Network and Communication Technologies; Vol. 7, No. 1; 2022
ISSN 1927-064X E-ISSN 1927-0658
Published by Canadian Center of Science and Education

An Assessment of Employee Knowledge, Awareness, Attitude towards Organizational Cybersecurity in Cameroon

Fosoh Holiness Nikel[1] & Austin Oguejiofor Amaechi[1]

[1] Department of Information and Communication Technology, The ICT University, Cameroon

Correspondence: Austin Oguejiofor Amaechi, Department of Information and Communication Technology, The ICT University, Cameroon Campus. E-mail: austin.amaechi@ictuniversity.edu.cm

Received: January 10, 2022 Accepted: February 7, 2022 Online Published: February 21, 2022

doi:10.5539/nct.v7n1p1 URL: https://doi.org/10.5539/nct.v7n1p1

Abstract

In our increasingly digitized and interconnected society, people are poorly protected against cyberthreats, with the main reason being user behavior. Human behavior and actions are unpredictable in nature and this make human an important element and enabler of cybersecurity. The objective of the study is promotion of adoption of non-technical countermeasures (such as user awareness) for a comprehensive and holistic way to manage cyber security in organizations in Cameroon. We conducted a subjective study to measure the level of employees' knowledge and general awareness, risky behavior they engage in, and attitude toward various aspects of cybersecurity and cyberthreats to show the need for user education, training, and awareness. For the study described in this paper, a self-report questionnaire was developed and data were collected from 214 participants. The results of a descriptive statistic percentage indicated that less than 50% of respondents have completed or has regular training program. We find that over 61% of the participants do not have sufficient knowledge of their organization cyber security policies. Among other findings, the over 60% of employees' mistakes or violations of security policy are not disciplined or penalized is a demonstration of lack of legal status of cyber-attacks. Cyber resilience in any organization is a responsibility shared by both management and employees. Proactive human management element that can actively hunt for malicious activity and indicators of compromise is recommended.

Keywords: Cameroon, cybersecurity, cybersecurity attitude, cybersecurity awareness, cybersecurity behavior, cybersecurity knowledge

1. Introduction

Cybersecurity has become crucial topic in Cameroon because cyber threats have become a very common occurrence in everyday life. Cybersecurity can be defined as the efforts organizations take to protect and defend their information assets, regardless of the form in which those assets exist, from threats internal and external to the organization (Dalal, Howard, & Bennett. 2021). Cybersecurity threat is becoming more frequent and the threat according to Pollini, Callari, and Tedeschi (2021) include: online fraud, distributed denial of service, drive by download, and social engineering attacks. The changing nature of cybersecurity is exploiting instances of human error or negligence along with system vulnerabilities. Organizational cybersecirity requires more than just the latest technology. All employees of an organization must act together to reduce risk and secure the organization. Research by Badie and Lashkari (2012) categorized the two most important factors affecting the security of computing systems as: (i) human factor and, (ii) organization factor. According to Jeimy and Cano (2019), humans represent a mystery to be deciphered by cybersecurity experts because their behaviors, attitudes, beliefs, rituals and decisions (the general characteristics that define a culture) constitute a little-understood universe for executives and their heads of security. In their study, Dreyer et al (2018) concluded that despite all the technical efforts and security procedures, people are highly likely to expose organizations to vulnerabilities. Insider threat from human behavior is one of the most difficult aspects of cybersecurity to control. Humans are the dominant security decision-makers in the face of cyber-attacks.

Employee's negligence and/or carelessness surrounding information security are the main of data breaches (Kessler et al 2020). Building a culture of cybersecurity within an organization guides employee behavior and increases cyber resilience (Huang & Pearlson, 2019). To be cyber resilient, organizations must have committed well informed, vibrant, sustainability-minded, and engaged employees. As Maalem, Caulkins, and Mohapatra (2020) summarized, employees have to be knowledgeable of the risks, and differentiate desired from undesired behaviors. Cybersecurity is a leading national security challenge facing Cameroon today. Taking into account the high turbulence and considerable pressure on the employees in the country to be effective performers within the current stressful environment, understanding their knowledge and general awareness, risky behavior and attitude towards cybersecurity is considered important. Measurement of cybersecurity awareness and attitude of employees in Cameroon has not received sufficient attention. Cybersecurity culture is difficult to identify, build and quantify. A critical first step in achieving this and enhancing cybersecurity readiness is to understand what the employees currently know and their attitude towards the concept. Every employee must act in ways that keep the organization cybersecure. Accordingly, this study performs an empirical assessment of attitude, knowledge and risk taking behavior towards cybersecurity among selected employees in selected Cameroonian organizations, focusing on the following research questions '*What is the employees' self-reported level of cyber security awareness and knowledge of cyber threats and cybersecurity?, What is the employees' self-reported level of exposure or risk taking behavior towards cybercrime activities?, and What is the employees' self-reported level of attitude towards cybersecurity?'*

The remainder of this paper is organized as follows: Section 2 discusses the related works, and Section 3 presents the methodology used to assess the cybersecurity awareness level. Section 4 describes the analysis results based on the dataset collected in this study. Section 5 concludes the paper.

