EXPLORING END-USERS' ENGAGEMENT WITH SECURITY THREATS: A SURVEY-BASED INVESTIGATION FROM ACADEMIC AND SECURITY EXPERTS' PERSPECTIVE

Mousa Jari[1,3], Kovila Coopamootoo[2] and Rasha Ibrahim[1]

[1] School of Computing, Newcastle University, Newcastle upon Tyne, UK
[2] Department of Informatics, King's College London, London, UK
[3] College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

Amid growing concerns about security and privacy, and their impact on decision-making, researchers have sought to understand the reasons behind users' seemingly risky behaviour in disregarding security advice. In this study, we delve into the perceptions of security experts on end users' threat models and their cybersecurity practices and habits. This research explores the perceptions of security and privacy experts regarding end users' threat models and their behaviours in relation to cybersecurity. A survey was conducted with 55 experts, including 27 females and 28 males, to gain insights into end users' habits, practices, and feelings from the perspective of security experts. The study reveals that end-users express moderate concern about privacy and security while carrying out their daily tasks. However, security experts believe that end-users tend to be passive towards organisational security policies, and their lack of knowledge about these policies which may lead to negative feelings. Additionally, experts perceive that end-users may be unaware of security measures, have difficulties understanding security concepts, and are at high risk of falling victim to phishing attacks by opening attachments and clicking on unknown links.

KEYWORDS

Security, Privacy, Policies, Phishing, Experts & End-users.

1. INTRODUCTION

The increasing reliance on technology and data-driven processes has amplified the potential risks posed by security breaches and privacy violations. Therefore, understanding end-users' compliance with security and privacy policies is of utmost importance in today's digital age. End-users, as insiders, can play a crucial role in making daily, routine decisions that directly affect the security of their organisations [1, 2, 14]. Compliance with security and privacy policies ensures that end-users within an organisation follow best practices and adhere to established protocols. This adherence fosters a secure setting and mitigates the likelihood and the potential of data breaches, cyberattacks, and other security incidents. The effectiveness of an organisation's security measures hinges on the diligence and knowledge of its end-users, regardless of the technological safeguards and measures in place [14]. To understand the critical issues and threats underlying information security and mitigate the risks associated with major security and privacy problems, it becomes essential to comprehend experts' perceptions towards security practices

David C. Wyld et al. (Eds): NSEC, InWeS, CSIP, BMLI, CACIT, EDUIT -2023
pp. 01-17, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131501

followed by end-users. Additionally, the adoption of information security solutions and standards remains low [3], and human factors, such as emotions (e.g., frustration and stress), introduce an element of unpredictability to security and privacy policies [8, 18]. Surveys exploring these aspects from the point of view of experts can help prioritise the most critical security issues and factors such as feelings related to cybersecurity, as emotions have been shown to have an impact on security and privacy-related issues.

This paper delves into the realm of end-users' compliance, security threats, and their potential feelings that may impact security and privacy-related matters. It explores the perceptions and information security practices of end-users from experts' point of view, aiming to identify end-users' behaviours and habits as well as common mistakes they make while uncovering the security issues that may induce stress or negative feelings and behaviour among them.

To achieve these objectives, the research conducted an initial and an exploratory online survey with security experts, providing valuable insights into the intersection of security perceptions, emotions, and behaviours among end-users. The study's findings carry significant implications for future planning, enabling effective strategies to address cybersecurity challenges and promote safer online practices among end-users.

This research identifies the issues, behaviours, and security decisions that security experts perceive about end-users regarding security threats, knowledge, understanding, level of concerns, and security policies and requirements. Also, this work explores experts' perceptions about specific security and privacy scenarios that may have an emotional impact or induce negative feelings among end-users.

2. BACKGROUND

In this section, we present an overview of various published research works related to security threats, end-users' compliance with security policies and procedures, and human factors such as behaviour, habits, feelings, and emotions in the security and privacy context.

Security risks and threats arise from multiple sources and motivations which can cause different types of damages. Loch et al. developed taxonomy threats to information security and were categorised into four dimensions [12]. It categorises as internal (human & non-human) and external (human & non-human). Subsequently, they categorized threats whether it is intentional, or it is accidental threats [12], but the greatest threat of all remains the insider threat from the organisational member [19]. In fact, insiders may cause great harm to the confidentiality, integrity, or availability of the Information System [20]. Kobis classified threats into the following: threats that are associated with the use of information technology, threats caused by human factors and actions, and lastly threats associated with the information technology model [11]. Kobis also discussed that human factors are the major factor in infiltrating information. Security threats are associated with human factors including social engineering and phishing.

On the other hand, organisations proposing solutions and measures for viruses, malware, threats, or services to counter hackers reinforce and highlight the importance of protecting against external attacks [16]. Nevertheless, it is essential not to overlook potential problems originating from end-users and insiders. In addition to the evidence of external attacks on organisations, there is substantial evidence to indicate that insiders, end-users within the organisation, have been involved in significant and costly security incidents which can arise from both intentional and accidental actions, making them a significant concern for organisations [16].

Organisations establish security policies to ensure the safety of information resources but if end-users do not understand the importance of these practices, and if they are unwilling to follow them, then these efforts are effect-less and in vain [7]. One of the causes of security incidents is that end-user negligence has led to security breaches within enterprises which lead to massive financial loss [7, 15]. Quader and Janeja [15] also provided an in-depth study of cyberthreats and studied cases of security threats. They investigated the factors that may cause attacks, including the human behavioural aspects, and they mentioned the security policies' adoption and training and awareness. They conclude that the human behavioural aspects lead up to cyberattacks and security threats and having security policies is vital to safeguard from threats.

