A Novel Framework to Enhance End-User Security Compliance

Zinnar Ghasem[1], Nathan Clarke[2], Steven Furnell[3]
[1]*The American University of Kurdistan, Duhok Kurdistan Region-Iraq*
[2]*University of Plymouth, United Kingdom*
[3]*University of Nottingham, United Kingdom*

Abstract

Protecting assets within organizations through technological measures continues to remain an ongoing problem in the cyber security domain. There is extensive literature pointing to the "human-element" being a significant factor in security breaches – whether than be intentional or unintentional. Current endeavors to raise the level of information security awareness within individuals have arguably not been effective as required – evidenced by the ongoing breaches caused by people. Indeed, enhancing user's security practice and behavior is a multifaceted problem and remains a challenging issue. The paper first presents the results of a survey whose findings revealed there is a lack of knowledge, and security barriers among a notable portion of respondents. The findings also revealed a discrepancy that while respondents claimed to do and know, do not represent their actual security knowledge and behaviours/practices. The paper then proposes a framework and focuses on enhancing individual user's security compliance in real-time through an intervention-based approach. The proposed framework continuously identifies users' security behaviours in relation to their individual role/job responsibilities and prior training to provide an intelligent, targeted and tailored intervention. The framework comprises various interconnected components and utilizes several sources including active evaluation, monitoring, role/job responsibilities, and manager observations to feed into an assessment of the individual users' needs. Different mechanisms seek to identify the reasons behind their non-compliance; and provide a targeted and tailored series of interventions to maximize the likelihood of improved security behaviours and compliance.

1. Introduction

Enhancing user's security practices through current security awareness programs have arguably not been effective as required. The ineffectiveness of security programs has been widely cited in literature, including Cyber Resilience report [1], [2], [3]. They have been generalized as "one-size fit all" in that they failed to pay adequate attention to consider individual user's security needs in framework design [4].

It has been argued that current security training programs are often boring and ineffective in improving users' security behaviours and compliance, as they have simply focused on raising users/employees' security awareness [2]. Such approaches are important, but they do not necessarily lead to user compliance. This raises an issue for organizations to determine whether those users who undertake training have acquired the necessary security awareness and knowledge, or whether they understand the training but choose not to comply. Therefore, security awareness and training need to be shifted from their current approaches to focus upon an integrated and connected approach that includes both education and compliance in a continuous harmonized lifecycle that is mindful of the individual.

This paper builds upon the existing limitations of current security awareness and related issues with view of continuously monitoring users' security behaviours in real times to identify reasons behind non-compliance and accordingly provide appropriate intervention to enhance security compliance within organizations. The paper is structured as follows: Section 2 explores the current state of art in security awareness and training. Section 3 discusses the survey methodology and then proceeds to discuss key results in section 4 and section 5. The paper then explores the proposed framework and outlines its components and intervention.in section 6. Finally, the tailored requirements are discussed in section 7. The paper concludes in section 8 with a discussion of future work.

2. Current security awareness

The importance of security awareness and training have been well documented. Different prototypes have been proposed to enhance user's understanding of security issues and practice. A summary of recent studies is presented in Table 1.

The need for tailored training has been recognized by many studies, most of which simply call for security awareness to be tailored for a group of users or according to policies and requirements of a specific organization [9], [17]. However, Furnell and Vasilei-

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

Table 1. Summary of Current Security Awareness

Study	Proposed approach	Implementation /evaluation
Korovessis et al. [5]	General security awareness toolkit.	Web-based tool. Focus-group and survey.
Furnell et al. [6]	Software-based tool. Three modes of operations.	Computer based training prototype.
Dominguez et al. [24]	Conceptual Framework	A survey
Haeussin-ger et al. [7]	Conceptual model.	A survey.
Srikwan and Jakobsson [8]	SA-based on malware, spoofing, phishing and password.	Web-based tool. Delivered based on cartoon.
Lötter and Futcher [9]	Email-phishing framework.	Email-client software.
Cone et al. [10]	video game-based security framework.	Game-based-CyberCIEGE-software.
Burke [11]	Game-based Security awareness.	Web-based game. Utilizes media and text.
Asanka and arach-chilage [12]	Phishing awareness prototype.	Phishing mobile-game based URL.
Ghazvini and Shukur [13]	A healthcare sec-urity framework.	Game-based framework.
Herath and Rao [22]	Framework-based on security policy.	Conceptual framework.
Niekerk and Von-Solms [14]	A holistic frame-work to improve security-culture.	Conceptual framework.
Siponen [23]	Conceptual security awareness.	Conceptual framework.
Poepjes and Lane [15]	ISA Capability Mode (ISACM),	Conceptual framework
Mejias [16]	SA-model asses-sing new techno-logical risks.	A survey.
Alotaibi, Furnell and Clarke [17]	Security Policy Compliance Framework	Conceptual framework.
Alotaibi [18]	Security compliance model.	A survey.
Furnell and Vasileiou [4]	A provisional Mo-del for-tailoring SA.	-

ou [4] proposed a desirable provisional tailored training, and Alotaibi, et al. [17] proposed a framework for improving home-users security management and awareness. The study suggested/tried to tailor awareness content for three groups: novice, intermediate and expert users. Although, the study may have tried to avoid using "one-size-fits all" training, it essentially creates a similar issue: One-size-fit a group.

Security awareness/training consists of two interrelated parts: Content and framework. Nevertheless, most current studies have focused only on content, and at their best customized content for an individual organization or a group. Thus, they are inadequate to address users' security compliance, as they have not considered individual user's needs in relation to their role responsibilities. Such approaches are important, but they do not necessarily lead to user compliance, and they have focused on user's intention and self-efficacy to predict user's ability in implementing and utilizing security technology and measures. Nevertheless, what users pretend to do and know is not necessary what they actually do and does not reflect on their level of security knowledge and practice.

