayel et al [7] emphasizes the importance of companies increasing their cybersecurity investments as remote work becomes more prevalent, considering both corporate-level factors and employees' information and computer security behaviors. Ideally, employees having good cyber hygiene will recognize the need to have updated software, a strong password policy and will make good use of the internet. On the other hand, employees with poor cyber hygiene lack knowledge and training about the fundamentals of cyber hygiene. They may engage in sharing passwords or sharing organizations' confidential data on public platforms. In that situation, organizations are more susceptible to cyber threats that can lead to business damage or even closure [2].

It is challenging to protect data and regrettably, many organizations may believe that security-related rules are sufficient and no further safety exercises need to be carried out [4]. Protecting organizational data remains a challenging task, and unfortunately, many organizations mistakenly believe that merely implementing security-related policies is sufficient, neglecting the need for proactive safety exercises [8]. There are measures already established by the organization, but these measures sometimes have an excessively positive or negative strong effect on employees. For example, certain phishing awareness training can raise many doubts and lead to employees not opening any e-mail attachments, including legit ones [9]. Nonetheless, some employees may believe that it is the organization's sole responsibility to ensure a secure environment while it is the responsibility of both the employees and the management of an organization to ensure good cyber hygiene is always in place. The management shall implement the necessary measures to ensure that everyone is contributing to the safety of the organization and employees need to be aware of the different threats and how to react to those threats.

This paper's main goal is to outline the top cyber hygiene techniques that businesses should follow to prevent various cyber-attacks. It emphasizes the techniques that both the employees and the management of an organization shall adopt when ensuring the security and privacy of any entity. The paper is organized as follows: Section I reviews existing cyber hygiene models and how human behavior, Covid-19, and cyber-attacks relate to cyber hygiene. Section II describes the research methodology. Section III describes the common cyber-attacks in the workplace, proposes the best recommended cyber hygiene practices to fight against those cyber-attacks and elaborates on the challenges in maintaining good cyber hygiene and section IV concludes the paper.

A. Literature Review

Cyber hygiene is a fundamental term referring to a set of best practices and procedures in cybersecurity that are utilized by both end-users and security personnel to ensure the health and security of an organization's digital infrastructure [10]. It involves proactive measures like regular software updates, robust password practices, and incident response planning to minimize vulnerabilities [11]. It also helps to promote behavioral changes in humans, thus achieving a more secure connected environment [12]. These practices are crucial, especially in sectors like healthcare, where human errors significantly contribute to cyber risks. The adoption of human-centric approaches and education tailored to user behavior has been highlighted as essential for improving cybersecurity outcomes and addressing the surge in cyber threats in digitally dependent industries [11].

In this section, 3 different assessment models of cyber hygiene are systematically evaluated on different levels. The different techniques of good and bad cyber hygiene are elaborated based on Infrastructure and Human factors. The last part of the literature review highlights the different cyber-attacks that can occur because of poor cyber hygiene.

1) Holistic Cyber Security Maturity Model

To comprehend the various techniques of cyber hygiene, it is necessary to be familiar with the potential cyber threats that an organization may face. Few companies possess security departments that can effectively cultivate a cybersecurity culture that encourages positive behavior among their personnel [13]. The Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) [14] evaluates the maturity of 15 specified domains to assess the effectiveness of cyber security practices. The 15 requirements are categorized into three groups: (1) Identify (2) Protect and Detect, and (3) Respond and Recover, as depicted in Fig. 1.

Fig. 1 Holistic cybersecurity maturity model assessment model [14]].

The HCYMAF is a comprehensive and adaptable tool that enables higher education institutions to evaluate their own cybersecurity maturity through self-assessment [15]. Based on the study carried out by Butler [15], this tool supports an organization's ability to review and assess its current measures to understand the overarching cybersecurity standards.

2) Cyber Hygiene Maturity Model

There are other Assessment models to improve cyber hygiene best practices, among which there is Cyber Hygiene Maturity Model (CHMM). This framework has been proposed by Skarga-Bandurova et al. [16], in a study named "Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios". The authors came up with this model after analyzing the state of the art in the best practices of cyber hygiene in the energy domain.

CHMM puts forward a systematic approach to cyber practices to help companies integrate the best practices in Smart Grid cyber security and cyber hygiene. The specified framework consists of 5 different levels to help end users in quantitatively assessing their position regarding cyber hygiene posture [16]. The 5 different levels vary from level 1, comprising basic cyber hygiene and progressing gradually to level 5, having a proactive approach to cyber hygiene. Each level takes into consideration 3 different domains: (1) Infrastructure, (2) Organization and (3) People. Table 1 summarizes the Cyber Hygiene Maturity Model in the 3 different domains.