Several researchers have introduced the concepts of "security and privacy fatigue" and "security-related stress," which specifically involve emotions in security and privacy experiences. Furnell and Thomson ?? used the term "security fatigue" to describe and define particular online security experiences. Their study aimed to identify the manifestations of decision fatigue and its impact on users' security decisions. They proposed that there is a threshold beyond which some users find it challenging to maintain security.

Various research scholars have addressed and discussed emotional issues related to security and privacy [6, 9, 10]. Coopamootoo et al. studied and discussed the effects of negative emotions (e.g., fear and frustration) on security and privacy issues [4]. They found that users often experience frustration and feeling tired, turned off, or overwhelmed with security technologies, making security solutions and measures more challenging for users instead of supporting their activities. The study also highlights the link between security fatigue and user frustration. Similarly, Furnell et al. [5] confirmed that security fatigue influences users' security decisions. Additionally, anger and related emotions like frustration and annoyance have been associated with password security, particularly in password choice. Gulenko et al. [19] conducted a study exploring the impact of positive and negative emotions on password habits and analysed their effects on password strength. Furthermore, emotions have been linked to privacy concerns, where privacy-related issues may evoke negative emotions such as fear. Namara et al. [13] found that users who are emotionally invested in protecting their privacy are more likely to use a VPN. Their research discusses the adoption of virtual private networks (VPNs), factors influencing VPN adoption, and the emotional decision-making process.

3. METHODOLOGY

The primary objective of this study was to investigate the most significant security threats from the perspective of security professionals, as well as the feelings and emotional impact of these threats on end-users when dealing with security and privacy issues. In this section we provide details about participant recruitment and characteristics, the study procedure and questionnaire design, and the research ethics process.

3.1. Participants

We recruited 55 security experts and professionals, comprising 27 females and 28 males. The distribution of respondents' details based on their educational degrees and gender are shown in table 1. It provides a comprehensive overview of the respondents' educational backgrounds and gender distribution, displaying the total counts and percentages for each educational degree category along with the corresponding numbers and percentages of female and male participants. The largest group of respondents holds a bachelor's degree (33%) and a master's degree or higher (45%). The majority of respondents, comprising 35.71%, fall within the 30 to 39 years old category, followed closely by 32.14% in the 20 to 29 years old group. Additionally, 25% of the

participants are between 40 to 49 years old, while a smaller portion, 5.36%, consists of experts aged 50 years or older.

Table 1. Distribution of respondents based on educational degrees and gender.

Degree	**Total**	**%**	**Gender**	
			Female	**Male**
High School	6	11%	3 (5.5%)	3 (5.5%)
Associate/College Degree	6	11%	4 (7%)	2 (4%)
Bachelor's Degree	18	33%	13 (24%)	5 (9%)
Master's Degree or Higher	25	45%	7 (13%)	18 (33%)
Overall	55	100%	27 (49%)	28 (51%)

The participants were selected from a diverse range of organisations, including public and private entities in the United Kingdom, Saudi Arabia, and the United States, with expertise in cybersecurity. These respondents are likely to have a good understanding of security threats and security-related decisions that likely impact end-users. We asked security experts to gain insights into their perceptions of their employees and end-users in general. Many of these experts deal not only with employees but also with other types of users and individuals due to their job positions or job experiences, such as students using labs and IT devices, clients, and visitors to these organisations, table 2.

Table 2. Job Titles and Counts.

Category/Area	Job Title	Counts
Managerial	Manager	7
	IT Governance Analyst & Auditor	2
	Cybersecurity Team Leader	1
Edu. Institutes	Researcher	7
	Lecturer	3
	Assistant Professor	3
	Faculty Member	2
	Dean & Chair	2
	Associate	1
IT	IT Support	7
	Administrator & Administration Assistant	3
	Technician 3	3
	IT Specialist & Software Engineer	2
Other	Officer, Senior Officer, Security Engineer, Comm. Supervisor, etc	12

The table presents job titles and their corresponding counts categorised into managerial, educational institutes, IT, and other areas. It showcases the distribution of job titles across different areas, with the highest count of 7 for "Manager" in the managerial category, 7 for "Researcher" in the educational institutes' area, and 7 for "IT Support" in the IT category. Additionally, the "Other" category encompasses 12 job titles, including Officer, Senior Officer, Security Engineer, Security Consultant, and Communication Supervisor, among others. The selection process involved targeted email and WhatsApp invitations, and participants were encouraged to share the survey with their colleagues with security backgrounds. We chose those participants in those countries because of previous connections during the first author's previous education and job history from different organisations: Universities and security organisations. In

total, 62 security experts were invited to participate in the survey, of which 55 willingly took part. The survey remained open for 10 days to allow ample time for responses.

3.2. Survey Design and Content

The survey, conducted in 2020 through an online web application form, comprised a demographic questionnaire, open-ended questions, and Likert scale questions. Participants had the opportunity to respond to the open-ended questions using free-form text. The Likert scale questions had 5-point ratings, ranging from "Very unlikely" (1) to "Very likely" (5), with a neutral midpoint (3). The survey covered the following areas: 1) Concerns of security risks and threats committed by end-users. 2) Perceptions of end-users' feelings regarding security requirements and security threats from the expert perspective. 3) Understanding and compliance with information security policies and procedures. 4) The greatest information security threats.

3.3. Ethics & Consent

Before initiating the study, we secured comprehensive approval from the Ethics Committee at Newcastle University. Prior to engaging with the questionnaire, participants willingly provided their consent for data collection. The research meticulously followed conscientious research protocols within the realm of computer science. It's noteworthy that all respondents affirmed possessing either a cybersecurity degree or certificate, or a minimum of 3 years of experience in information security or a closely aligned domain of expertise.