Users may overestimate their security knowledge, understanding and ability in the process of implementing security measures. Users may not comply with security for various reasons including malicious behaviours. Furthermore, the current security awareness/training neither helps nor provides any information to support organizations in their process of deciding when and which employee(s) need and should attend a training. Therefore, current security awareness and training arguably needs to shift from their present approach to focus on applications of user's actual security behaviours and compliance and provide organizations with the required information to understand their security status in relation to employee's security needs and compliance.

3. A Survey of End-User Security Behaviours, Knowledge and Practice

While the literature highlighted limitations of current security awareness and programs, lacked to provide detailed insight into the process of addressing these limitations. The survey intents to comprehensively evaluate current security awareness of end-users to understand their knowledge, barriers, attitude/perception, and behaviours. This baseline assessment serves as a critical foundation for devising a more nuanced and effective intervention to improve their security behaviours and compliance, and in turn, to be integrated into a framework. This approach ensures that the resulting interventions are grounded in end-user's responsibilities needs and enhancing the framework ability to provide intervention as required to enhance end-suer security practice and behaviours. The aims of survey are:

- Security barriers that potentially prevent cyber-users from implementing and/or complying with best security practices.

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

- Evaluate current security practices. Users' beliefs toward threats, and risks from cyberspace.
- Users' knowledge and whether what users may claim to do, know or comply with, represent their actual security knowledge.
- To identify and prioritize factors of interest and identify methods that may possibly enhance the process of identifying individual user's needs and level of security practice.

The survey was conducted online (and hosted on https://www.jisc.ac.uk) to maximize the number of participants. It comprised of five sections: background information; use and protection of systems; cyber-security threats; barriers to security; and security knowledge. The background section is concerned with general information about the background of participants including the level of education, country of origin, and level of skills and knowledge of security. Use and protection of systems explores users' current security practices and evaluate their knowledge levels. This helps to gain understanding of cyber-users' security needs. While cyber-threats and related problems section seeks to understand the way respondents feel about risks, threats, and whether they have been victims of cybersecurity. The barriers to security section seeks to understand and identify various potential barriers that may constrain end-users from adopting, implementing, and complying with best security practice. The last section aims to understand users' security knowledge and explores whether what participants claim in self-reported non-knowledge-based questions reflect their actual knowledge and practice. The survey was distributed to a wide range of people including undergraduate students, academic staff and non-academic staff within universities in Kurdistan region/Iraq and U.K. As above-mentioned, the survey was conducted online, and people were invited to participate in the survey through a link within email.

4. Results

A total of 372 participants responded to the questionnaire. The majority of whom (64%) were male. While acknowledging the potential influence on this gender imbalance, it is important to underline that such disparity is not foreseen to adversely impact om the integrity of the survey results. Participants were drawn from various universities and different departments within UK and Kurdistan region/Iraq educational establishments, predominantly falling within 18-44 years – a demographic assumed to be actively engaged as internet user [19].

Considering academic backgrounds of the participants, coupled with their pursuit of study/degrees, it is logical to assume that they are equipped with more robust understating and have a higher level of security related knowledge and awareness than general population. This suggests the results of the survey are likely to be more positive, reflecting a high-level of security related knowledge among participants, which might vary from the overall trends observed in the general population.

4.1. Background

One of the key questions in the survey was to explore how respondents rate their security knowledge and skills in protecting their devices (computer, mobile, or tablet). A good portion (87%) of respondents rated their level of knowledge/skills as an average and above to protect their devices, as illustrated in Figure.1.

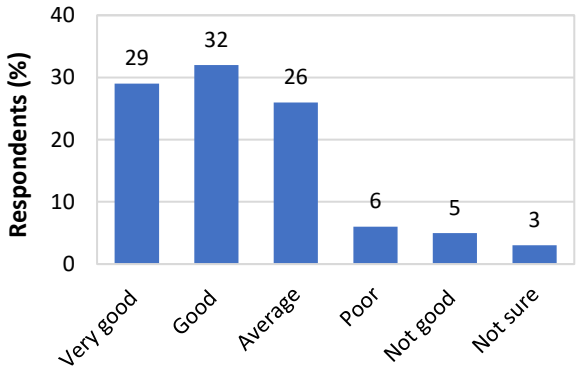

Figure.1. Respondents' claimed level of security knowledge and skills

The results show that majority of participants are confident and able to protect their devices. This indicates that the respondents are well educated and knowledgeable about information security.

4.2. Use and protection of systems

Understanding how respondents perceive the security measures for their device, their adherence to good security practices and their use of safeguards is essential. Respondents were asked to indicate the extent to which their devices are protected against malware. The result in Figure. 2, reveals that most respondents believe their devices are protected from malware. However, a notable portion of participants lack awareness about the security of their devices.

Most participants claimed their devices are protected, many of them do not follow recommended security practices. Opining links and email attachments from unknown sources is generally considered poor security practices and could potentially result in device being infected with malware. Nevertheless, more than half of participants

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

open email attachments and (46%) acknowledge occasionally or frequently following links within messages from unknown sources, as illustrated in Figure.3.

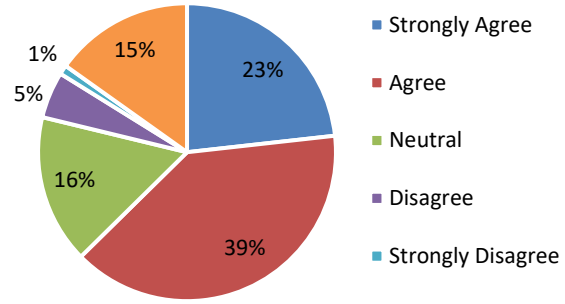

Figure 2. Respondents' perception of their devices being protected from malware.