TABLE I
SUMMARIZES THE CYBER HYGIENE MATURITY MODEL

Level 1	Level 2	Level 3	Level 4		Level 5
Infrastructure	Basic cyber hygiene	Intermediate cyber hygiene + level 1	Good cyber hygiene	Substantial cybersecurity	Evolve continuously to meet cyber security threats
			Effective security requirement + level 2	Proactive cybersecurity + level 3	Repel advanced + level 4
Organization	No process maturity	Establish policies, procedures and plans	AT programs are renewed actively	Cyber hygiene for different departments	A document approach for the AT is optimized across organization
		Awareness and Training (AT)	AT programs are updated annually + level 2	Customized AT programs for different departments + level3	Identify activities and share improvements + level 4
		Periodical security awareness training	Demonstrate awareness of security risks by end users + level 2	Include practical exercises	Security Awareness metrics across different departments + level 4
				Use of RI tool + level 3	
People	Security risks awareness by end users	Document practices to implement AT	Resource plan for the AT (social engineering, phishing)	Review and measure AT for effectiveness	AT annually updated

3) Cyber Hygiene Conceptual Model

With the rise in cyber-attacks where society is now more exposed to security risks, Li et al. [17] focused on the conceptual domains of employees' security behaviors. The authors proposed and tested the conceptual model in Fig. 2 to enhance information security behavior research in the workplace [17]. To this study, the Protection Motivation Theory (PMT) framework was used to determine how employee behavior is affected by the organizational environment through cyber security threats, employee appraisal and beliefs.

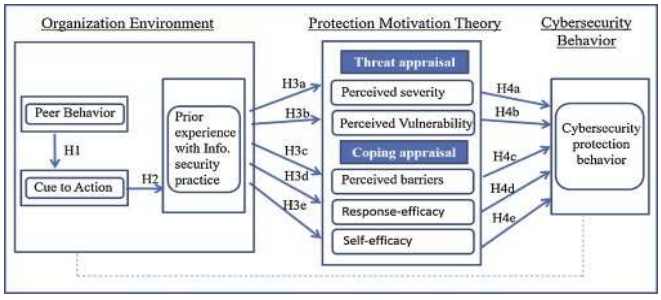

Fig. 2 Conceptual Model [17]

The research methodology used for this research was data collection. Data was gathered from 579 employees from different organizations in the U.S. to test the conceptual model. Through this survey, it was deduced that 53.89% of the employees were not even aware of their company information security policy. In reference to employee behavior in the workplace, another study was carried out by Nigel et al. [18]to access the human factors and individual characteristics that influence cyber hygiene. The authors surveyed 173 university individuals which illustrate multiple factors, such as password management, handling of information and incident reporting are associated with good cyber hygiene [18].

4) Cyber Hygiene and Human Behavior

End users' cyber hygiene has a significant impact on cybersecurity breaches. Cain et al. [10] conducted a study to get a deeper understanding of user behaviors resulting in good and bad cyber hygiene. They provided descriptive findings regarding the level of awareness among end users and the measures they take in relation to cyber hygiene. The research showed that most users failed to perform regular scans, despite their findings showing that 47% to 78% of users have antivirus software. They even compared their research with prior studies and concluded that users are not using the best practices to protect passwords or to protect themselves from phishing scams [10]. Regarding poor cyber hygiene, Theberge et al. [19] conducted a comparative analysis

involving anti-smoking, climate change and cyber hygiene awareness and concluded that the widespread use of the internet, smoking and industrialization have led to a significant decline in cyber hygiene, personal hygiene and the planet wellbeing, respectively [19]. This conclusion is very accurate and relevant to the way organizations need to be motivated to protect themselves from cyber threats. Smoking and climate change awareness campaigns proved to be helpful for companies to enhance their awareness concerning the latter. Similarly, companies need to be encouraged to effectively safeguard their employees and assets through proper cyber hygiene mechanisms.

In a study on "Extracting key factors of cyber hygiene behavior among software engineers", Kalhoro et al. [4] conducted a systematic literature review to empirically analyze the behavior of software engineers concerning cyber hygiene. The authors identified the elements that motivated software engineers to practice cyber hygiene and examined the positive and negative aspects associated with those factors. They classified the identified factors into five categories: Personal Factors, Social Factors, Socio-Cognitive Factors, Environmental Factors, and Technological Factors. According to their study, the Technological Factor had the highest negative impact, followed by Social and Environmental Factors. The Technological Factor comprises of IoT devices, communication networks and business privacy which bring up issues like theft, eavesdropping, phishing and spoofing.

5) Cyber Hygiene and COVID-19

The COVID-19 pandemic has brought a wave of cyber-attacks targeting the healthcare industry, universities, and other public and private organizations. Wilner et al. [20] accentuate the various ways by which Canadian healthcare can be targeted, focusing on three empirical studies of healthcare cyberattacks. Time sensitivity has a major impact on healthcare industries as one's health can be in a critical state if quick medical attention is not given. Based on these limitations, patients' safety takes precedence over cybersecurity where for instance, healthcare personnel may be willing to forego good cyber hygiene practices to deliver faster care. In one of the empirical studies (Boston Children's Hospital), improper cyber hygiene resulted in significant financial costs of approximately USD 600,000 due to repairs of damaged equipment and networks due to DDOS attacks [20].