3.4. Data Analysis and Qualitative Coding

We employed a conventional line-by-line coding method to analyse the participants' free-form text responses. Each response was read thoroughly to identify specific themes. The coding process was validated and refined through discussions with another coder and reviewed by the authors [4]., ensuring a robust analysis. Other data were analysed descriptively.

4. RESULT

In this section, we will present the results of our study in both descriptive and quantitative formats. For the scale questions, scores were calculated by averaging the responses for each question and calculating the standard deviation. Furthermore, we meticulously coded the qualitative data to enhance comprehension and gain deeper insights.

4.1. Concerns About S&P

On a Likert scale, we asked the security experts to gauge the extent to which their employees or end-users expressed concerns about privacy and security while carrying out their daily work. The results revealed a significant level of concern among the end-users. Out of the total respondents of the experts, 15% indicated that end-users were extremely concerned about security and privacy, while 29% expressed moderate concern, and another 29% showed a somewhat concerned attitude, as shown in 1. Additionally, 22% of the respondents were slightly concerned, and only 5% reported not being concerned at all. The average score was found to be 3.25, with a standard deviation of 1.13, suggesting a moderate level of variation in the responses. The median value of 3 further corroborated the overall moderate level of concern. These findings indicate that a considerable proportion of employees and end-users are conscious of the importance of privacy

and security in their daily work, emphasising the significance of robust security measures and awareness programs within organisations.

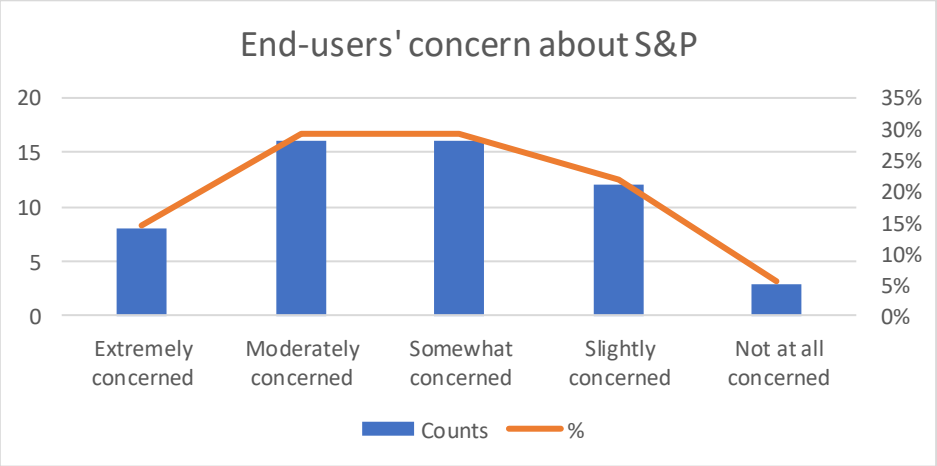

Figure 1. Security Experts' Assessment of End-Users Privacy and Security Concerns

4.2. Understanding S&P Policies & Procedures

We asked the security experts about their perceptions regarding the time it takes for employees and end-users to comprehend the organisation's policies and procedures. The majority of respondents, constituting 62%, agreed that employees do indeed take some time to grasp the policies and procedures, while 11% strongly agreed with this notion, table 2. In contrast, 20% disagreed, expressing the belief that employees do not require a substantial amount of time to understand the policies and procedures. Notably, no respondents strongly disagreed with the statement. The average score of 3.64 indicated a general agreement among the experts regarding the learning process for employees, while a standard deviation of 0.93 suggested a moderate level of variation in their opinions. Furthermore, the median value of 4 supported the notion that, on average, employees take a reasonable amount of time to become familiar with the organisation's policies and procedures.

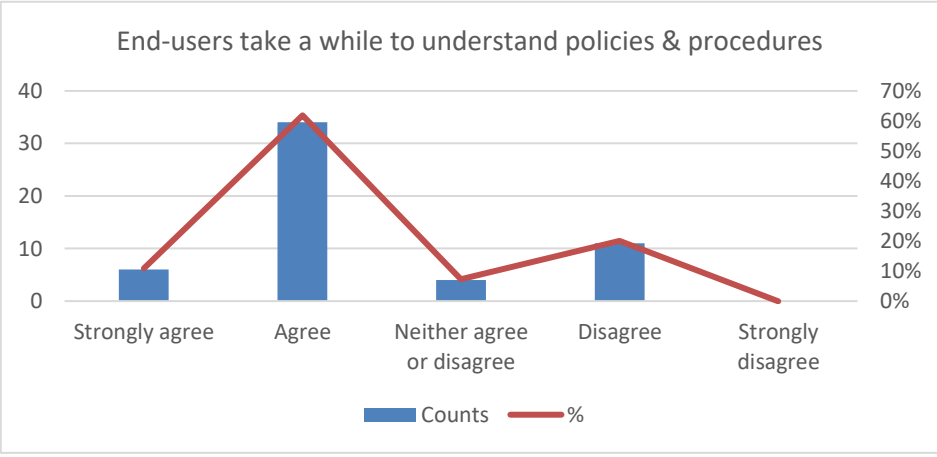

Figure 2. Security Experts' Perception of End-users Understanding: Policies & Procedures

4.3. Knowledge of Information Security

We asked the security experts about their perceptions regarding end-users' knowledge of information security and their ability to comply with the organisation's policies. The responses indicated varying viewpoints among the experts. Among the respondents, 33% agreed, and 13% strongly agreed that end-users do not possess sufficient knowledge about information security to comply with the organisation's policies, figure 3. Conversely, 33% disagreed, while 5% strongly disagreed with the statement, expressing confidence in end-users' understanding of information security. The average score of 3.15 signified a moderate level of agreement among the experts, with a standard deviation of 1.18, suggesting a moderate level of variation in their opinions. The median value of 3 further supported the perception that, on average, there is a perceived lack of comprehensive knowledge among end-users regarding information security and their adherence to organisational policies.