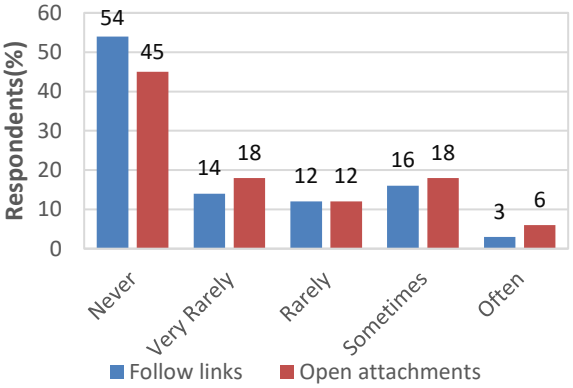

Figure 3. Following *links and* open email attachments from unknown sources

Respondents' confidence in the protection of their devices may have contributed to their risky behaviours. The lack of security awareness and knowledge could also be contributed factors. Participants may be unaware of various methods/techniques through which their devices can be infected with malware and may not fully understand the potential threats and risks associated with opening email attachments and following the links within messages from unknown sources. These assumptions highlight the need to provide end-users with tailored help/guidance, ensuring not only awareness of potential cyber-attacks but also understanding of vector/domain through which such cyber-attacks can take place.

To further understand how respondents protect their devices and data, they were asked several questions in relation to passwords, data backup and data protection. The results show significant portion of respondents comply with best security practice as illustrated in Figure 4.

While the findings suggest participants are aware of the importance of data protection and have knowledge about safeguarding their data from unauthorized access, the effectiveness of their protective practices relies on their understanding of data protection principles, and the methods they employ. Nevertheless, there is a possibility that some participants may lack a comprehensive understanding of entire data protection process. For example, they might mistakenly believe that saving data on a password-protected computer ensures the security of their files/data. This simplified belief, may not provide robust protection against various potential threats. It is important to emphasize that a comprehensive and nuanced approach to data protection is crucial to mitigate risks/threats and ensure an overall security of sensitive data.

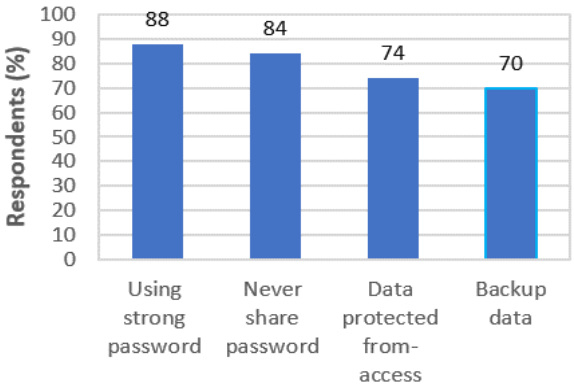

Figure 4. Percentage of respondents in relation good security practices

Moreover, participants' confidence in employing robust and strong password depends on their understanding and interpretation of what constitute a strong password. If a user believes their password is strong, it may not necessarily align with recommended security practices, potentially leading to a false sense of security. This misperception constitutes a significant security issue for many users. Additionally, even though a good portion of participants avoid sharing their password, the risk to privacy remains and depends on the methods employed to keep the password confidential.

The respondents were further assessed regarding their adherence to security practices, specifically in terms of applying security updates/patches and enabling the firewall in their computer or home network. The responses varied for both inquiries. While just under two-third of respondents apply security update/patches, half of them neglected an important security measure by not enabling the firewall on their computer or home network. as illustrated in Figure 5.

The results highlight a noticeable lack of knowledge and understanding among many respondents regarding the importance of updating

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

software and activating the firewall. This may be due to many factors, such as limited awareness of the benefits associated with these practices or lack of understanding of potential threats resulting from neglecting such security measures. Therefore, it is crucial for users to understand the benefits and the consequences of implementing or neglecting these security measures.

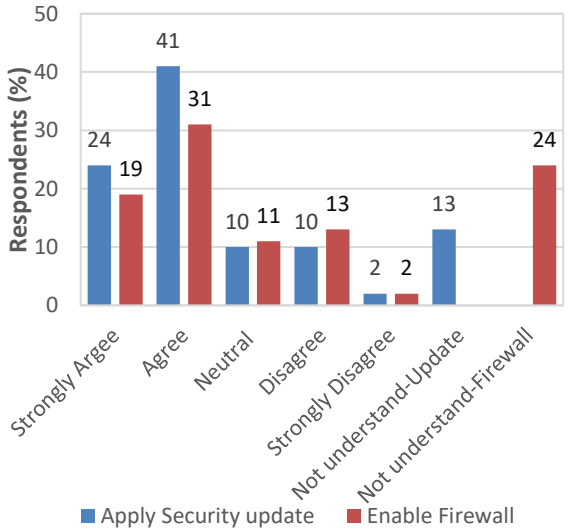

Figure 5. Apply security update and enable firewall

However, one possible reason why respondents are more inclined to apply security updates/patches than enabling firewall on their computer/mobile could be attributed to the frequent reminders provided by security software/operating systems. These reminders might have contributed to users' familiarity with a concept of security updates rather than that of a firewall.