2. Literature Review

Monitoring cyber security has gained attention lately due to the rise in cyber-attacks. Humans are considered [*rightly or wrongly*] the greatest vulnerability to cybersecurity. This is a position taken by different research studies looked in preparation of this study. Research by Nobles (2018) estimated that 95% of cyber and network attacks are due to human errors and inappropriate behaviors. According to Ahram and Karwowski (2019), human as the end user can be a critical backdoor into the network. As also reasoned by Mc Mahon (2020), a trope that has long dominated cyber security is the idea that humans are the weakest link.

In research by Aamir, Parul, Sangeeta, and Darshana (2020), employees are seen as the most vulnerable links, they need cyber security awareness and training to protect themselves and the company against new evolving cyber-attacks. According to numerous other authors (e.g. Arachchilage & Love, 2014; Hiller & Russell, 2013), employees' information security awareness plays a vital role in mitigating the risk associated with their behavior in organizations. Where employees are not aware of the value of a cybersecurity awareness, then employees were not able to detect any cyber security issue and also not aware of the risks that are associated with their actions. For this reason, it is critical to develop employee cyber security awareness training programs that are capable of improving the cyber security posture.

To study cyber security awareness of employees, Arquilla and Guzdial (2017) proposed a standardized questionnaire focusing on cyber security awareness and behavior of employees as the most appropriate measure. Khalid et al. (2018) noted the effect that the knowledge of cyber security had on the participants' ability to be aware of online risks during the use of the internet.

Egelman and Peer (2015) develop the Security Behavior Intentions Scale (SeBIS). It comprises 16 items and includes four sub-scales addressing attitudes toward password design and applicability, digital device protection, proactive engagement and recognition, and finally software update. Another interesting study was the Human Aspects of Information Security Questionnaire (HAIS-Q), developed by Parsons et al. (2017); the authors uses a scale composed of 63 items, divided into three separated sub-areas that measure knowledge, attitudes and behaviors. This questionnaire intends to evaluate and understand the levels of information security awareness in an organization.

Kennison and Chan-Tin (2020) in their research concluded that individuals' use of insecure cybersecurity behaviors, including the use of weak passwords, is a leading contributor to cybersecurity breaches. The authors stated developing profiles of individual who are likely to become victims of password hacking, phishing scams, and other types of breaches would be useful, as they could be used to identify individuals with the highest likelihood of engaging in insecure cybersecurity behaviors.

In another study, Alotaibi et al. (2016) the authors investigated the cyber security awareness, cyber security practices, incident reporting of the public people in Saudi Arabia. The results shows that the Saudi citizens had a good knowledge of IT, but they have limited awareness of the threats associated with cyber as security practices, cybercrime, and the organizations and government roles in guarantee information safety across the Internet.

In Hadlington (2018) the author measured employee's attitude towards cyber security and general awareness of cybercrime and the types of risky online behaviors they were engage in; in the United Kingdom. The results demonstrated a significant negative correlation between attitudes towards cyber security and risky cyber security behaviors, with more negative attitudes being linked to higher levels of risky behaviors.

The Abdulaziz Alzubaidi (2021) study focuses on measuring the current level of cyber-security awareness in Saudi Arabia, in terms of cyber-security practices, level of awareness, and incident reporting, by means of an online questionnaire. The results showed that 31.7% used public Wi-Fi to access the Internet, 51% used their personal information to create their passwords, 32.5% did not have any idea about phishing attacks, 21.7% had been victim of cybercrimes while only 29.2% of them reported the crime, which reflects their levels of awareness.

Cybersecurity as a public concern is receiving insufficient robust education and attention in Cameroon neither from the government nor from organizations. A 2008 law was one attempt at cyber security and consumer protection in the country but implementation is hindered. Some commentators on the country's efforts have attributed the failure to the country's so-called clientele driven government. According to (Andeme Bikoro et al 2018), in the Cameroonian public administration, young people are more concerned about the inconveniences that could result from the non-use of cyber security measures. A 2020 State Of Application Security in Enterprises study [https://gefona.org/rapports/] findings show that for the majority of organizations, cyber-attacks happen through web application and people are ignorant of most cybersecurity terms such as phishing.