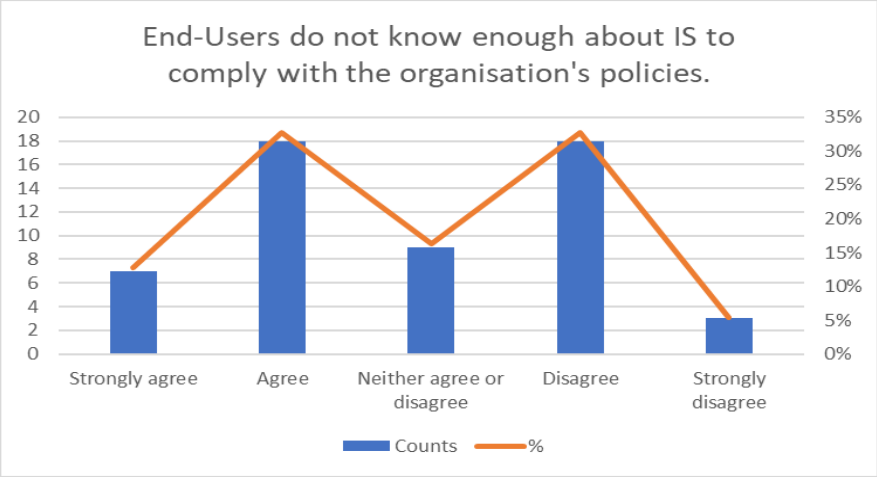

Figure 3. Security Experts' Perception of End-Users' Information Security Knowledge and Compliance with Policies.

4.4. Greatest Threat is Phishing

In an open-ended question, we sought the opinions of security experts regarding the greatest information security threats perceived by insiders, employees and end-users, within their organisations. The responses were carefully analysed and categorised into distinct themes. The identified themes and corresponding results are presented in table 3 below:

Table 3. Greatest Information Security Threats Perceived

Theme	**Counts**	**%**
Phishing	11	15.71%
Data leakage	9	12.86%
Malware/Malicious software	9	12.86%
Data breaches / Unauthorised access	9	12.86%
Lack of awareness and training	8	11.43%
Hackers' attacks	8	11.43%
Noncompliance with policies / careless	7	10.00%

The table above displays the different themes that emerged from the responses, along with the corresponding counts and percentages. It indicates the relative significance of each information security threat as perceived by insiders in the organisations. Data leakage and phishing were mentioned by 12.86% and 15.71% of respondents, respectively, as the most prominent threats. Additionally, malware/malicious software and data breaches/unauthorised access were perceived as significant concerns, with each accounting for 12.86% of the responses. Lack of awareness and training, hackers' attacks, and noncompliance with policies/careless behaviour were also identified as noteworthy threats, each representing approximately 10% to 11.43% of the perceptions. Other internal and external threats were mentioned by 12.86% of respondents. These findings offer valuable insights into the information security landscape from the perspective of insiders and highlight the importance of addressing these specific threats to enhance overall security measures in organisations.

Several security experts provided insightful responses regarding the greatest information security threats perceived by insiders within their organisations. Here are some notable examples:

P 4: "***Everyone should know how not to get baited by fake emails or any attempt to steal important data. I have realised that people between the ages of 40 and 70 have no idea how all of this happens; they need to have a background about it***." P4's insight highlights the need to educate employees, especially those in the 40 to 70 age group, about avoiding fake emails and data theft attempts.

P 7: "***Spam emails and opening viruses are common methods employed to access information about the organisation. GDPR regulations are often broken, leading to data being passed to the wrong people.***" P7's response draws attention to the common methods employed by attackers, such as spam emails and viruses, and the importance of adhering to GDPR regulations to prevent data breaches.

P 27: "***Malware attacks, phishing attacks, bad/weak passwords, and lack of encryption are the major concerns in security***." P27's perspective emphasizes the key of information security concerns, including malware attacks, phishing attacks, weak passwords, and lack of encryption.

P 47: "***Phishing attacks are a significant issue, as users have fallen victim to the methods hackers employ. If a phishing attack is successful, bad actors gain entry to an entire network of sensitive information through a user's email and password***." P47's input underscores the seriousness of phishing attacks and how they can grant hackers access to sensitive information through compromised email credentials.

4.5. Ignoring Security Advice

Another open-ended question was posed, where we sought the opinions of security experts regarding their perspectives on examples of employees and end-users ignoring security advice and policies within organisations. The most frequently mentioned theme was related to the Password/Credentials Policy, accounting for 22% of the responses. Unauthorised Devices/Services/Software and Email/Website Policies were also cited, each representing 15% of the responses. Other themes included Unauthorised Data Sharing/Misuse (12%), Noncompliance with Policies in general (11%), and Data Protection Regulations/Privacy (9%). Themes such as Physical Security, Backups/Updates, Firewall/Anti-virus/Two-factor Authentication, and Following Security Practices received smaller percentages of responses.

Table 4. Examples of Employees Ignoring Security Advice and Policies

Theme	**Counts**	**%**
Password/Credentials Policy	16	22%
Email/Website Policies	11	15%
Unauthorised Devices/Services/Software	11	15%
Unauthorised Data Sharing/Misuse	9	12%
Noncompliance with Policies: Ignoring & Not Reading	8	11%
Data Protection Regulations/Privacy (Law & Encryption)	7	9%
Physical Security	4	5%
Backups/Updates	4	5%
Firewall/Anti-virus/Two-factor Authentication	2	3%
They Follow Security Practices	2	3%

Regarding their perspectives on examples of employees and end-users ignoring security advice and policies within the organisation, several security experts provided insightful responses regarding the examples of employees and end-users ignoring security advice and policies within their organisations. Here are some notable examples:

P24: "***Download and install software from the internet, use bad passwords (and the same one for everything), sharing sensitive information, losing keys/codes, and being chatty***." P25: "***Increasing the number of devices with access to sensitive data, proliferation of sensitive data moving outside the firewall on mobile devices, and sharing passwords.***" P32: "***Sharing access to devices, passing passwords, or choosing easy passwords for their accounts, and accessing personal accounts using the organisation's devices and network***."