Poor cyber hygiene opens doors to a multitude of cyber-attacks related to hardware, software, and the employees in an organization. Cyber hygiene deteriorated during the pandemic since many were working from home. In February 2021, an independent research company, Censuswide conducted a survey involving 3006 employees who have worked from home [21]. As a result, it was found that poor password hygiene was a big issue, with 54 % of the employees using the same password across multiple platforms and with 22% writing their passwords down to remember them. Surprisingly, 60% of the employees thought it was the sole responsibility of the IT teams to ensure security in their workplace.

6) Cyber Hygiene and Cyber-Attacks

The consequences of poor cyber hygiene are significant, as they can lead to various cyber threats. Kalhoro et al. [4] highlight the various cyber threats that can arise due to inadequate cyber hygiene in their paper titled "Extracting Key Factors of Cyber Hygiene behavior Among Software Engineers: A Systematic Literature Review". These threats include social engineering, phishing, ransomware, DDOS attacks and malware attacks, such as viruses, worms, Rootkit and Trojan horses. The paper highlights how the WannaCry Ransomware Attack could have been mitigated if end-users were aware of good cyber hygiene and had updated their software security. Another study carried out by Singh et al. [22] explored the various ways of maintaining proper cyber hygiene in the world of cyberspace to keep individuals and businesses safe from cyber-attacks. BYOD, crypto-malware, insecure API, Stegware and Whaling are other cyber-attacks that can occur due to poor cyber hygiene. To overcome these issues, both the employees and the management of the organizations must adhere to policies and practices, from recognizing the weakest connections and security escape clauses to applying security at each level of an entity. Security Hardening, Security Patches, Backups and Effective Training are good cyber hygiene techniques that any individual must identify and prioritize [22].

II. Material and Method

This section provides the methodology used to collect information about cyber hygiene models, techniques, and their effectiveness. There have not been many studies published on cyber hygiene over the years, especially on cyber hygiene in the workplace. The systematic literature review (SLR) approach was used to gather information from multiple data sources. The proposed models that the researchers came forward with proved to be beneficial for an organization to maintain good cyber hygiene at different levels. The quantitative research done by the researchers was accessed and summarized for the literature review. Based on their findings, it has been deduced that there are still a major number of individuals who are victims of poor cyber hygiene. This paper aims to clearly present the research questions below:

- What are the most common cyber-attacks faced by organizations?
- What are the best cyber hygiene practices that should be used to mitigate cyber-attacks in an organization?
- How do employees and the organization contribute to cyber hygiene respectively?
- What are the challenges in maintaining cyber hygiene?

III. Results and Discussion

A. Common Cyber-Attacks in the Workplace

Cyber-attacks have become a significant threat to organizations of all sizes, causing financial losses and severe damage to their reputation. This section elaborates on the common cyber-attacks currently faced by organizations.

1) Phishing

Phishing attacks are a prevalent form of cyber-attack that targets individuals or organizations with the intent to steal sensitive information, including login credentials, financial details, or personal data. Phishing attacks in the workplace can be particularly harmful, as they can compromise an entire

organization's security, making it vulnerable to further cyber-attacks.

Phishing attacks involve a perpetrator sending an email that appears to originate from a legitimate source, such as a trusted vendor, client, or colleague. The email will typically contain a link to a fake website, which is made to look like a legitimate one, which prompts the user to enter confidential information, such as login credentials [23]. Alternatively, the message may contain an attachment that, when opened, installs malware on the recipient's device. A successful phishing attack can result in the theft of sensitive information, financial losses, damage to an organization's reputation and regulatory penalties.

2) Malware Attacks

Malware attacks are a common form of cyber-attack that can have devastating consequences for organizations. Malware refers to any software specifically created to cause harm or exploit a computer system, including viruses, worms, Trojan horses, ransomware, and spyware [23]. Malware attacks can compromise an organization's security, steal sensitive information, and cause significant financial losses associated with remediation, such as cleaning infected systems, restoring data backups, and repairing damaged infrastructure.

Malware attacks can take many forms, but most commonly, they involve an attacker sending an email or message containing an infected attachment or link to a malicious website. When the recipient opens the attachment or clicks the link, the malware is downloaded onto their computer or network, allowing the attacker to gain unauthorized access to sensitive information or control over the system.