3. Methodology

3.1 Research Selected Controls

Research design aims to fulfill the objectives of the research and find the solutions for research questions. To determine which cybersecurity controls and associated cyberthreats should be included in the questionnaire, the research adopted questions from previous questions raised by Pew Research Center's cyber security quiz (Olmstead & Smith, 2017), the ISO 27002 standard (ISO27002, 2017), Security Behaviors Intentions Scale [SeBIS] (Egelman & Peer, 2015), Risky cybersecurity behaviors scale (RScB - partly based on the SeBIS developed by Egelman & Peer, 2015), Aljohani and Elfadil (2020) and Attitudes towards cybersecurity and cybercrime in business (ATC-IB) (Hadlington, 2018) and (Elbelekia, 2020).. Specific controls were selected according to the following criteria. The control *1) can be implemented at an individual level, 2) is not very context-dependent, and 3) has a clear, unambiguous description.* As such, a total of 52 controls were shortlisted. After expert interviews (n = 3), 45 controls remained

3.2 Data Collection

Data was collected through a self-reported paper-based questionnaire. Self-reported measures are subject to a range of well-known biases and demand effects (Dimoka, Pavlou, & Davis, 2011), including the social desirability bias. Social desirability bias is the tendency of individuals to portray themselves and their behavior in ways that are more socially acceptable. Measuring was conducted between March and May 2021. The questionnaire design followed closely Harrell and Bradley (2009) semi structured interviews guide. Attempt was made to avoid high-tech jargon rather using plain term to better match employee's background IT knowledge. Their consent was important for us. Participants were informed that the topic of the questionnaire was 'the human side of cybersecurity', that completing the questionnaire would take approximately 30 minutes, and that all data would be processed anonymously. It was also explained that the questionnaire was about the participant's perception and opinion relating to cybersecurity. To discourage people from giving answers based on perceived social desirability, respondents were instructed to choose the option 'I don't know' if they did not know the answer or choose the option 'not applicable or do not understand' if the participants had never used the control in question.

This study used purposive sampling. An identified and willing manager at a higher level helped to distribute the questionnaire to her or his subordinates. Participants are from both private and public healthcare, education, telecommunication environments. A total of 214 valid responses were used in the final interpretation. As suggested by Osborne and Costello (2004), there are no absolute rules for the sample size needed to validate a questionnaire. However based on the Gorusch's respondent-to-item ratio ranged from 5:1 (i.e., fifty respondents for a 10-item questionnaire) (Gorusch, 1983) analysis, this research's 214 participants are judged reasonable because of the ongoing covid-19 pandemic and Anglophone crisis in Cameroon which has affected numerous data collection projects. Below are the results from the analysis, frequency tables, statistics and charts.

4. Results Analysis & Discussion

4.1 Demographic Analysis

The final dataset included 214 participants, comprising of 128 Males and 86 Females. For the sample of 214 participants, the participants had an age range of 18–61, (18-24 = 17%, 25-34 = 33%, 35-44 = 12%, 45-54 = 22%, 55-64 = 13%, 61+ = 3%). The distribution of the participants shows the majority of respondents (45%) being full-time employees, (25%) are graduate students, and the remainder (30%) being part-time employees.

As presented in Table 1, the participants in the study were employees and graduate students of private education institution, private hospitals, public IT and Communication institution [government ministry and telecommunications], public financial services provider, public education institutions and collection of employees that made decision not to disclose their sector but whom we classified as public. In total, there were [66] 30.84% of respondents from the private sector and [148] 69.16% of respondents from the public sector (Table 1).

Table 1. The sample across the combined private and public organizations

S. No.	**Type of Institution**		**Sample Size [n]**	**Percent [%]**
1	Private Education		45	21. 03
2	Public Education		68	31.78
3	Public IT & Comm		25	11.68
4	Public banking and insurance		12	5.61
5	Private Hospital		21	9.81
6	None Specified		43	20. 09
Total			214	100. 00
Type of Organizations	Frequency [n]	Percent [%]	Valid Percent [%]	Cum Percent [%]
Private	66	30.84	30.84	30.84
Public	148	69.16	69.16	100. 00
Total	214	100. 00	100. 00	

The answers for education level were distributed as follows: Graduate (38.32%) or high schools & diplomas (35.05%), and Post-Graduate (26.63%) [see Table 2], with total work experience of 1–5 years (16.9%), 6–10 years (27.0%), 11–15 years (13.4%), 16–20 years (28.8%), or more than 20 years (13.9%).