The above responses highlight a concerning trend of inadequate security practices among end-users, encompassing insecure password habits, sharing sensitive information, and expanding risks associated with mobile device usage and device access sharing.

The additional responses below from the participants emphasise various risky behaviours, particularly those related to email and internet policies, such as becoming susceptible to phishing: P 5: "***Clicking any random link, visiting random untrusted websites***." P 23: "***Opening attachments in emails without being 100 percent sure they are genuine***." P 30: "***Receiving links via email from unknown senders***." P 34: "***Clicking on phishing emails. Accessing information they shouldn't. Holding doors open to others without checking if they have ID***." P 45: "***Social engineering is always a concern***."

4.6. Mistakes End-users Make? Again Phishing !!

After obtaining responses from security experts regarding examples and scenarios where security advice and policies were ignored by end-users, we further introduced an open-ended question to gain insights into the most common mistakes made by employees and end users within their respective organisations. The responses provided were meticulously analysed, and several prominent themes emerged as follows:

Being Susceptible to Phishing (31%): Many employees and end-users displayed susceptibility to phishing attacks. Common mistakes included opening attachments they shouldn't, trusting unauthorised individuals, and clicking on any links or downloading attachments they receive in their emails. Noncompliance with Policies and Training (23%): from the expert point of view, a significant number of employees and end-users demonstrated noncompliance with security policies and training. Mistakes encompassed not being careful, not taking security issues

seriously, not reading the policies properly, and underestimating the importance of organisational security.

Password/Credentials Policy (16%): End-users exhibited poor password management practices, such as writing down passwords and using weak passwords. Additionally, some respondents noted that end-users did not use unique passwords for different accounts and incorporated personal information into their passwords, compromising the security of their accounts.

Data Protection Regulations (15%): Respondents mentioned instances where staff occasionally emailed customer information to their private email accounts to access work-related data at home for completing additional tasks. Moreover, some respondents reported cases where sensitive documents were not stored on secure access-restricted drives, posing potential risks to data security. Instances of data misuse were also highlighted.

Other mistakes (15%): Under this category, additional mistakes were reported. Examples of those mistakes are 1) Unauthorised use of devices, services, or software. 2) Negligence in physical and system security measures, such as not logging off computers and accounts. 3) Some respondents stated that they were not aware of any specific mistakes, and a few noted that employees in their workplace strictly followed and apply security steps and policies. However, there were comments regarding individuals pretending to know everything while lacking the necessary knowledge.

4.7. Feeling Negative and frustrated

In response to the open-ended question about whether any employees or users within their respective organisations expressed difficulties or negative emotions regarding compliance with the organisational security and privacy policy or regarding any security threats, 45% of the security experts stated that such feelings were indeed expressed. Table 5 below provides a breakdown of the specific feelings expressed by the end-users:

Table 5. Feelings Expressed by End-users Regarding Security Compliance and Threats.

Feelings	Count	%
Negative Feelings - not specified	11	44%
Frustration	5	20%
Unhappy & Sad	2	8%
Difficulty	2	8%
Anger	2	8%
Discomfort & being blamed	2	8%
Stressed & overwhelmed	1	4%

Out of the respondents who mentioned negative feelings expressed by employees or users, the most common feeling was "Negative Feelings - not specified," with 44% of respondents who respond to this question reporting this. Frustration was the second most prevalent feeling, mentioned by 20% of the respondents. Other feelings such as "Unhappy & Sad," "Difficulty," "Anger," "Discomfort & Being blamed," and "Stressed & Overwhelmed" were each expressed by 8% of the respondents. Next, we explore the responses from participants about their perceptions. The requirement to complete numerous compliance courses may result in elevated stress levels for the employees or end-users (P10). They stated that "We have a number of compliance courses to complete each month, and they can cause stress." Some individuals within the organisation

perceive the security measure as a violation of their privacy rights. They express a desire for the removal of this security measure. P17: "Yes, they feel negatively that the security measure is a breach of privacy, and they believe it should be removed." New systems and technological changes in the organisation can lead to negative feelings and resistance among some older staff members (p28). P 28: "Yes, some older members of staff, who have become accustomed to working in a specific manner, find it challenging and difficult to adapt to new systems, and they prefer the old way and using paper copies that are accessible to anyone." Employees may feel frustrated with strict password policies and the need to frequently change passwords(p37). P 27: "Frustration is expressed regarding the password policy." A lack of commitment from management to comply with information security policies can lead to negative feelings among employees and potentially result in a disregard for these policies. P 47: "Employees are often influenced by their management, and if there is a lack of commitment in complying with information security policies from the management, the employees may feel negative and are most likely to follow the same practice." Another response by P 43 pertains to the password policy, which requires employees to change their passwords every 90 days. This policy can lead to frustration and difficulty for some individuals, resulting in increased password reset requests and potentially lower overall security as employees struggle to comply. Additionally, they observed IT employees not following security instructions and feeling that the security instructions and policies are overly strict. P 43: "Some employees have trouble with changing their password every 90 days, and they become frustrated because they can't remember their password and need to reset it. I have also observed IT employees who don't follow the security instructions and feel that the security instructions are too strict." Individuals tend to resist and express negative feelings towards any new policy introduced within the organisation. P 52: "They are always complaining about any new policy." One of the experts expressed that the employees in the workplace have a positive attitude towards security policies and do not face any challenges or negative emotions in complying with them. P 8: "No, the employees in my workplace are well-behaved, and they never express negative feelings or encounter difficulties."