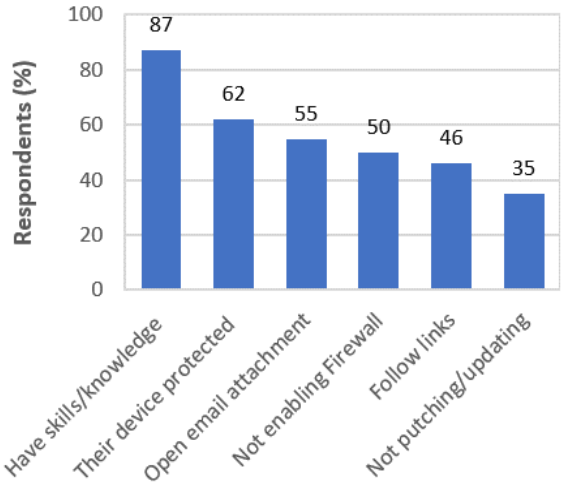

Figure 5. Respondents with high skills/knowledge, but poor security practice

Given the effectiveness of reminder notifications for software updates, the framework may benefit from incorporating a similar reminder mechanism. This approach aims not only to reinforce end-suer security awareness but also to continuously monitor their security behaviours, ensuring continuous compliance. However, despite the majority of respondents believing they have required security knowledge and skills, and asserting the protection of their devices, there exists a discrepancy, as shown in Figure.6, where they do not consistently adhere to basic recommended security practices for various reasons.

The findings in Figrue.6 suggest that having security knowledge and skills or having received training does not automatically guarantee in security compliance for end-users. Ensuring adherence to security policies, it is vital to continuously monitor their behaviours and provide the necessary help and guidance when needed.

4.3. Cyber threats

Respondents' perception toward cyber threats, specifically online-fraud, malware, and social engineering (SE) including phishing were explored, as illustrated in Figure.7.

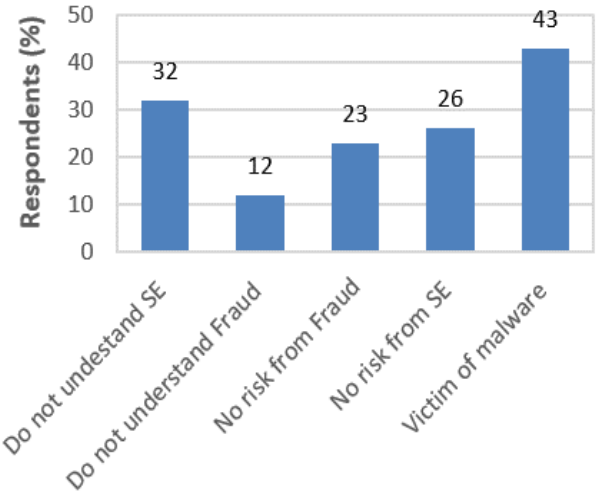

Figure 6. Users' perception toward malware, se, and fraud

It is not surprising to observe that nearly half of respondents falling victim to malware. However, the actual number of victims could potentially be higher, considering that respondents may be unaware of their devices being infected with malware. This is emphasized by findings that 58% of respondents lack understanding or perception of risks associated with social engineering such as phishing. Furthermore, one-third of respondents demonstrate a lack of understanding or perception of risks related to online activities. This observed trend may be due to end-

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

user's limited knowledge, awareness, and understanding of threats and their potential consequences.

Not perceiving threats/risks could arguably form a basis for insecure environments, potentially exposing individuals or an organization to various security risks. Therefore, continuous enhancements and reinforcement of end-users' awareness and knowledge should involve continuous monitoring of their behaviours and implementation of tailored interventions, ensuring both improvement and compliance.

4.4. Security barriers

Obviously, end-users' security practices can be influenced by various factors, some of which may constrain their ability to implement required security measures. The questionnaire aimed to understand these factors by exploring respondents' perception regarding the importance of cyber security, their responsibility for securing devices, their capability in securing their devices, understanding of security controls, recognition of the need for security updates and awareness of potential threats may face. The results are illustrated in Figure.8.

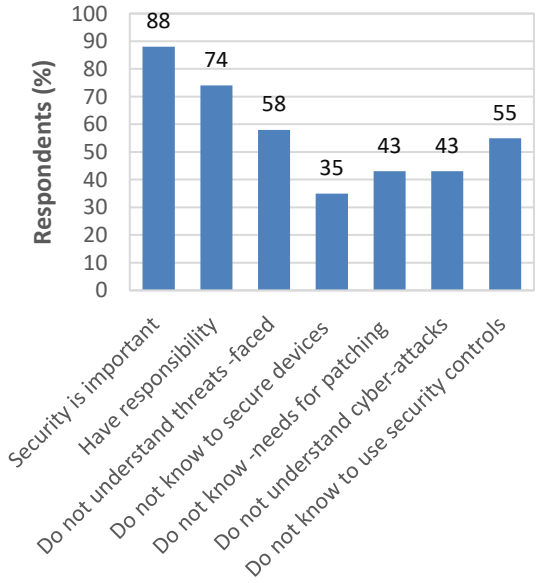

Figure 7. Respondents' perception and potential barriers

The results indicate a lack of knowledge and skills among respondents, potentially limiting their ability to adhere to best security practices. This lack of security knowledge may stem from participants not actively engaging in self-education about information security, possibly due to various reasons. Additionally, limited or no access to security awareness and training resources could contributed to this knowledge gap. However even if an end-user has undergone a training, or self-educated on security, there is still a risk of forgetting crucial information. Therefore, there is a need for continuous, appropriate, and tailored help and training for end-users, with goal to enhancing their awareness, knowledge, and improve their adherence to good security practices and compliance.