Table 2. Level of Education

Item	**Frequency [n]**	**Percent [%]**	**Valid Percent [%]**	**Cum Percent [%]**
High School Diploma	75	35.05	35.05	35.05
Bachelors	82	38.32	38.32	73.37
Masters	46	21.49	21.49	94.86
PhD	11	5.14	5.14	100.00
Total	214	100.0	100.00	

Another part of the demographic questions evaluated how often the respondents access the Internet. The answers were distributed into 68 (31.78%) accessing the Internet frequently, 112 (54.67%) once or twice a day, 11 (5.14%) accessing the Internet less frequently such as once a week, while 18 (8.41%) did not answer the question. On the question about which devices they access their networked systems and internet regularly, smartphone devices came first with a percentage of 52.4%, laptops (28.41%) while 21.65% was distributed among desktops, and tablets.

Another interesting question on this part is regarding the purpose for accessing the Internet (the user had the ability to select one or more options), and concluded that utilizing the Internet for education, social networking, online services, and communication was the most frequently selected choice, with 80 subjects (37.38%), government services and professional reasons had the lowest percentage of answers, with less than 16.36%, and the remaining percentage was distributed among education or information seeking, social media, online services, entertainment (e.g. playing games) and communication (e.g. email, Zoom, etc.).

4.2 Measuring Employee's Cybersecurity Concepts, Knowledge and Awareness

According to Bloom et al (1956), knowledge can be defined as 'remembering specific and general issues, remembering methods or processes or remembering patterns, structures or contexts'. Knowledge Rasmussen said is a precondition for adopting correct behavior in a given situation (Rasmussen, 1983). In the field of cybersecurity this involves recognizing and knowing about cyberthreats (Ben-Asher & Gonzalez, 2015), understanding their potential impact, and being conscious of the measures that can be taken against them (Siponen, 2001; Du Plessis & Von Solms, 2002). In another view, cybersecurity research, knowledge can be measured using an option where a statement is given and the respondent has to evaluate whether this statement is correct or not. In this type of question, the answer options are the same for each question, for example 'true/false' (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013). These types of statement were used in the research detailed here. Also measured is the respondent's awareness. The difference is that knowledge consists of knowing the facts, but awareness means being cautious because of the facts. Knowledge also refers to the detailed understanding of cyber security, while awareness warrants taking necessary actions to prevent cyber-attacks without needing that deep understanding. However, assessing the knowledge of the participant is also a significant means of measuring awareness. Table 3, which is a numerical representation, shows the results of all 214 participants, percent and our analysis/comments of their answer.

Table 3. Cyber Security Concepts Knowledge and Awareness

Questions	**Yes %**	**No %**	**Don't know or Understand %**	**Researcher Analysis**
Do you have prior knowledge about cybercrimes [*a crime where a computer is the object of the crime or is used as a tool to commit an offense*]?	55.14	41.12	3. 74	There is good awareness and knowledge of cybercrime. Cyber security education has two elements: first people need to become aware of the need to take precautions, and then teachers need to impart the skills they require to take the required precautions. Each must be cultivated to be of high priority in Cameroon
Do you have sufficient information about cyber security policies and procedures	23.30	73.43	3. 27	Cyber security policies provide direction upon which a control framework can be built to secure the organization against external and internal threats. Low awareness is obvious here. Communication around cyber security must be improved
Does government/ organization supervise the Internet?	88.32	11.68	00. 00	Government have demonstrated the fact that it controls and supervises the information over the cloud with actions over the ongoing Anglophone crisis
Are multi-factor authentication, auto-updates and regular patches practiced in your organization	46.73	33.18	20. 09	All the listed factors are critical to secure connectivity. At worst, organizations should encourage employees to set up consultations with knowledgeable staff if they have questions about their security apparatus.
Is your office computer connected to the Internet?	47.66	52.34	00. 00	When onsite in the office*,* respondent's computer is connected *to the* local area network of their organization. Even with a marginal difference between Yes and No, employees must be made aware to assume that everything they do on their work computer is being watched and tracked
Is the firewall on your computer enabled?	33.65	31.76	34.59	A high percent of *Don't Know or Understand* is reflection of a need for more cyber security awareness – educational approach
Does anyone have your computer password or is it written where someone can see it?	69.16	30.84	00. 00	The results indicate suspicion and a high lack of awareness and indifference to nearby or internal risks. Cyber security education is as essential
Is anti-virus currently installed in your computer	49.53	5.61	44.86	The results indicate suspicion and a high lack of awareness and indifference to nearby or internal risks. A score of 44.86% of Don't Understand probably means not understanding what anti-virus represents. Cyber security education is as essential.
Do you connect your mobile device with public networks?	46.7	53.3	00. 00	Although availability of connection via Wi-Fi networks is acknowledged. How much the respondents knows of the great difference between the secured and unsecured Wi-Fi networks is not known
You have been cyber bullied?	15.42	72.90	11.68	The results indicate that cyberbullying is not restricted to children only. Cyberbullying has been deemed a public health problem and proper education of employees on its recognition and prevention are needed
Have you cyber bullied someone else?	27.10	61.22	11.68	The results indicate that for you to know if you have been bullied or you are bullying someone else requires an understanding of what cyberbullying is.