4.8. Security and Privacy Threats (Likert Scale)

In the survey, security experts were asked to rate the likelihood of employees engaging in various security and privacy threats on a Likert scale ranging from 1 to 5 (see 3.2). The threats were related to having weak passwords or not changing passwords regularly. Table 6 summarises the responses.

Table 6. Likelihood of End-users Engaging in Security and Privacy Threats: Weak Passwords

Scale	Response	Count	%
5	Very likely	19	35%
4	Likely	14	25%
3	Neutral	10	18%
2	Unlikely	9	16%
1	Very unlikely	3	5%

Table 7. Likelihood of End-users Engaging in Security and Privacy Threats: Ignoring Updates

Scale	Response	Count	%
5	Very likely	16	29%
4	Likely	12	22%
3	Neutral	16	29%
2	Unlikely	8	15%
1	Very unlikely	3	5%

The results show that 35% of the security experts believed that it is "Very likely" for employees to engage in security threats related to weak passwords or not changing passwords regularly. Additionally, 25% considered it "Likely," while 18% were "Neutral" about this possibility. On the other hand, 16% of the respondents considered it "Unlikely," and only 5% believed it to be "Very unlikely." The average/mean rating was 3.67, with a median rating of 4. The standard deviation was 1.26.

Table 7 represents the likelihood of end-users engaging in the security and privacy threat of "Ignoring System and Software Updates. The results show that 29% of the security experts rated it as "Very likely" that end-users may ignore system and software updates. Additionally, 22% considered it "Likely," while another 29% were "Neutral" about this possibility. On the other hand, 15% of the respondents rated it as "Unlikely," and only 5% believed it to be "Very unlikely." The average/mean rating for this threat was 3.55, with a median rating of 4. The standard deviation was 1.21, indicating some variation in the responses but relatively close agreement among the experts.

Figure 4 visually represents the distribution of the responses on the Likert scale, showing the varying levels of likelihood perceived by the security experts for end-users engaging in these security and privacy threats for using weak passwords, and ignoring system and software updates. For the threat of "Not running anti-virus or anti-malware software," the responses showed a range of perceptions among the experts. Approximately 18% of the experts believed it was "Very likely" that some end-users may neglect this crucial security practice, potentially leaving their systems vulnerable to various threats. Another 20% of experts rated it as "Likely," suggesting a significant number of end-users might not consistently run security software. On the other hand, 20% were "Neutral," reflecting some uncertainty in their perceptions. Additionally, 22% considered it "Unlikely," expressing confidence that certain end-users would not skip anti-virus and anti-malware practices. Similarly, 20% rated it as "Very unlikely," indicating a belief that some end-users would adhere to these security measures.

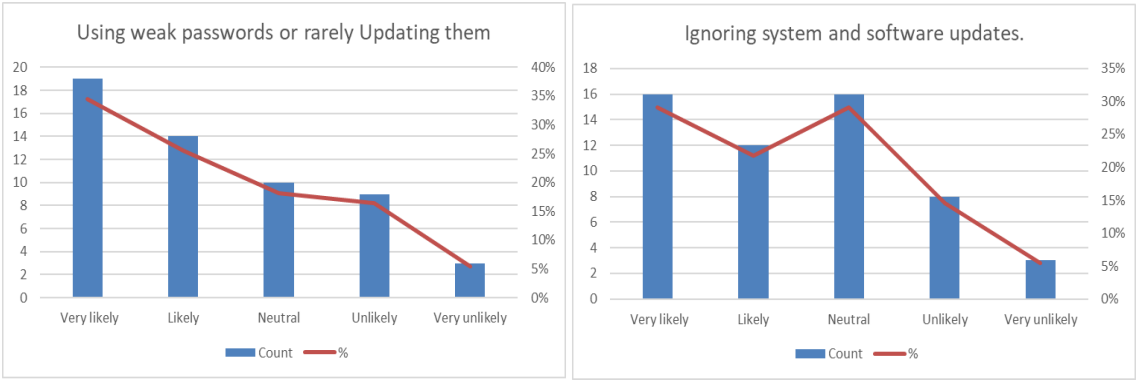

Figure 4. Weak passwords and ignoring updates.

Regarding the threat of "Clicking on links and attachments," a higher level of concern was evident among the experts. Approximately 38% of respondents rated it as "Very likely," indicating a substantial number of end-users might engage in clicking on suspicious links and attachments, potentially exposing themselves to phishing attacks or malware. Another 29% of experts rated it as "Likely," suggesting a considerable portion of end-users might still engage in this risky behaviour despite potential risks. In contrast, 16% were "Neutral," reflecting some uncertainty in their responses. Additionally, 16% rated it as "Unlikely," suggesting a degree of confidence that certain end-users would avoid clicking on suspicious content. Notably, none of the experts believed it was "Very unlikely," indicating that they perceived a non-zero risk of end-users engaging in this behaviour. The average/mean rating for the "Not running anti-virus or anti-malware software" threat was 2.95, with a median rating of 3. For the "Clicking on links and attachments" threat, the average/mean rating was 3.89, with a median rating of 4. The standard deviation for both threats indicate some variance in the expert responses, with the threat of "Not running anti-virus or anti-malware software" showing slightly higher dispersion. Also, it appears that security experts perceive end-users as more likely to engage in the threat of "Clicking on links and attachments" compared to "Not running anti-virus or anti-malware software."

Table 8. Not running anti-virus/malware.

Scale	Response	Count	%
5	Very likely	10	18%
4	Likely	11	20%
3	Neutral	11	20%
2	Unlikely	12	22%
1	Very unlikely	11	20%

Table 9. Clicking on links and attachments.