4.5. Security knowledge

The final section of questionnaire assessed respondents' knowledge and examined whether their stated security practice and knowledge align with their real-world security practices and knowledge. Respondents were asked about their understanding of what constitutes a strong password and the individual with whom password cab be shared. The results are illustrated in Table.2. and Table.3. respectively

Table 2. Percentage of respondents in relation to strong password

Which one of the following makes a stronger password? Please, select one that is relevant	%
Password that easy to remember such as names or other dictionary words	9
Password that consists of lowercase/ uppercase	10
Password that consists of both number and letters	17
Password that contains letters, symbol, punctuation characters and numbers	59
Password that consists of only numbers and symbol/punctuation characters	5

Table.3. Percentage of respondents in relation to sharing password

In which of the following situations do you think that it is acceptable to share your password?	%
Sharing password with close friends or family members	23
Sharing password with colleague who has the same access to systems as you do	10
Sharing password with manager or network administrator	10
Sharing password with someone who has shared their password with you	10
None of the above	48

The findings reveal a lack of knowledge among a notable number of respondents in creation of strong password. Moreover, most of participants seem unaware that password should not be shared with others, possibly they believe that sharing password in certain situations is acceptable.

Furthermore, respondents' security knowledge was examined in relation to data protection from

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

unauthorized access. The findings are shown in Table.4.

Table.4. Respondents' knowledge about data protection

Possible techniques	%
Backup information/data in another external device such as external Hard-disk or USB.	41
Save data in a compressed format.	21
Encrypt data and protect it with password.	22
Save a copy of data on my computer.	40
All of the above.	16

The results in Table.4. is worrying, as a vast majority of respondents lack knowledge to safeguard their data from unauthorized access. They have difficulty to differentiate between processes such as of backing up data, saving data copies, compressing data and protecting data from unauthorized access. This demonstrates a clear lack of awareness and knowledge in relation of data protection among respondents.

Respondents were also asked about their data backup practices, including the frequency of such backup. Surprisingly, only 33% of participants indicated regular data backups, whether on a monthly, weekly, or fortnightly basis. while one might argue that the frequency of data backup is usually related to changes in the data and its values, but given professional roles of respondents, it is expected that they would be more concern and regularly perform data backup. The observed non-compliance is possibly due to lack of knowledge, unawareness, or carelessness in adhering to best security practices. However, negligence in security compliance among end-users within organizations is a challenging issue and addressing it may involve monitoring their security practices and implementing appropriate interventions. Respondents were also asked about their activities that could potentially lead to malware infection on their devices. The result is shown in Table.5.

While majority of respondents show understanding of certain ways in which malware spread such as through email attachments, downloading files and clicking on social media links, there is a noticeable lack of awareness about other methods such as using USB, and hyperlinks. Surprisingly, over half of the participants are unaware that hyperlinks in emails and removable devices such as USB can be used for malware distribution. Furthermore, despite recognizing malware distribution though links, email attachments and USB, about half of respondents do not fully comply with best security practices, as shown in Figure. 9.

The findings in Figure 9 clearly indicate that respondents are not adhering to best security practices. This non-compliance may be due to users' carelessness, posing security concern for many

Table.5. Respondents' knowledge of malware distribution methods

Which of the following can potentially cause your computer to be infected with malware?	%
Through email attachments	61
Downloading files from the web	70
Social media scam links	58
Removable devices such as USB	49
Hyperlink(s) within email	48

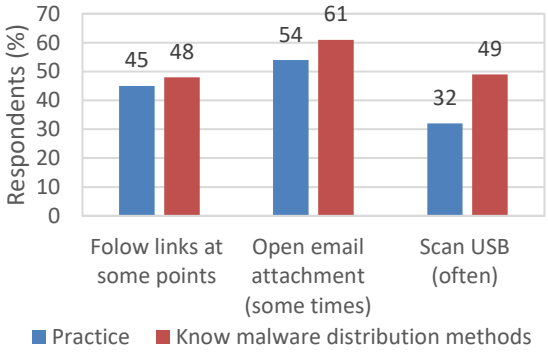

Figure 8. Not complying with best security practices

organizations. Addressing end-users' carelessness is challenging, specifically when they already have the required knowledge. Moreover, the results from Figure.9. reveals discrepancy between what users claim to do and know, and actual security behavior and knowledge.

Similarly, findings from Figure.10 also suggest that there is a discrepancy between what respondents claim to know and do, and their actual security knowledge and skills. Their knowledge does not reflect their claimed skills and knowledge. Such behaviours may give false sense of confidence, and in turn false sense of protection.

Figure 9. Discrepancy between respondents claim and their knowledge/practice

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

5. Survey Analysis

The results of the survey are based on a wide range of respondents from different universities. It is perceived that respondents have required knowledge and skills to protect their devices, with notable 87% expressing confidence in their abilities to do so. Nevertheless, lack of knowledge among respondents is evident. While a high proportion of participants recognize the importance of security and acknowledge their responsibility in device protection, they are constrained by lack of knowledge when it comes to implementing security controls and measures. Moreover, they find it difficult to understand the various type of attacks, social engineering, threads they face and importance of security updates. It also evident that what respondents claim to do or know are not aligned with their actual security practices, as shown in Figure 10. This discrepancy could result in end-users having false sense of security, which, in turn, creates a vulnerable environment for security attacks within organizations. However, it is arguably challenging for users to acquire the necessary knowledge and skills promptly when it is needed. Even if they have the opportunity to participate in awareness and training programs, there is no guarantee that they will retain the required knowledge over an extended period or when it is needed. Thus, providing users with appropriate and tailored interventions when needed is crucial for ensuring security compliance.

Furthermore, overall findings suggest that many respondents are not adhering to recommended security practices, as illustrated in Figure.9. This lack of compliance may be due to several factors, including a lack of knowledge, skills, awareness, training or intentional malicious behaviours or carelessness. All these factors can pose risks to the security of the organization. Addressing this issue is both challenging and complicated, and as result, it is more likely that the problem cannot be effectively resolved with current security awareness measures.

Therefore, an alternative approach to current security training/awareness is required where it considers abovementioned factors and integrate into a framework that provide a platform to continuously monitor end-users' security behaviours and provide them with a tailored interventions when is required.