3) Ransomware Attacks

Ransomware is a form of malicious software that encrypts an organization's data and demands payment in exchange for the decryption key. These attacks usually happen when an employee opens a malicious email attachment or clicks a malicious link. The ransomware then infects the system and begins encrypting files, rendering them unusable. The attackers then demand payment, usually in the form of cryptocurrency, in exchange for the decryption key [24]. In some cases, the attackers threaten to publish sensitive data if the ransom is not paid. Ransomware attacks can be delivered through a variety of channels, including email, social engineering, and drive-by downloads. Social engineering is a common tactic used by attackers, where they use convincing language or tricks to deceive employees into clicking a link or downloading an attachment.

The impact of ransomware attacks can be damaging. The attackers can lock down an organization's critical data, leading to financial losses and reputational damage. In some cases, organizations are forced to pay a ransom to regain access to their data, which can be costly. Even when the ransom is paid, there is no guarantee that the attackers will provide the decryption key, or that the decrypted data will not be corrupted.

4) Distributed Denial of Service (DDOS)

Distributed Denial of Service (DDoS) attacks are a type of cyber-attack that is designed to overload an organization's network or server with traffic, making it inaccessible to legitimate users. DDoS attacks are a growing threat to organizations of all sizes and industries. DDoS attacks in the workplace typically start with an attacker using a botnet [23], which is a network of compromised devices, to flood an organization's network or server with traffic. This causes the network or server to become overwhelmed and unresponsive, denying access to legitimate users. DDoS attacks can target different types of services, including web applications, email servers, and DNS servers.

DDoS attacks can lead to the loss of critical data. When a network or server is inaccessible, an organization may lose revenue, productivity, and customer trust. In some cases, DDoS attacks can be used as a diversion tactic to distract security personnel while attackers launch other types of cyber-attacks, such as data theft or malware attacks.

5) Man in the Middle (MITM)

Man-in-the-middle (MITM) attacks are a type of cyber-attack that allow an attacker to eavesdrop, change, or otherwise manipulate the data being transmitted between two parties by intercepting their connection [25]. MITM attacks involve an attacker intercepting communication between two parties, such as an employee and a server or between two employees. The attacker does this by positioning themselves in the middle of the communication channel, allowing them to intercept, monitor, and manipulate the data being transmitted.

MITM attacks can be launched through a variety of channels, including rogue access points, phishing emails, and social engineering. Attackers can use IP spoofing or DNS hijacking to reroute traffic to their devices, intercepting and manipulating transmitted data. When an attacker intercepts communication between two parties, they can gain access to usernames, passwords, and other confidential information. This information can then be used for identity theft, fraud, or to launch further cyber-attacks.

B. The Top Ten Cyber Hygiene Practices

Cyber hygiene is everyone’s responsibility. In an organization, it is the responsibility of all the employees and the management to practice good cyber hygiene techniques. Most importantly, it must be enforced as part of a routine for it to be effective in the long run. Good cyber hygiene practices will protect individuals, organizations, and businesses from various cyber threats such as phishing, malware, ransomware and other cyber-attacks. They also safeguard sensitive data and prevent it from being stolen, compromised, or misused by cybercriminals.

Good cyber hygiene also helps an organization boost their productivity by helping the employees and the management of the organization to work more efficiently and avoid disruptions caused by cyber-attacks or data breaches. It will also reduce the risk of financial losses that can result from cyber-attacks or online threats. Adopting good cyber hygiene can help the organization build trust and credibility with customers, clients, and other stakeholders by demonstrating that they can take digital security and privacy seriously.

The following ten cyber hygiene are the fundamental techniques that are strictly encouraged by organizations to keep their employees, their business, their reputation, and their assets safe and secure.

1) Backup Data to Prevent Data Loss

One of the pillars of cyber hygiene is data backup. In essence, it refers to creating a copy of data in case the original one is compromised due to human error and external factors. External factors such as theft, power failure and broad-based phishing can cause data loss in an organization [26]. Human errors like opening emails that contain viruses, expired antivirus software or mishandling devices are also frequent challenges that result in data loss. According to statistics [27] in 2022, 40% of data loss incidents are due to hardware failure or another technical issue.

Social engineering and phishing attacks are common sources of viruses and malware infections that can result in data loss. These attacks can be used to encrypt data, which can only be unlocked by paying a ransom. Educating employees on the nature of phishing attacks can reduce the likelihood of them opening suspicious emails or downloading unknown attachments, ultimately helping to prevent these types of cyber-attacks.

Preventing data loss is important for organizations to protect their infrastructure and protect their privacy. Organizations can enforce frequent backups to external hard drives or to the cloud. Companies must also ensure that data is encrypted when backed up. There are also data loss prevention (DLP) features provided by Google and Microsoft to protect from data loss [26].

2) Firewalls to Prevent Access to Unauthorized Users

Employing firewalls is another key habit when maintaining good cyber hygiene. It acts as a first-line defense for network security by prohibiting unauthorized users from accessing the organization's infrastructure and other online sources. They are one proven method for preventing attacks like SQL injections and malicious requests. Organizations must ensure that firewall software is installed on all employees' devices to ensure that hackers cannot access their data. Firewalls must also be deployed on all network infrastructures, and they must be regularly reviewed to control incoming and outgoing traffic effectively.