Scale	Response	Count	%
5	Very likely	21	38%
4	Likely	16	29%
3	Neutral	9	16%
2	Unlikely	9	16%
1	Very unlikely	0	0%

Figure 5 visually represents the likelihood and distribution of end-users engaging in security and privacy threats, specifically susceptibility to phishing by clicking on unknown links and downloading untrusted attachments in emails. It also illustrates the distribution of responses on the Likert scale, indicating the varying levels of likelihood perceived by security experts for end-users not running the necessary antivirus and anti-malware software.

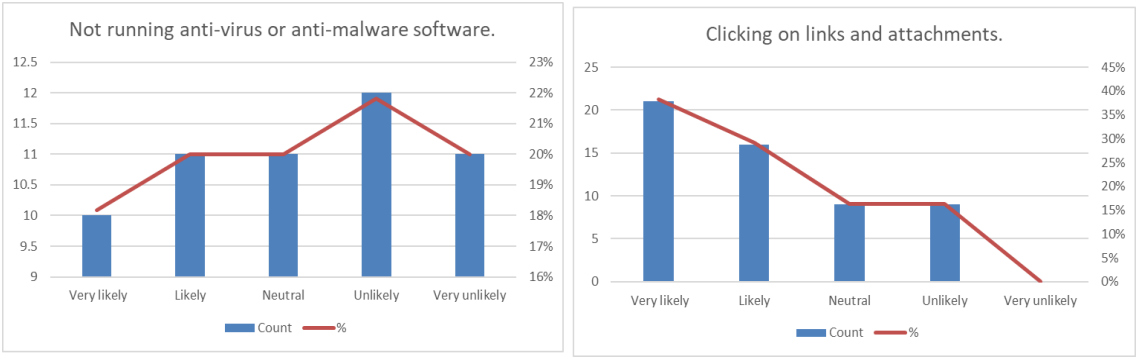

Figure 5. Clicking on links & attachments, & not running anti-virus/malware software.

The likelihood of end-users engaging in the security and privacy threat of ignoring system and software updates is as follows: 29% of the security experts rated it as "Very likely" that end-users would ignore system and software updates. Similarly, 22% considered it "Likely," and another 29% were "Neutral" about this likelihood. On the other hand, 15% of the respondents rated it as "Unlikely," and only 5% believed it to be "Very unlikely," as shown in Table 10 and Figure 6 visually represents the distribution of the responses. The average/mean rating of 3.55, with a median rating of 4, and a standard deviation of 1.21, indicates that while the majority of security experts expressed moderate concern about end-users ignoring system and software updates, there was some variation in their responses, with a subset showing stronger apprehension and others being more neutral in their assessment.

Table 10. Ignoring System & Software Updates

Scale	Response	Count	%
5	Very likely	16	29%
4	Likely	12	22%
3	Neutral	16	29%
2	Unlikely	8	15%
1	Very unlikely	3	5%

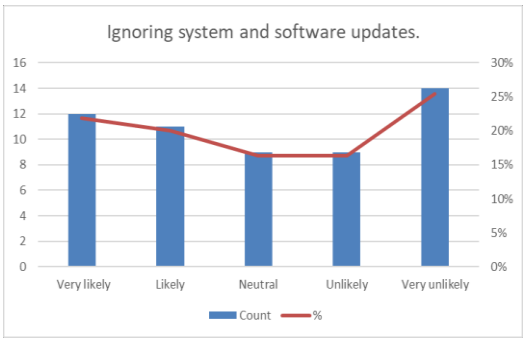

Figure 6. Ignoring System and Software Updates.

5. DISCUSSION

The survey of security experts brought to light several concerning aspects regarding end-users' security practices and perceptions. Although end-users demonstrate a moderate level of concern for privacy and security in their daily work, their lack of adequate knowledge of information security and potential non-compliance with organisational policies pose significant risks. The most prevalent issue observed was their susceptibility to phishing attacks, with 31% falling victim to such threats due to actions like opening suspicious attachments, trusting unauthorised individuals, and clicking on links or downloading attachments from unknown sources in emails. These findings underscore the urgent need for targeted security awareness training and education to empower end-users with a better understanding of information security best practices and to foster a security-conscious culture within the organisation.

To address these vulnerabilities, implementing proactive measures such as simulated phishing exercises, multi-factor authentication, and robust email filtering can substantially reduce the risk of successful phishing attacks and bolster the overall security posture. By taking these steps, organisations can better safeguard sensitive data and systems, minimising the potential impact of security breaches caused by end-users' mistakes. Additionally, the survey highlights concerns about end-users posing potential threats to organisations, such as data breaches and unauthorised access. While these threats were identified, further investigations should be conducted to assess their potential damage and impact.

As Sarkar stated [17], some organisations tend to overlook the threats posed by insider activity due to perceived low damage levels. Therefore, it is essential for organisations to recognise the significance of insider threats and take appropriate measures to prevent and detect such incidents. Regular security assessments and monitoring can aid in identifying potential insider threats and mitigating risks before they escalate. A comprehensive approach that combines user education, technology safeguards, and continuous evaluation is crucial for maintaining robust security and safeguarding the organisation from various threats, both internal and external. The findings from the study indicating that a significant proportion of users within their respective organisations expressed difficulties or negative emotions regarding compliance with the organisational security and privacy policy or concerning security threats have important implications for organisations.