6. A Novel Cyber Security Awareness and Compliance Framework

To overcome the aforementioned issues, a holistic and connected approach is required. Based upon an analysis of the problem and the prior art, the following requirements have been identified:

- To continually monitor and capture user's actual security behaviours and compliance with organizational policy.
- Seek to maximize learning and engagement through tailoring learning to both the job role and the individual – taking into account specific learning requirements of the role and the prior education of the individual.
- To intelligently generate tailored feedback, interventions and reminders based on user behaviours.
- To embed a continuous lifecycle into monitoring, education, and compliance on an individual basis.

The proposed framework aims to enforce and enhance user's actual security compliance and performance through the process of identifying individual user's needs, targeted intervention and help, including a tailored security program which meets individual security needs and job functionalities. The proposed system considers both content and framework, but mainly focuses on framework architecture as a platform to tailor security interventions and facilitates the process of determining and identifying objectives and required tasks for individual learner's security subject matters. This forms the foundation for the process of identifying user's needs and provide appropriate interventions according to role to enhance individual user's actual security behaviours and application.

The process of enhancing user's security compliance encompasses four main principles:

- Continuously monitor and capture user's security behaviours and practice.
- Evaluate the captured behaviors.
- Identify and analyze user's weakness, strength and learning requirements.
- Provide tailored and appropriate interventions and help.

The principles are conceptualized in Figure. 11. The framework provides a multi-modular system to address the principles of enhancing and enforcing user's security compliance. The process starts with monitoring and capturing user's actual security behaviours. This is vital to understanding and evaluating user's security practices and compliance. Such evaluation enhances the process of identifying user's security weakness, strengths and needs, and accordingly to allocate, provide and implement interventions. To achieve this, the system utilizes several sources to identify user's needs including monitoring, active evaluations; role/job responsibilities; end of learning test results; and manger's

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

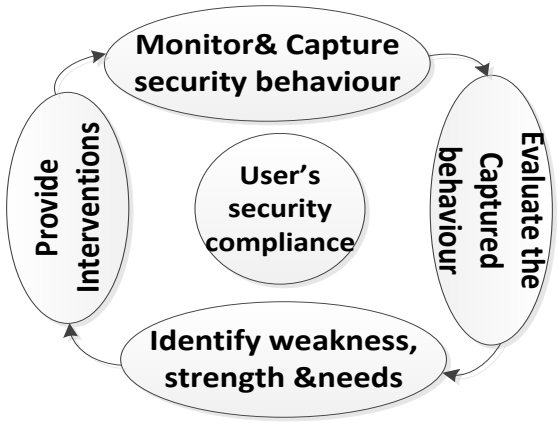

Figure 11. Principles of enhancing security compliance

observation(s). The needs are then analyzed to identify and understand the user's security constraints and the reason(s) for any security non-compliance. Then based on results, the system provides appropriate interventions, which are centered around individual user's achieving compliance related to their job responsibilities and tasks. The interventions examples include manager's alert, quick reminders, tailored training, testing, feedback/guidance, reward and punishment.

The interventions are developed and utilized to address user security needs and to improve their security compliance. Figure. 12. provides an overview of the proposed system. It consists of several interconnected components working together to improve user's actual security behaviours and practice in real world settings.

The framework components are listed and briefly described in the following sections.

- Monitoring and capturing module: The primary aim of this module is to continuously monitor and capture user's security behaviors in real time. Recognizing that individuals are likely to utilize multiple devices (e.g., laptop, mobile, tablet), the system will aggregate these behaviors into a single profile. It is also essential that capture of this data is at an appropriate resolution to enable the framework to function but is also mindful of user's privacy.

- Compliance Module: The aim of this module is to determine whether the captured behaviors meet the recommended security requirements or not by checking them against recommend security practice defined in security policies and role responsibilities. Then it classifies the behaviors either into positive or negative class, based upon whether the behaviors meet recommended security requirements.

- The assessment and Intervention Module: The aims of this module are twofold:

  - Identify and understand the reasons for user's non-compliance behaviors.

  - Provide appropriate intervention(s) according to the user's needs.

The module comprises of Assessment Agent and Interventions Agent. The Assessment Agent assesses a user's security aptitude for each behavior that does not meet recommended security requirements. The Intervention Agent analyses the received result(s) from testing agent and selects a set of appropriate action(s) / intervention(s).

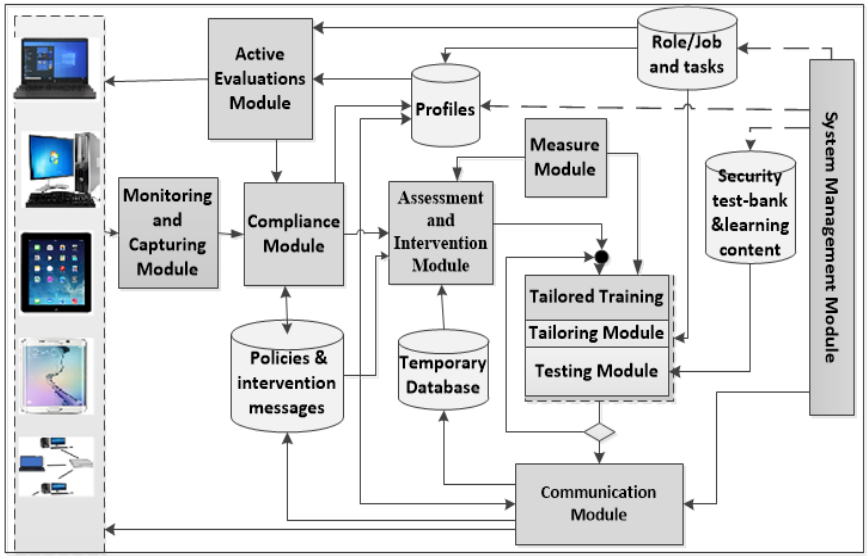

Figure 12. Architecture of the proposed Framework

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

- Active Evaluation Module: This module actively tests user's actual security behaviours and performance in real setting. The module for example can simulates Social Engineering (SE) attacks and target individual user on regular bases in relation to their job responsibilities.