Next-Gen Firewalls are the most recent and advanced firewalls nowadays. These third-generation firewalls have successfully passed all standard security measures, including header and port/protocol verification. It handles application-level inspection, intrusion prevention, and deep packet inspection and brings intelligence to the outer layer of the firewall [28].

3) Updated Antivirus, Latest Patches, and Automatic Updates

Lack of updated security patches, automated updates, and antivirus software is the cause of many cyber incidents. Most companies provide security patches and anti-virus but unfortunately, they are not always supported and updated accordingly [29]. Security patches are released whenever there are security vulnerabilities in the earlier versions. Security vulnerabilities pose significant risks as they can lead to exploitation across all devices and systems using that software.

An update of software must always be expected in an organization, so it does not disrupt the normal function of their business. The management of the organization must ensure that their employees are using updated applications, web browsers and operating systems. Administrators within the company must ensure automatic updates are activated on every device and that the latest antivirus is well configured. Employees should not have the privilege to disable those features.

4) Encryption

Any data which is left unprotected is at risk. Therefore, protecting data should naturally be one of the prime objectives of an organization. Data encryption protects data by making it unreadable to unauthorized users. It also works as a defense mechanism if there is a breach. An organization must make sure all devices used by the employees are encrypted. This includes laptops, PCs, hard drives, and backups. An encrypted file-sharing solution, such as Microsoft Outlook and Gmail, must be used to prevent data from being compromised during transmission.

The same applies to the network traffic within the organization. Attacks like 'middle way attacks mostly use techniques such as session hijacking to obstruct, block or change communications between devices. As a control measure, the appropriate encryption and decryption techniques must be used when sending and receiving data between end-to-end users [22]. The OWASP Transport Layer Protection Cheat Sheet is a good reference when it comes to securing the transport layer of a network while considering the use of TLS 1.2/1.3 and strong ciphers like GCM [30].

Encryption keys are the main entry point to access data whether symmetric or asymmetric encryption is being used. Organizations must implement and follow good practices to ensure proper management of encryption keys. The correct algorithm and key size are of utmost importance. AES 256, RSA 2048, Curve25519 are some preferred algorithms that organizations should consider. Various cipher modes can be used as an additional layer to protect data. GCM and CCM are the first preference of ciphers when it comes to guaranteeing integrity and authenticity of data. The OWASP Cryptographic Cheat Sheet is a good reference when it comes to encryption of data [31].

5) VPNs for Secure Remote Access

As a result of the pandemic-driven increase in remote work, it has become essential for organizations to provide their employees with VPN access to ensure that they can work remotely in a secure manner. A VPN is a technology that allows for secure remote access to the internet via the organization's network infrastructure. This technology uses encryption to create a private communication tunnel on a public network, ensuring the secure transmission of data between the client and the VPN [32] and leveraging attacks like spoofing and brute force attacks. The encryption prevents unauthorized access to sensitive information, making it more difficult for hackers and cybercriminals to intercept and steal data. VPNs also enable users to browse the internet anonymously by hiding their IP address, which can help to protect their online privacy [33].

6) Security Awareness Training to Prevent Social Engineering Attacks

Educating employees on how they play a major role in mitigating cyber-attacks like phishing, Business Email Compromise, USB Drops, malware and Tailgating help

companies to defend themselves against those attacks. Organizations should define effective and regular security awareness training programs to engage employees in prime cyber security practices. That training must be updated according to the latest attacks targeting organizations and must be reviewed at least quarterly. To render this training even more effective, training can include security awareness quizzes and campaigns.

After security awareness training is done, there should be follow-up by managers to review the feasibility of those training and quiz. If employees have failed those training, further actions like formal training and coaching shall be given to ensure that all employees contribute to the safety of the organization. Furthermore, regular phishing campaigns can be done to see if employees are still in touch with good cyber hygiene. According to the annual report of Proofpoint Inc, a security company [34] 80% of organizations stated that security awareness training has reduced their employees' susceptibility to phishing attacks.

7) Password Hygiene and MFA

There are several ways in which passwords can be compromised. Brute Force Attacks, Phishing Attacks and Credential Surfing are only a few examples. To prevent those attacks, organizations must establish proper password hygiene across all systems in the organization. Password hygiene is the practice of creating and maintaining strong passwords to protect accounts and systems from hackers. Avoiding password reuse, avoiding writing the password down, password policies comprising of a set of characters, long password combinations and automatic password rotation are some examples of good password hygiene. Multi-Factor Authentication adds an extra layer of security to determine the right people or devices who have access to a particular system.