Have you use the same password for everything that needs a password	59.81	40.19	00. 00	Password reuse is an understandable human behavior, but organizations need to make good password hygiene a priority to ensure that passwords are not a weak link in their security posture. A score of 59.8% Yes score shows a high level of individuals that can be compromised as a consequence of poor cyber security practices
Do you know of the practice of sending fraudulent communications that appear to come from a reputable source	41.12	14. 02	44.86	The score of 44.86% is clear indication of employees not understanding what phishing is and what dangers to organizational cyber security this type of social engineering attack represent. More and better cyber security education is the solution; forewarned is forearmed
We have regular, ongoing or completed training in the area of cyber security?	37.38	59.81	2. 81	It is clear that most of the participants will benefit from a training program aimed at heightening security awareness within their organization.
Do you know if punishment for failing to comply with security policies are same for everyone	15.89	14.95	69.16	A high percent of *Don't Know or Understand* is reflection of a need deep for a messaging of the cyber security policies. Severity of punishment if any should have procedural fairness with regard to rules and regulations

Do you frequently delay in or even not at all installing software updates			
I think it is updated automatically %	I know it is updated automatically %	I updated mine manually %	Don't know or Understand %
50.47	27.10	14.49	7.94

Research by Moustafa, Bello and Maurushat (2021) said that complying with security policies is one key behavior to protect computer and network systems. A score of 73.43% of the total participants not having *sufficient information about their cyber security policies and procedures and* 69.16% *with no knowledge or understanding if punishment for failing to comply with security policies are same for everyone* in their organization is a profound matter of concern**.** The results also indicate that 50.47% of the participants *think that software is updated automatically.* This is a serious human error and according to (Rajivan, Aharonov-Majar, & Gonzalez, 2020), it is one common error underlying cybersecurity behaviors. Research by San Nicolas, Schooley, and Spears (2014) found that the best outcome to increase compliance with security policy is to provide opportunity to employees to participate in the development of the information security awareness and training programs. This is one strong option available to organizations in Cameroon; there is not much available evidence that organizations are strongly investing in such practices.

4.3 Understanding Employees Exposure & Risk taking behaviors to Cybersecurity Activities

Risk is generally defined as engaging in a behavior with an uncertain outcome, usually for the benefit of gaining more (Saleme et al., 2018). According to King et al., computer system users who are high in risk taking may be more likely to fall victims to cybercrimes (Henshel et al., 2015; King et al., 2018). According to Greitzer and Hohimer (2011) the only way to be proactive in the cyber domain is to take behavioral data into account. Human can be tricked and manipulated, are sometimes ignorant, often make mistakes, and suffer lapses in judgment, therefore understanding employees' feedback on their exposure to activities that constitute cybercrimes should increase security behaviors [see Table 4].

Table 4. Measuring Exposure to Activities that constitute cybercrimes

Survey Question	Importance - Participant's answers		
	Always%	Never%	Don't Know Sometimes%
Do you normally share passwords with friends and family	31.76	45.79	22.45
Do you always ignore security warnings?	45.79	47.20	7. 01
I manually lock my computer screen when I step away from it	24.30	67.29	8.41
Do you commonly establish trusting online relationship with strangers	62.08	23.36	14.56
Do you think that you have been exposed to a materials that promotes hatred	29.91	19.63	50.46
Do you feel trusted in your organization to obey rules and regulations	19.63	50.46	29.91
Does your passwords based on personal information	54.21	23.36	22.43
Do you distribute materials that promotes hatred	18.69	54.21	27.1
DO you respond to messages announcing contests involving winning huge gifts	36.45	2.34	61.21
I use a password/passcode to unlock my laptop or tablet	30.84	57. 01	12.15
Do you always open an attachment from a known or unknown source	36.45	30.84	32.71

People will continue to be primary targets of cyber-attack. Phishing remain a major threat for many organizations. The results from this study are mixed. About 36% of the subjects clicked on the link or opens an attachment from a known or unknown source and 31% always gladly gave their password. Phishing is a serious global issue. Data released from the U.K.'s Information Commissioner's Office (ICO) cyber breach data from 2017 – 2019 shows the majority of data breaches began with a phishing attack. Every day 156 million phishing emails are sent and 16 million of these get through security filters into inboxes. What's more, 8 million phishing emails are opened and 800,000 malicious links in those emails are clicked.