- Tailored Training: This component provides a platform to deliver tailored training according to the user's needs. It consists of the following modules:

  - Tailoring module: Provides a platform for delivering a tailored training session. This module operates in two modes. The first mode provides a short, tailored training session on specific security aspects, where the second mode provides full tailored training in relation to job responsibilities.

  - Evaluation module assesses users' security knowledge and awareness at end of each training session.

- Communication Module: The primary function of this module is to respond to different requests from different agents and fulfil each request to make communication possible among different components of the system.

- Measure Module: This module provides various assessment methods including self-reported questions, knowledge-based questions and hand-based on practice questions.

- System Management Module: This module provides an interface to the system's users to perform required tasks. It utilizes three modes of operation:

  - Author mode: Enables authors to manage and develop training content, questions, and interventions.

  - User mode: Provides users with different functions including register, view profile, navigate system and take training sessions.

  - Administrator mode: Provides high-level of system administrative privileges to manage and perform a wide range of tasks.

7. Tailoring requirements aspects

Cyber security is not only the responsibility of security specialists or those with a security related role, but it is the responsibility of everyone within an organization. Many employees who can find themselves having security-related responsibilities (e.g. receptionists, human resources, help desk supporter, finance, etc.) neither hold formal security certificates/qualifications nor work toward them [20]. Therefore, understanding and identifying user's job/role responsibilities are important in the process of identifying user's needs, possible security attacks, risks, and impact of breach(es) on assets through individual user. And in that to provide and tailor interventions to enhance user's compliance in relation to job responsibilities.

7.1. Principles of identifying role and responsibilities

While cybersecurity should be responsibility of everyone within an organization to maintain confidentially, integrity and availability (C.I.A) of the assets, the nature of vulnerabilities, threats/risks, and attacks to the organization through one user to another vary. Such variations are mainly due to individual characteristics and role responsibilities. Thus, cyber attackers often target individual user based on role within organizations [21]. For example, a targeted attack against a receptionist will differ from a targeted attack against a manger. Nevertheless, role responsibilities are not uniform across organizations. The same role within two different organizations may be assigned with different responsibilities/tasks, and in turn the impact of a security breach may vary accordingly.

To set the context of identifying role for tailored security interventions, it is important to look at the process of considering job responsibilities from different perspectives. Unlike other studies in which they have mapped role with knowledge/skills areas, this study goes beyond on that by also considering possible type of attacks, risks, and impact of potential breaches, attacks vector, and possible mitigation methods/techniques. Therefore, responsibilities for each individual role need to be analyzed independently, as each position has its own responsibilities with different security requirements. As such a uniform curriculum cannot be applied to the same role or individual, as no single program is applicable to everyone. However, the following steps could be used as guidance in identifying role and job responsibilities with required competency.

i. Identify/establish individual user/employee's role/position.

ii. Identify, analyze, and understand user/ employee's role/ job responsibilities and tasks.

iii. Analyze and understand user/employee's level of access to assets and its criticality.

iv. Identify possible types of attacks/threats based on role responsibilities or what threats/attacks are user/employee vulnerable from.

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

v. Identify possible techniques that could potentially be used in an attack.

vi. Identify the potential impact of security breaches on the assets through a user based on level of impacts: Low, medium and high.

vii. Develop possible security countermeasures including required knowledge, skills, and ability (according to job responsibilities) which user/employee needs to learn and implement to mitigate threats and attacks in relation to C.I.A.

7.2. Example of a tailored policy

A set of security policies and responsibilities needs to be developed for each role. This is shown in Table 2, where they are then used to define compliance and non-compliance behaviors.

Table 6. Example of tailored security policy-HR

Task	Minimum requirement /policy
Password	12 characters
	Mixture of symbols/characters, digits, upper/ lower letters.
	Must me changed every 90 days.
	Should not be shared.
	Should not be written down on unsecure piece of paper.
	Multi-factor authentication needs to be enabled.
Computer /laptop	Unattended computer must be logged out.
Email	Email from unknown sources should not be opened.
	Hyperlink within unknown email should not be opened.
	Attachments should not be downloaded from unknown sources.
	Information should not be provided for unverified email.
Sensitive Data	Data should be encrypted.
	Data should be handled in compliance with General Data Protection Regulation (GDPR).
	Should be backed up regularly.
	Should not allow a third-party access.
Physical files	Sensitive files must securely be stored.
Clear desk	All sensitive data should be kept in a secure place.
External disk	Attached disk must be scanned

7.3. Interventions

Interventions aim to address individual users' security needs and enhance their security competency and compliance by providing appropriate interventions according to individual's security behaviours and needs. Multiple interventions may be suggested and used to improve, strengthen, and maintain an individual's security compliance.

Table 7. List of interventions

Intervention	Description
Manager observation	The framework allows managers to feed their observations about user's behaviours (e.g., sharing password with colleagues,) into the system.
Manager alert	The system informs managers about a user who is competent, yet does not comply with good security practice.
Quick reminder	Aims to raise SA and knowledge. The messages are of two types. • General messages (e.g., do not share your passwords with others.) are aimed at all users. • Semi-tailored messages are tailored according to individual user's role and responsibilities. The system considers the nature of behaviours. A user with competent compliance behaviours will receive less frequent messages than a user with non-compliance behaviours.
Feedback and guidance	These interventions assist individuals to implement and comply with security policies. They are provided in the following formats: • Hint: Shows the user how to perform a task. • Reminder message: Informs the user that a task needs to be completed (e.g., Change password within 10 days). • Alert message: Informs the user about current security tasks (e.g., alert user if s/he uses previous password for creating a new one).
Reward and punishment	The system analyses user's profile over period of times and suggest one of the followings: • Reward: if the user's security compliance has been improved or sustained with good security practice, • Punishment: if the user has competency but does not comply with best security practice.