Password hygiene walks together with security awareness training. Employees must be aware of the importance of good password hygiene so they can use those tips within the organization and outside the organization. Along with good password hygiene, employees should also be cautious when entering passwords on a particular website and they should be able to distinguish between secure and insecure websites.

8) Organization Policies

Li et al. [17] tested the conceptual framework in Figure 2 using the survey results from 579 business operators. The findings on the study have shown that employees are better able to manage cyber security tasks when they are aware of the organization's security policies compared to those who are not. Implementing organization policies such as Information Security Policy, Internet Usage Policy, and Devices Policy have a positive impact on employees' cyber security compliance behavior. Yet, just enforcing those policies is not enough. The organization must ensure that employees are aware of those policies and that they are making use of the best practices while following those policies. Organizations can make use of their internal platform or 3rd party platforms where employees can read and acknowledge those policies accordingly. The management of the organization must regularly review organizational policies to make sure their current information security policy reflects the current situation of the company and the different cyber-attacks that are emerging.

9) Audits by Third Parties

Audits such as ISO 27001 and PCI DSS are crucial for cyber hygiene because they provide a framework for assessing an organization's cybersecurity posture. ISO 27001 acts as a global benchmark for managing information security, while ISO 27001 is an international standard for information security management, while PCI DSS is a set of security rules designed to ensure a secure environment for businesses handling credit card information during acceptance, processing, storage, or transfer. Compliance with these audits is essential because they ensure that organizations have the necessary policies and procedures in place to protect their digital assets and sensitive data. In a study carried out by Carla and Eduardo [35], it shows how an enterprise chose to examine and increase the security level of its information and communication system by adhering to the best practices of ISO 27001. The audits require the implementation of specific cybersecurity practices, such as access control, data backup, vulnerability assessments, and regular monitoring, to maintain a secure network environment. In addition, these audits provide a roadmap for the organization to continually improve its cybersecurity posture and identify potential vulnerabilities or areas for improvement.

By adhering to these audits, organizations can not only protect themselves from cyber-attacks but also demonstrate to customers and stakeholders that they take cybersecurity seriously and are committed to maintaining a secure digital environment. Thus, compliance with audits such as ISO 27001 and PCI DSS is an essential aspect of good cyber hygiene practices for any organization that processes, stores, or transmits sensitive data.

10) Incident Response Plan

An Incident Response Plan (IRP) is a set of documents and procedures underlying the actions that should be taken if ever a breach happens. It consists of guidelines, standardized protocols, roles and responsibilities, communication plans, the severity of incidents and more. There should be a dedicated team to frequently respond to simulated data breach situations and access how well and fast they can respond to the attacks which will in turn evaluate the effectiveness of the IRP. According to a survey done by IBM [36], the average breach cost savings at organizations having an IR team who tested their IRP was $2.66 million.

IRP is critical to any organization so as to anticipate and react accordingly to an attack and thus limiting the cost, damage and time it takes to mitigate the damage and minimize the downtime of the attack. A good IRP will reduce the severity of an attack, saving the company time and money, and even saving its reputation in the market.

C. Challenges in Maintaining Cyber Hygiene

Maintaining good cyber hygiene practices is essential for protecting against cyber threats and ensuring digital security and privacy. However, it can be challenging to maintain good cyber hygiene due to a range of factors which are defined in this section.

1) Human Error

Human error is one of the biggest challenges in maintaining good cyber hygiene. Even the most sophisticated security

systems can be compromised if one employee clicks on a malicious link or falls for a phishing scam. Employees can have their devices stolen, which can expose sensitive data to unauthorized parties. To address these challenges, organizations can provide regular cybersecurity training to employees, implement strong password policies, use multi-factor authentication, monitor employee activity, and conduct regular security assessments and audits. Organizations can also implement technical controls, such as firewalls, intrusion detection systems, and antivirus software, to mitigate the impact of human error.

2) Limited Resources

Maintaining good cyber hygiene can require significant resources, including time, budget, workforce, and expertise, which may be challenging for individuals or small businesses with limited resources. These limitations can make it difficult to implement and maintain effective security measures. For example, an organization may not have the financial resources to purchase the latest security technologies or to upgrade its existing systems. This can leave the organization vulnerable to cyber threats, such as malware and phishing attacks, which can compromise its data and systems. Furthermore, limited resources can affect an organization's ability to provide cybersecurity training to its employees. Without adequate training, employees may not be aware of common cyber threats, or they may not know how to follow proper cybersecurity protocols, such as using strong passwords, avoiding phishing emails, and securing their devices.

Overall, limited resources can make it challenging for organizations to maintain good cyber hygiene. However, there are still some measures that can be taken to improve cybersecurity, such as prioritizing security investments, partnering with external security experts, and providing regular training to employees.