One of the primary implications is that organisations must pay close attention to the user experience and sentiment surrounding their security policies and practices. If a large number of employees or end-users experience negative emotions, such as frustration, it could lead to reduced motivation to comply with security protocols. For instance, strict password policies may be a source of frustration for employees as they can be cumbersome and challenging to remember, potentially resulting in security vulnerabilities. To address this issue, organisations should strive to strike a balance between robust security measures and user-friendly policies. This view is supported by Gulenko et al. [6], whose study found that anger and anger-related emotions, such as frustration and annoyance, are associated with password security, particularly concerning the choice of passwords. This aligns with the aforementioned implication for organisations. When users experience negative emotions due to stringent and burdensome password policies, they might resort to using weaker passwords or adopting unsafe practices to cope with the frustration, thereby compromising security.

Moreover, it is imperative for organisations to proactively seek feedback from all end-users and their employees regarding their experiences with security policies and procedures. This essential step can be accomplished through various means, such as conducting surveys, hosting focus groups, or establishing regular communication channels. By gaining insight into the perspectives

and concerns of end-users, organisations can make well-informed decisions to enhance their security practices and cultivate a more positive and secure work environment.

In essence, taking the time to address user frustrations and negative emotions associated with security compliance or threats becomes paramount in establishing a robust security culture within the organization. By actively engaging with end-users and acknowledging their viewpoints, organisations demonstrate a commitment to their well-being and security, leading to increased trust and cooperation in upholding and strengthening the overall security posture.

6. CONCLUSION

In conclusion, this study aimed to investigate the perceptions of security experts regarding end-users' threat models and cybersecurity practices. The findings highlighted the views of security professionals, with end-users displaying a moderate level of concern about privacy and security, but security experts expressing concerns about their passive approach to organisational policies and lack of knowledge in information security. With phishing identified as the most common threat from the expert perspective, it is essential to conduct further research from the user's perspective. This new study will delve deeper into end-users' experiences and perceptions of security threats, shedding light on the reasons behind their risky behaviours and disregard for security advice. By understanding these perspectives, organisations can design more effective security measures and awareness programs that align with end-users' needs and concerns. Additionally, there is a need for a separate study focused on phishing education and delivery methods. By exploring the most effective ways to educate end-users about phishing risks and implementing suitable delivery methods for security awareness training, organisations can significantly reduce successful phishing attempts. By combining insights from both studies, organisations can develop comprehensive strategies to enhance cybersecurity practices and protect sensitive data effectively. Ultimately, empowering end-users to actively participate in their organisation's security efforts will be critical in maintaining a strong security posture and mitigating potential threats.

REFERENCES

[1] Eirik Albrechtsen. A qualitative study of users' view on information security. Computers & security, 26(4):276–289, 2007.

[2] Eirik Albrechtsen and Jan Hovden. The information security digital divide between information security managers and users. Computers & Security, 28(6):476–490, 2009.

[3] Yves Barlette and Vladislav V Fomin. The adoption of information security management standards: A literature review. Information Resources Management: Concepts, Methodologies, Tools and Applications, pages 69–90, 2010.

[4] Kovila Coopamootoo and Thomas Gross. Why privacy is all but forgotten. Proceedings on Privacy Enhancing Technologies, 2017, 10 2017.

[5] Steven Furnell and Kerry-Lynn Thomson. Recognising and addressing 'security fatigue'. Computer Fraud & Security, 2009(11):7–11, 2009.

[6] Iwan Gulenko. Improving passwords: Influence of emotions on security behaviour. Information Management & Computer Security, 22(2):167–178, 2014.

[7] Tejaswini Herath and H Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems, 18:106–125, 2009.

[8] Khairul Khalil Ishak, Noor Afiza Mat Razali, Anitawati Mohd Lokman, and Kinoshita Toshiyuki. Kansei information security assessment (kisa): characterizing trust as stimuli for user emotional assessment in information security. Indian Journal of Science and Technology, 9(41), 2016.

[9] Mousa Jari. A comprehensive survey of phishing attacks and defences: Human factors, training, and the role of emotions. International Journal of Network Security & Its Applications, 14(5):11–24, September 2022.

[10] Mousa Jari. An overview of phishing victimization: Human factors, training and the role of emotions. Computer Science and Information Technology (CS & IT), 12(13):217–228, July 2022.
[11] Paweł Kobis. Human factor aspects in information security management in the traditional it and cloud computing models. Operations Research and Decisions, 31(1), 2021.
[12] Karen Loch, Houston Carr, and Merrill Warkentin. Threats to information systems: Today's reality, yesterday's understanding. MIS Quarterly, 16:173–186, 06 1992.
[13] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. 2020.
[14] Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, and Ross T. Hightower. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information Management, 51(5):551–567, 2014.
[15] Faisal Quader and Vandana P Janeja. Insights into organizational security readiness: Lessons learned from cyber-attack case studies. Journal of Cybersecurity and Privacy, 1(4):638–659, 2021.
[16] Kuheli Roy Sarkar. Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3):112–133, 2010. Computer Crime - A 2011 Update.
[17] Kuheli Roy Sarkar. Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3):112–133, 2010. Computer Crime - A 2011 Update.
[18] Nurjannatul Jannah Aqilah Md Saad, Mat Razali Noor Afiza, Khairul Khalil Ishak, Nor Asiakin Hasbullah, Norulzahrah Mohd Zainudin, Suzaimah Ramli, Norshahriah Wahab, and Mohd Fahmi Mohamad Amran. Fear as emotion assessment in information security using kansei engineering methodology. In Proceedings of the 7th International Conference on Kansei Engineering and Emotion Research 2018: KEER 2018, 19-22 March 2018, Kuching, Sarawak, Malaysia, pages 654–663. Springer, 2018.
[19] Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. Analysis of end user security behaviors. Computers and Security, 24(2):124–133, March 2005. Funding Information: This research was supported in part by a small grant from the SIOP research foundation and by an award from the National Science Foundation. Neither SIOP nor the National Science Foundation necessarily endorse the results or conclusions of this study.
[20] Merrill Warkentin and Robert Willison. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18(2):101–105, 2009.