With 57% of the participants admitting to *not using password/passcode to unlock their laptop* is a significant lack of non-compliance of cybersecurity policy if well defined. Developing in-depth knowledge and awareness among every employee through continual robust education would again make the difference on the numbers recorded. Research by Moustafa et al (2021) said, a lack of complying with security policies is risky as the benefit is not doing any additional work, such as software update (which is rewarding), but the risk is falling victim to cybercrimes and phishing.

4.4 Measuring Employees' Attitudes towards Cyber security and Cybercrime

According to Dwyer (1993), despite some objections, a fast and user-friendly way to measure attitudes in a larger group is through self-reporting based on a series of statements in a questionnaire. Questionnaire is the best method to measure attitude effectively and it is what is reported here. The main problem with self-reporting is that there is a chance that people will provide an answer motivated by social desirability. To prevent respondents from giving socially desirable answers, the instructions emphasize that the study gains most from sincere answers. To allow for the possibility that people may not have an opinion on a given question, the option 'not applicable/no opinion' was added. Answers could be provided along a five-point Likert scale ranging from 'Strongly disagree' (1) to 'Strongly agree' (5), and also the options 'I don't know' and 'not applicable'. The responses to the items are presented in Table 5.

Table 5. Attitudes towards Cyber security and Cybercrime

Survey Question	**Importance - Participant's answers**				
	Strongly Agree%	Agree%	Disagree%	Strongly Disagree%	not applicable /I don't know
I think that the management of my organization fully considers risks in determining the best course of action.	8.41	31.78	23.36	31.78	4.67
I think that it's the management that has the responsibility to ensure our organization is protected from cybercrime	30.84	41.12	27.10	0.94	00.00
I am aware of my role in keeping the company protected from potential cybercriminals.	21.03	45.79	30.84	2.34	00.00
I believe everyone in the company has a role to play in protecting against threats from cybercriminals.	47.20	44.86	5.10	2.84	00.00
I can help protect my organization from cybercrime	16.82	56.54	26.17	0.47	00.00
I do not feel that IT security is a priority within my organization.	7.94	45.33	36.45	10.28	00.00
I think computer systems already provide the protection an organization needs.	8.41	28.04	41.12	22.43	00.00
The cybercriminals maybe more knowledgeable than the people protecting our systems.	4.21	70.56	10.28	14.95	00.00
I think more could be done to communicate the risks from cybercrime to employees.	33.18	29.91	22.89	14.02	00.00
I don't think that reporting a cyber-attack on the company is my responsibility.	30.84	45.79	21.03	2.34	00.00
I don't pay attention to company material about the threats from cybercrime.	8.88	28.97	35.05	27.10	00.00
I am confident that I would be able to spot the signs of a cyber-attack.	28.50	33.64	22.43	15.43	00.00
I intend to report a cyber-security incident if it happens to me, for example ransomware, identity theft and/or a data breach.	7.00	16.36	52.33	18.69	5.61
I think that cybercriminals only target a company when there is a substantial financial gain.	41.59	39.72	8.41	7.01	3.27
I believe only large companies are targeted by hackers and cybercriminals.	41.59	42.99	8.41	7.01	00.00
I think cyber security is a public safety issue that should be handled by a wider authority.	14.02	63.55	16.82	3.74	1.87
In my organization, end user mistakes or violations are disciplined or penalized	21.03	45.79	30.84	2.34	00.00

The results indicate highlight a failure to fully understand the risks of cyber security both in mindset and in practice by the respondents. People also had a positive attitude towards cybersecurity questions asked. Complying with security policies is one key behavior to protect computer and network systems. Many of the employees do not see cyber security as their primary concern. For instance on the question: *I don't think that reporting a cyber-attack on the company is my responsibility [30.84% of the participants strongly agree* with the comment and *Agree - 45.79%* of them *Agree].* This is an indication that many of the Cameroon employees are devolving a responsibility for their cyber security to technical interventions and senior management. On the statement: *I think that it's the management that has the responsibility to ensure our organization is protected from cybercrime; 30.84% of the participants strongly agree and 41.12% said Agree]***.** A total of *63.55%* of the employees *Agree* to the statement that *I think cyber security is a public safety issue that should be handled by a wider authority.* This would nicely fit into a risk compensation framework (Hadlington & Parsons, 2017), where an individual who believes they are protected by technical interventions provided by their host organization may in turn engage in more risky cyber security behaviors. Research by Maqbool, Aggarwal, Pammi, and Dutt (2020) had argued that penalizing individuals not in compliance with security policies should increase security behaviors.