3) Evolving Threats

Cyber threats are constantly evolving, and cybercriminals are becoming increasingly sophisticated in their tactics, techniques, and procedures. This means that organizations need to be constantly vigilant and adapt their cybersecurity strategies to keep pace with the changing threat landscape. Cyber criminals are developing advanced malware and new attack methods that can evade detection by anti-virus software and other security technologies.

To address these challenges, organizations need to take a proactive approach to cybersecurity. This includes staying up to date with the latest threats, implementing effective security controls, monitoring systems for suspicious activity, and conducting regular security assessments and audits. Organizations should also invest in cybersecurity training for employees, implement multi-factor authentication, and ensure that all software and systems are up to date with the latest security patches and updates.

4) Balancing Security and Usability

Organizations need to ensure that their security measures are effective in protecting against cyber threats, while at the same time allowing employees to work efficiently and productively. However, security measures can sometimes be cumbersome and difficult to use, which can lead to employees bypassing or disabling them, thereby increasing the risk of cyber threats. Finding the right balance between security and usability, such as implementing security measures, and regular cybersecurity training can be helpful in this situation. Regular security assessments will help in identifying vulnerabilities and areas of improvement. On the other hand, employees will understand the importance of cyber security and their role in protecting the organization.

5) Complexity of Technology

As technology evolves, organizations are adopting new and complex systems, applications, and devices to improve their business processes and stay competitive. While these technologies offer numerous benefits, they can also introduce new vulnerabilities and create challenges for maintaining good cyber hygiene. As systems become more complex, it becomes more difficult to identify vulnerabilities and ensure that they are adequately secured. Configuration and patching of systems and applications become more challenging, resulting in misconfigured systems susceptible to attacks.

To address these challenges, organizations need to implement strong security controls and policies that can manage the complexity of technology. This includes conducting regular security assessments, implementing effective configuration and patch management processes, and investing in technologies that can help manage and secure complex systems. Additionally, organizations should have clear security policies and procedures in place and communicate these to all employees and should provide regular cybersecurity training to employees to help them understand the risks and best practices related to technical complexity.

However, it is essential to act appropriately to protect against cyber threats and maintain good cyber hygiene practices. This requires ongoing awareness, education, and resources to stay ahead of evolving threats and maintain effective security measures. Individuals and organizations must take the necessary steps to protect themselves from digital threats and maintain good cyber hygiene practices to ensure their digital security and privacy.

IV. Conclusion

Cyber hygiene is an essential aspect of supporting a secure workplace in the digital age. With the increasing number of cyber threats and the growing amount of sensitive data stored online, organizations must prioritize the implementation of cyber hygiene best practices to protect their employees, resources, and reputation. This paper underscores the top cyber hygiene practices and the importance of overcoming the challenges of cyber hygiene to mitigate the risks of cyber threats and protect sensitive information and assets. Good cyber hygiene habits in the workplace include security patches, strong passwords, and awareness of common cybersecurity threats, among others. The effective implementation of these measures requires a combination of technical and non-technical approaches, including employee training and regular software updates. By practicing good cyber hygiene in the workplace, organizations can reduce the risk of data breaches, financial losses, and reputational damage. Investing in cyber hygiene is an investment in the long-term security and success of any organization. Organizations that prioritize cyber hygiene will be better

prepared to navigate the continually evolving cybersecurity landscape.

REFERENCES

[1] M. H. U. Sharif and M. A. Mohammed, "A literature review of financial losses statistics for cyber security and future trend," *World J. Adv. Res. Rev.*, vol. 15, no. 1, pp. 138–156, 2022.

[2] CyberGhost, "How to Improve Cyber Hygiene & Stop Cyber Attacks." Accessed: Jan. 28, 2023. [Online]. Available: https://www.cyberghostvpn.com/en_US/privacyhub/what-is-cyber-hygiene

[3] K. Bennouk, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, A. Z. Faroukhi, and D. Mahouachi, "A comprehensive review and assessment of cybersecurity vulnerability detection methodologies," *J. Cybersecurity Priv.*, vol. 4, no. 4, pp. 853–908, 2024.

[4] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, "Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 99339–99363, 2021, doi: 10.1109/ACCESS.2021.3097144.

[5] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health," *Int. J. Qual. Heal. Care*, vol. 33, no. 1, Feb. 2021, doi: 10.1093/intqhc/mzaa117.

[6] S. Furnell and J. N. Shah, "Home working and cyber security – an outbreak of unpreparedness?," *Comput. Fraud Secur.*, vol. 2020, no. 8, pp. 6–12, Jan. 2020, doi: 10.1016/S1361-3723(20)30084-1.

[7] T. Karayel, B. Aktaş, and A. Akbıyık, "Human factors in remote work: examining cyber hygiene practices," *Inf. Comput. Secur.*, vol. 33, no. 1, pp. 96–116, Jan. 2025, doi: 10.1108/ICS-11-2023-0215.