Several interventions are developed and used by the system, not only to improve user's security practice and compliance, but also to inform and help managers to understand how each individual employee complies with good security practice and as well as possible reasons for any non-compliance.

 | DOI: 10.20533/ijcc.2046.3359.2023.0029

The framework tailors each intervention including training sessions according to an individual user‘s needs and role. The system provides various interventions and they have been described in Table 3.

8. Conclusion

The primary aims of the proposed framework are to enhance and enforce user’s actual security behaviours and compliance and enable organizations to quantify their security status and identify possible risks from individual users. Continuously monitoring and capturing user’s security practice adheres users to comply with recommended security and enable the system to identify the reasons behind any non-compliance behaviours and accordingly allocate and implement appropriate interventions. Utilizing interventions address user needs in that provides required tailored training, help and guidance to enhance their security practice and inform management for any undesirable user security behaviours and subsequently an organization’s overall security status. Future work will focus upon developing and evaluating a prototype of the proposed approach.

9. References

[1] Axelos. (2016). Cyber Resilience: Are your people your most effective defence? DOI: 10.1177/0266382116650299.

[2] Caldwell, T. (2016). Making security awareness training work. Computer Fraud and Security, 2016(6), 8–14. DOI: 10.1016/S1361-3723(15)30046-4.

[3] Bada, M., Sasse, A., and Nurse, J. R. C. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? In Proceedings of the International Conference on Cyber Security for Sustainable Society (pp. 118–131).

[4] Furnell, S., and Vasileiou, I. (2017). Security education and awareness: just let them burn? Network Security, Elsevier, (12), 5–9.

[5] Korovessis, P., Furnell, S., Papadaki, M., and Haskell-dowland, P. (2017). A toolkit approach to information security awareness and education. Journal of Cybersecurity Education, Research and Practice, 5(2), 34.

[6] Furnell, S. M., Warren, A. G., and Dowland, P. S. (2003). Improving Security Awareness Through Computer-Based Training. Security Education and Critical Infrastructures, 287–301.

[7] Haeussinger, F. J., and Kranz, J. (2015). Information security awareness: Its antecedents and mediating effects on security compliant behavior. In Thirty Fourth International Conference on Information Systems (pp. 1–16).

[8] Srikwan, S., and Jakobsson, M. (2008). Cryptologia Using Cartoons to Teach Internet Security Using Cartoons to Teach Internet Security. DOI: 10.1080/01611190701743724.

[9] Lötter, A., and Futcher, L. (2015). A framework to assist email users in the identification of phishing attacks. Information and Computer Security, 23(4), 370–381. https://doi.org/10.1108/ICS-10-2014-0070 (Access Date: 27 June 2023).

[10] Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers and Security, 26(1), 63–72. DOI: 10.1016/j.cose.2006.10.005.

[11] Burke, I. D. (2011). Design of cyber security awareness game utilizing a social media framework. In Information Security South Africa (ISSA) (pp. 1–9). Ieee. DOI: 10.1109/ISSA.2011.6027538.

[12] Asanka, N., and Arachchilage, G. (2012). Security Awareness of Computer Users : A Game Based Learning Approach. PhD Thesis. Brunel University.

[13] Ghazvini, A., and Shukur, Z. (2017). A Framework for an Effective Information Security Awareness Program in healthcare. International Journal of Advanced Computer Science and Applications, 8(2), 193–205. www.ijacsa.thesai.org (Access Date: 14 June 2023).

[14] Niekerk, J., and Von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. Issa, 1–13.

[15] Poepjes, R., and Lane, M. (2012). An Information Security Awareness Capability Model (ISACM). In Australian Information Security Management Conference (pp. 1–8). DOI: 10.4225/75/57b55238cd8d2.

[16] Mejias, R. J. (2012). An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. In 2012 45th Hawaii International Conference on System Sciences (pp. 3258–3267). DOI: 10.1109/HICSS.2012.104.

[17] Alotaibi, M., Furnell, S., and Clarke, N. (2015). Towards dynamic adaption of user’s organisational information security behaviour. Australian Information Security Management Conference., 2015, 28–36. DOI: 10.4225/75/57b698e1d9389.

[18] Alotaibi, M. (2017). A model for monitoring end-user security policy compliance. PhD Thesis. University of Plymouth. https://login.ezproxy.leidenuniv.nl/ (Access Date: 24 June 2023).

[19] Statista. (2019). Statista.pdf. https://www.statista.com (Access Date: 14 May 2023).

[20] Uk-gov. (2018). UK Initial National Cyber Security Skills Strategy, increasing the UK’s cyber security capability. https://assets.publishing.service.gov.uk (Access Date: 12 October 2023).

[21] Burns, A., Johnson, M., and Caputo, D. (2019). Spear phishing in a barrel : Insights from a targeted phishing

campaign. Journal of Organisational Computing and Electronic Commerce, 29(1), 24–39.

[22] Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. DOI: 10.1057/ejis.2009.6.

[23] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness A conceptual foundation for organizational information security awareness. Information Management and Computer Security, 8(1), 31–41.

[24] Dominguez, C. M. F., Ramaswamy, M., Martinez, E. M., and Cleal, M. G. (2010). A framework for information security awareness programs. Information Systems, 11(1), 402–409.

 | DOI: 10.20533/ijcc.2046.3359.2023.0029