5. Conclusion

Organizations and their employees made decisions that influenced attitudes, beliefs and values around cybersecurity. For cybersecurity resilience, organizations in Cameroon must act to minimize human behaviors that create cybersecurity vulnerability and increase behaviors that protect their organizations. Creating and communicating cybersecurity awareness and security best practices culture is imperative in the fight against malicious intent. Protection and defense of analogue and digital electronic devices, their communications channels, their processing and control logic and algorithms stands better to improve in Cameroon when organizations begin to proactively adopt a user-centered perspective. According to Pollini et al. (2021), better cyber-security culture does not always correspond with more rule compliant behavior; conflicts among cybersecurity rules and procedures may even trigger human vulnerabilities.

The human factor is the underlying reason why many attacks on institutions systems are successful because the uninformed user is the weakest link targeted by cyber criminals but yet people are the most important element of a cybersecurity solution strategy. This paper recommends that organization in Cameroon invest in cybersecurity education for her employees focusing on communication, engagement, collaboration, and social engineering. We also recommend prioritization of creation and implementation of a cybersecurity strategy, on which policies and other security efforts could be based. A wider study of cyber security culture (attitudes, knowledge, assumptions, norms and values of the workforce of an organization with respect to cyber security) in many Cameroon based IT users is suggested. Developing profiles of employees who are likely to become victims of password hacking, phishing scams and other types of breaches by organizations is advocated. This would be useful as such profiles could be used to identify individuals with the highest likelihood of engaging in insecure cybersecurity behaviors. Organizations must deploy a variety of cybersecurity measures and techniques to match the complexity of a blended or single attack. It should be noted that the opinions of stakeholders from the North West Region, sampled for this study do not represent the entire country. Due to limited resources and time constraints, we were unable to sample all 10 regions in the country. Thus, a major limitation of this study is the fact that we interviewed a small convenient sample in one Region.

References

Aamir, H. K., Parul, B. S., Sangeeta, D., & Darshana, P. (2020). SartCyber Security Awareness Measurement Model (APAT). *International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC).* https://doi.org//10.1109/PARC49193.2020.236614

Ahram, T., & Karwowski, W. (2019). Advances in Human Factors in Cybersecurity In: AHFE: *International Conference on Applied Human Factors and Ergonomics,* 66-96. Springer, Washington D.C. https://doi.org/10.4018/978-1-5225-9742-1.ch003

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior,* 38, 304-312. https://doi.org/10.1016/j.chb.2014.05.046

Arquilla, J., & Guzdial, M. (2017). Crafting a national cyberdefense, and preparing to support computational literacy. *Communications of the ACM*, 60(4), 10-11. https://doi.org/10.1145/3048379

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia, *2016 11th International Conference for Internet Technology and Secured Transactions* (ICITST), Dec. (2016). https://doi.org/10.1109/ICITST.2016.7856687

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk

Management based on AHP. *Journal of Basic and Applied Scientific Research, 2*(9), 9331-9347.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48,* 51-61. https://doi.org/10.1016/j.chb.2015.01.039

Bloom, B., Engelhart, M., Furst, E., Hill, W., & Krathwohl, D. (1956). *Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook 1: Cognitive Domain* (New York: David McKay Company, 1956), 1.

Bikoro, A. D. M.; Samuel, F. W., & Jean, R. K. K. (2018). Determinants of Cyber Security Use and Behavioral Intention: Case of the Cameroonian Public Administration. Á. Rocha et al. (Eds.), *WorldCIST'18 2018, AISC 746* (pp. 1087-1096), 2018. https://doi.org/10.1007/978-3-319-77712-2_104

Boraine, P. A., & Leno, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC), 35*(1), 87-100. https://doi.org/10.18278/ijc.7.1.1

Dalal, R. S., Howard, D. J., & Bennett, R. J. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *J Bus Psychol* (2021). https://doi.org/10.1007/s10869-021-09732-9

Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). Research commentary—NeuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research, 22*(4), 687-702. https://doi.org/10.1287/isre.1100.0284

Dreyer, P., Jones, K., Klima, J., Oberholtzer, A., Strong, J. Welburn, Z., & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk: Methodology and Examples. *Rand Corporation,* 2018. Retrieved from https://www.rand.org/pubs/research_reports/RR2299.html

Dwyer, E. (1993). Attitude Scale Construction: A Review of the literature. *ERIC Institute of Education Sciences, no. ED359201* (1993), 1-48. Retrieved from https://eric.ed.gov/?id=ED 359201

Elbelekia, M. S. S. (2020). *Attitudes of employees towards cybersecurity* (Unpublished master's thesis). Near East University, Nicosia.

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proc ACM CHI'15 Conf Hum Factors Comput Syst [Internet], 1*, 2873-2782.

Gorusch, R. L. (1983). *Factor Analysis* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Greitzer, F. L., & Hohimer, R. E. (2011) Modeling Human Behavior to Anticipate Insider Attacks. *J Strat Secur 4*(2), 25-48. https://doi.org/10.5038/1944-0472.4.2.2. http://scholarcommons.usf.edu/jss/vol4/iss2/3/

Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. https://doi.org/10.5281/zenodo.1467909

Harrell, M., & Bradley, M. (2009). Data collection methods: semi-structured interviews and focus groups. *RAND Corporation* 2009, 1-146.

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29*(3), 236-245. https://doi.org/10.1016/j.clsr.2013.03.003

Huang, K., & Pearlson, K. (2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. https://doi.org/10.24251/HICSS.2019.769

Kennison, M. S., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Front. Psychol., 4*. https://doi.org/10.3389/fpsyg.2020.546546

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cybersecurity. *An International Journal of Engineering & Technology*, *7*(4), 11-14. https://doi.org/10.15345/iojes.2019.02.004

Jeimy, J. & Cano, M. (2019). The Human Factor in Information Security. *ISACA Journal*, 9. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security

ISO27002 (2017). *NEN-EN-ISO/IEC 27002: Information technology - Security techniques – Code of practice for information security controls*. 2017 https://www.iso.org/standard/54533.html

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., Spector, P. E., Kessler, S. R., Pindek, S., … Spector, P. E.

(2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Inform. J., 26*, 461-473. https://doi.org/10.1177/1460458219832048

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Front. Psychol.* 9:39. https://doi.org/10.3389/fpsyg.2018.00039

Maalem Lahcen, R. A., Caulkins, B., & Mohapatra, R. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecur, 3*, 10 (2020). https://doi.org/10.1186/s42400-020-00050-w

Maqbool, Z., Aggarwal, P., Pammi, V. S. C., & Dutt, V. (2020). Cyber security: effects of penalizing defenders in cyber-security games via experimentation and computational modeling. *Front. Psychol., 11*, 11. https://doi.org/10.3389/fpsyg.2020.00011

McCrohan, K., Engel, K., & Harvey, J. (2010). Influence of awareness and training on cybersecurity. *Journal of Internet Commerce, 9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

McMahon, C. (2020). In Defence of the Human Factor. *Front. Psychol., 11*, 1390. https://doi.org/10.3389/fpsyg.2020.01390

Moustafa, A. A., Bello, A. & Maurushat A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Front. Psychol., 12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica, 9*, 71-88. https://doi.org/10.2478/hjbpa-2018-0024

Olmstead, K., & Smith, A. (2017). *What Americans Know About Cybersecurity.* Retrieved from http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity

Osborne, J. W., & Costello, A. B. (2004). Sample size and subject to item ratio in principal components analysis. *Pract Assess Res Eval, 9*, 8. https://doi.org/10.7275/ktzq-jq66

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Comput Secur, 66*, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Pattinson, M, Butavicius, M, & Jerram, C. (2013). An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations. *Proceedings of the European Information Security Multi-Conference (EISMC 2013),* 34-44.

Pollini, A., Callari, T. C., & Tedeschi, A. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn Tech Work*. https://doi.org/10.1007/s10111-021-00683-y

Saleme, D. M., Kluwe-Schiavon, B., Soliman, A., Misiak, B., Frydecka, D., & Moustafa, A. A. (2018). Factors underlying risk taking in heroin-dependent individuals: Feedback processing and environmental contingencies. *Behav. Brain Res., 350*, 23-30. https://doi.org/10.1016/j.bbr.2018.04.052

San Nicolas-Rocca, T., Schooley, B., & Spears, J. L. (2014). Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance. *Proceedings of the 47th Annual Hawaii International Conference on System Sciences,* (pp. 3432-3441). https://doi.org/10.1109/HICSS.2014.427

Siponen, M. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society, 31*(2), 24-29. https://doi.org/10.1145/503345.503348

Rajivan, P., Aharonov-Majar, E., & Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *Journal of Cybersecurity, 6*(1), tyaa002. https://doi.org/10.1093/cybsec/tyaa002

Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man, & Cybernetics, SMC-13*(3), 257-266. https://doi.org/10.1109/TSMC.1983.6313160

Copyrights