[8] M. Johnson and T. Lee, "Data protection strategies in modern organizations," in *International Conference on Cybersecurity and Information Systems (CIS)*, 2023, pp. 88–92.

[9] NIST, "You've Been Phished."

[10] 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.

[11] K. Kioskli, T. Fotis, S. Nifakos, and H. Mouratidis, "The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0," *Appl. Sci.*, vol. 13, no. 6, p. 3410, Mar. 2023, doi: 10.3390/app13063410.

[12] K. Maennel, S. Mäses, and O. Maennel, "Cyber Hygiene: The Big Picture," 2018, pp. 291–305. doi: 10.1007/978-3-030-03638-6_18.

[13] 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, 2019, doi: 10.1016/j.procs.2019.01.108.

[14] A. Aliyu *et al.*, "A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom," *Appl. Sci.*, vol. 10, no. 10, p. 3660, May 2020, doi: 10.3390/app10103660.

[15] S. Butler Lamar, "Managing cyber hygiene at a higher education institution in the united states," 2022.

[16] I. Skarga-Bandurova, I. Kotsiuba, and E. R. Velasco, "Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios," *Front. Comput. Sci.*, vol. 3, p. 614337, 2021.

[17] 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, doi: 10.1016/j.ijinfomgt.2018.10.017.

[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, p. 101731, May 2020, doi: 10.1016/j.cose.2020.101731.

[19] J. Thebarge, M. Reith, and W. Henry, "Increasing industry profitability and cyber hygiene utilizing awareness progression methods," in *International Conference on Cyber Warfare and Security*, Academic Conferences International Limited, 2022, pp. 325–332.

[20] A. S. Wilner, H. Luce, E. Ouellet, O. Williams, and N. Costa, "From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector," *Int. J. Canada's J. Glob. Policy Anal.*, vol. 76, no. 4, pp. 522–543, Dec. 2021, doi: 10.1177/00207020211067946.

[21] R. Manning, "Yubico Research Reveals Lackluster Cybersecurity in Europe," Yubico. [Online]. Available: https://www.yubico.com/blog/yubico-research-reveals-lackluster-cybersecurity-in-europe/

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

[23] S. Anawar, D. L. Kunasegaran, M. Z. Mas'ud, and N. A. Zakaria, "Analysis of phishing susceptibility in a workplace: a big-five personality perspectives," *J Eng Sci Technol*, vol. 14, no. 5, pp. 2865–2882, 2019.

[24] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100013, Nov. 2021, doi: 10.1016/j.jjimei.2021.100013.

[25] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 2, no. 2, pp. 109–134, 2019.

[26] J. R. Brown, "Data Loss: What it is, How it Works, Common Causes," Investopedia. Accessed: Feb. 27, 2023. [Online]. Available: https://www.investopedia.com/terms/d/data-loss.asp

[27] B. Krstic, "15+ Scary Data Loss Statistics to Keep in Mind in 2023," WebTribunal, 2023. Accessed: Feb. 13, 2023. [Online]. Available: https://webtribunal.net/blog/data-loss-statistics/

[28] A. U. Nabi, M. Ahmed, and A. Abro, "An overview of firewall types, technologies, and functionalities," *Int. J. Comput. Relat. Technol.*, vol. 3, no. 1, pp. 10–16, 2022.

[29] A. Maurushat and K. Nguyen, "The legal obligation to provide timely security patching and automatic updates," *Int. Cybersecurity Law Rev.*, vol. 3, no. 2, pp. 437–465, Dec. 2022, doi: 10.1365/s43439-022-00059-6.

[30] OWASP, "Transport Layer Protection – OWASP Cheat Sheet Series." Accessed: Feb. 13, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

[31] OWASP, "Cryptographic Storage – OWASP Cheat Sheet Series." Accessed: Feb. 13, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

[32] Z. Xu and J. Ni, "Research on network security of VPN technology," in *2020 International Conference on Information Science and Education (ICISE-IE)*, IEEE, Dec. 2020, pp. 539–542. doi: 10.1109/ICISE51755.2020.00121.

[33] W. Y. Leong, Y. Z. Leong, and W. S. Leong, "Strengthening Security in Computing," in *2024 IEEE Symposium on Wireless Technology & Applications (ISWTA)*, IEEE, Jul. 2024, pp. 113–116. doi: 10.1109/ISWTA62130.2024.10651781.

[34] STATE OF THE PHISH, "2021 State of the Phish: An In-Depth Look at User Awareness, Vulnerability and Resilience," 2021. [Online]. Available: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2021.pdf

[35] C. Carvalho and E. Marques, "Adapting ISO 27001 to a Public Institution," in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, Jun. 2019, pp. 1–6. doi: 10.23919/CISTI.2019.8760870.

[36] IBM, "Cost of a data breach report 2022," IBM. Accessed: Feb. 15, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach