IJAER/July-August 2023/Volume-12/Issue-4 ISSN: 2278-9677

International Journal of Arts & Education Research

TO ENHANCE CYBERSECURITY AWARENESS AND PROTECT THEIR INFORMATION SYSTEMS AND DATA.

Rahul Saini
Research Scholar
Computer Science
CMJ University Meghalaya

Ajay Agarwal
Guide
Computer Science
CMJ University Meghalaya

ABSTRACT

Data and systems within organisations are vulnerable to breaches because of inadequate security education, training, and awareness (SETA) initiatives The purpose of this qualitative multiple case research was to examine the tactics used by IT chiefs. When it comes to the hospitality sector, efficient implement SETA, drawing on social cognitive theory as its theoretical foundation. Based on the current trends, Cyber-attacks disproportionately affect firms with less than 500 employees [SMEs]. Previous research has shown that insufficient funding in cyber security by SMEs is the main cause of this occurrence. Finally, the mental component elucidates the ways in which negative emotions, such as guilt and shame, influence the cyber security decision-making and behaviour of IT personnel ways that are unproductive on the job.

keywords: Cybersecurity, Awareness, Protect, Information and Education

Introduction

Cybersecurity has evolved over the years, keep in mind that the phrase the Computer Science and Telecommunications Board's 1991 paper " Ensuring the Security of Computers in the Digital Era " served as its foundation). Based on the study findings, cybersecurity is "the safeguarding of systems themselves and the protection against unwanted disclosure, modification, or destruction of data in a system". There are three distinct varieties of CS, as stated by Nissenbaum (2005). The first is protecting critical societal infrastructures—including financial institutions, healthcare providers, news outlets, and government agencies—from malicious, antisocial, and disruptive online messages and groups. Secondly, avoiding the complete or partial deactivation of ISs.

Still, we need to define the first word of the phrase "cyber security" as it is a two-word phrase. One common definition of a "cyber" environment is one that has strong ties to the Internet (Hunton, 2009). Guariniello and DeLaurentis (2014) provide a definition of the word "cyberspace" as "the interdependent network of information technology infrastructures and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." A further addition supplementing the definition with the term "space" makes it more thorough. A "cyber" space is one that can be "moved through" and reached via an online network. may be deduced from the reasons outlined before. As an alternative, Ng, Kankanhalli, and Xu (2009) define "security" as defensive technology, but the term may usually mean protection against anything. But in the context of this research, "security" means precautions.

The offered meanings lead one to believe that the protections are referred to as "cyber security" put in place for areas that are accessible over the Internet in this particular research. Organizational, technical, and psychological factors are all taken into account in this research on cyber security measures (Julisch, 2013). In this study, the organizational aspect is defined as decisions about security priorities and roles. Regulations pertaining to cyber defence on a global, regional, and European Union scale, written policies and their implementation, prioritization of information value, authorization to access systems, measures to prevent and analyses cyber-attacks, and the process of informing stakeholders about these incidents are all part of this aspect (Julisch, 2013). System backups, analysis of antivirus threats, sophisticated password rules, internet firewall rules, and inventory lists of hardware and software, and system logs are all examples of cyber technology security tools that are part of this study's technical side. From a psychological perspective, it is important to differentiate between IT workers' propensity to feel guilty and shame and to analyses the correlation between these emotions and their levels of counterproductive work behaviour.

Hathaway et al. (2012) states that cyber-attacks primarily aim at computer networks connected to the Internet. However, it should be noted that in addition to desktop and laptop computers, the ultimate target could also include devices command any item that can be accessible by computer networks, including elevators, traffic signals, cell phones, washing machines, televisions and more. Cyberattacks were formerly reserved for a select group of extremely intelligent computer programmers known as "hackers"; however, with the development of more accessible tools, anyone with an internet connection and a desire to launch such an attack can do it (Potts, 2012).

Literature Review

Lesko (2019) evaluated the significance of the practical need for cyber security program institutions to establish a collaborative learning area or centre. A cyber-security learning area should have certain features as cyber security education is essential for the general public. The article outlines the essential characteristics and final layout of every particular learning environment. Among these goals are the promotion of extracurricular cyber security activities, the reduction of the computer footprint, the optimisation of advances in wireless and IoT access, and the accommodation of diverse learning styles. Students will have an easier time navigating the cyber-security classroom according to the proposed physical arrangement in this article. Online, hands-on experience and personalized learning are prioritized. Theoretically, these designs for group study rooms should help students better grasp internet safety by playing to their spatial awareness.

Barbosa et al. (2023) compared the reactions of kids in Brazil and Europe to various internet dangers. In order to do this, we gathered information using open-ended questions. In this research, the hazards found in online spaces were categorized into three main areas: content, contact, and behaviour. Roughly half of the youngsters surveyed in Europe (58%) and Brazil (49%), respectively, expressed extreme worry about content-related hazards. There is a larger disparity between the two groups with regard to conduct-related hazards (19% vs. 30%), while both samples report fewer incidents involving contact-related threats (13% vs. 12%). The study's findings provided policymakers with evidence and made it possible to compare the results internationally.

Cyberbullying and other (2023) sexually explicit content may be difficult for people to grasp, but books published by Giant, E-Safety for the i-Generation: Fighting the Abuse and Misuse of Technology in Educational Institutions, examines and gives practical resources to assist people understand these concerns. As an added bonus, the book teaches readers everything about e-safety, how to make it a school-wide priority, how to get parents and teachers involved, and what to do in the event of an incident. It also includes a comprehensive e-safety paradigm to follow when implementing an e-safety policy. Activities are provided with picture handouts that may be copied to educate young people how to be safe while using the internet.

Cabero-Almenara et al. (2020) assessed the seven competency models with the most global use. A professional's opinion is sought for in making the assessment. In all, 412 persons took part in the research, with 155 being specialists and 257 being laypeople. The results of the expert evaluation were in, and Teachers' Digital Competence: A European Framework for Success was proclaimed the winner. Learn Dig-Comp is the gold standard and suitable reference, with INTEF following closely after.

Researchers Saxena et al. (2022) looked at cyber-security problems in India and provided a variety of approaches to educate elementary school students. This paper primarily aims to discuss the relevance of combating potential cyberattacks in schools. The report emphasizes the significance of educators' ability to promote good online habits as a foundation for students' IT skill development. As a result, building instructors' skills and raising their level of awareness would support technological training. The report concludes by stressing the need of educating all industries on cyber security, and the need for an all-encompassing strategy and curriculum on cyber-defense.

RESEARCH METHODOLOGY

Here we provide the research strategy, methodology, and interpretative philosophical approach to qualitative research. Following that, everything from data collection to respondent selection to analytic procedures is laid out in great detail. The potential for diverse cyber security measures to be designed for use in small and medium-sized enterprises (SMEs), where IT professionals are asked interview questions that are based on their work experience and knowledge, complexity to the issue that this research introduces. In qualitative research, participants' experiences and insights may be explored and the data was gathered in an abundant manner (McHugh et al., 2019). Qualitative research avoids making broad generalizations and instead focusses on specific populations better when looking at occurrences in a specific context (Singer et al., 2019). In this qualitative investigation, the researchers opted for a methodology based on multi-case exploration. Squires and Dorsen (2018) state that story research, ethnography, case studies, and other kinds of qualitative research are all available. Researchers may compare the outcomes of many case studies using a multiple case study approach (Ridder, 2017).

DATA ANALYSIS

The Analysis of the Organizational Aspect Examining the Business Facet

To get the information technology experts' thoughts, we made up a set of eight questions. Three stages were used to separate these eight questions. Five questions covering topics such as cyber security standards, written policies, regulations in practice, information value prioritization, and system access rights were part of the first phase, which reflects the time before the cyber assault. Phase 2's lone inquiry probed whether or not safeguards are in place in the event of a cyberattack and connected the time period of the attack itself. Two questions investigated the existence of cyber-attack analysis and the process for informing customers and other stakeholders as part of the third phase, which is concerned with security measures after a cyber-attack.

Interview responses from six IT experts were grouped into topics based on the large quantity of empirical data collected from them. The topics were organized and shown in Table 1.

Table 1: Themes incorporated in the responses of respondents regarding organizational aspects

No	Phase	Questions	Firm1	Firm2	Firm3	Firm4	Firm5	Firm6

1	Pre	Standards	LOE	**CWA, LOE**	NGL	HUWA	**CWA**	LOE
2		Written cybersecurity policy	HUWA	**CWA**	HUWA	NGL	**CWA**	HUWA
3		Rules used in practice	PTC	**CWA**	PTC	PTC	**CWA**	PTC
4		Information value prioritization	PTC	**CWA**	PTC	PTC	**CWA**	PTC
5		System access permissions	LOE	**CWA**	PTC	HUWA	**CWA**	PTC
6	During	Measures	PTC	**CWA**	NGL	PTC	**CWA**	PTC
7	Post	Cyber-attack analysis	PTC	**CWA**	HUWA	LOR	**CWA**	HUWA
8		Informing clients	NGL	**CWA**	NGL	NGL	**CWA**	NGL

Safety Precautions for Cyber Attacks

The first question sought to determine if the participating organisations employed cyber security standards and whether the IT professionals were acquainted with them; this is shown in the table above. Based on the data collected in this section, it seems that only Companies 2 and 5 have instituted any kind of policy. To be more specific, although Company 5 has adopted an international standard for cyber defence known as ISO27001, Company 2 has adopted the national norm. While the IT staff at the other four businesses couldn't name a single cyber security standard, those working in IT for these two firms were more than happy to share their knowledge. Company 1, Company 3, Company 4, and Company 6 do not have cyber security standards established in their organisation, according to the empirical data. Company 3's IT staff expressed satisfaction with their cyber security measures, in contrast to Companies 1 and 6, whose staff said that management's choice led to the lack of standards. Company 4's IT specialist attempted to lend credence to the idea that their organisation lacks standards implementation by claiming that they are too swamped with work to do anything about it.

Only two businesses meet this criterion in their cyber security policies. Both of these businesses are known as Company 2 and 5. Both companies' IT departments worked together to develop these policies, according to the companies' representatives, and having management on one side and the IT department on the other is essential because, while management knows the company's business inside and out, the IT department can show management all the different ways the system can work. Each employee is required to read and sign this policy, according to their addition. Information technology experts from Companies 1, 3, and 6 said that although their employers do not have a formal policy outlining how workers are to behave online while on the clock, there are informal understandings and guidelines on inappropriate behaviour. They elaborated by saying that the IT department and upper management worked together to establish these unspoken guidelines. On the flip side, the person in charge of IT at Company 4 said that they don't have a formal cyber security policy since their employees already know what they can't do online and wouldn't have the time to implement it anyway due to their heavy workload. Interestingly, this IT expert only thinks such a strategy is necessary for businesses whose operations are heavily dependent on the internet. According to the IT experts from Companies 1 and 6, a written cyber security policy is not necessary because small businesses do not have a large workforce and can communicate these rules verbally. On the other hand, the expert from Company 3 said that such a document is necessary only from a legal standpoint.

During the analysis of IT professionals' responses during the pre-cyber-attack decision-making phase, five distinct patterns emerged. In these two firms, we can see CWA, which will appear again in IT Professional 2 and 5, since they meet all the standards in all three areas. In the other four organisations, we can see PTC's theme appear 10 times. Most of the IT professionals who took part in this research had a poor level of cyber security awareness, as shown by the incidence of PTC in all four organisations compared to CWA in organisations 2 and 5. Table 3 shows that the rising HUWA theme occurs five times, reflecting the limited knowledge of IT professionals in the pre-cyber-attack era. During this phase, management exerts a strong influence over IT professionals. The LOE theme appears four times, with its most prominent appearance in the requirement to implement cyber security standards. IT professionals express their empowerment to make decisions that will have an impact. Finally, NGL is the least emerging topic, which is remarkable since despite its small number of appearances, it is very relevant to the results of this research.

Security Measures to Implement During a Cyberattack

The following respondents were asked about the presence of steps to be taken during a cyberattack. In contrast to Company 3, which has no security procedures in place in the event of a cyberattack because its employees believe that firewall and antivirus software provide complete protection, all of the other IT experts surveyed claimed to have a plan in place. Since all of Company 1's data is saved on the Internet server, the decision to switch it off is reflected in the company's measures. On top of that, the staff alerts the IT specialist if they see any suspicious cyber activity. Companies 2, 4, and 6 take a different approach; in the event of a cyberattack, their IT staff switches off the Internet. Company 2 has a little different policy: in the event that an employee is unable to locate an IT specialist, they are allowed to power down their computer by pushing the power button for a longer duration than normal. It seems that the IT specialist from Company 5 is being very careful in preparing for the possibility of a cyberattack. In such a situation, IT expert 5 would first power down the whole network, and then the server that connects to it. Because it is impossible to tell whether a virus or malware has already infected the device, he says, the Internet server must also be turned down.

This phase is dominated by PTC, which demonstrates that the majority of IT professionals have developed organisational cyber security procedures to be used in the event of a cyber security incident. There are also Companies 2 and 5 that have a CWA. But at one firm, the NGL motif appears, especially in IT professional 3, and it was already there before the cyberattack.

Precautions to Take Following a Cyberattack

Upon asking IT professionals how they determine whether a cyberattack was targeted at their Organisation or if it was a random incident, half of the participants admitted that they do not do this kind of analysis. Only Companies 1, 2, and 5 do this kind of study; Companies 3, 4, and 6 do not. According to IT expert 3, doing such a study would be very laborious and complicated. They claim that if they were really interested in receiving this information, they would approach their Internet service provider for assistance. Curiously, the IT specialist from Organisation 6 said that this kind of investigation is superfluous as his Organisation isn't big enough to be a tempting target for cybercriminals.

Last but not least, the IT expert from Organisation 4 believes that assessing cyber dangers is a good idea, but he argues that the Organisation doesn't have the resources to implement this approach. various firms' IT departments use various methods when analyzing cyber risks. Company 2's IT specialist, in addition to reviewing system logs, also watches to see if the same cyber-attack will happen again, while Company 1's IT specialist attempts to discover trends in the internet firewall and system logs. But according to Company 2's IT expert, this might take a long time as waiting for a threat rehearsal can take a long time. Not only did IT expert 5 verify the existence of threat analysis, but he also detailed the signs that, in his opinion, are crucial for doing it out. He begins by confirming the specific data categories that the criminal had in mind. Additionally, he assesses the extent of the data destruction. In the end, he guesses whether the assault was deliberate and directed at the firm or whether it was a random cyberattack based on the findings.

An Examination of the Technical Facet

According to Julisch (2013), the six questions included in the empirical results of the cyber security technical element provide credence to the technological basis of cyber security. Analyzing system logs, keeping an up-to-date inventory list of software and hardware, backing up system data, analyzing threats identified by antivirus software, using advanced password rules, and applying internet firewall rules are all essential components of a technological cyber security foundation.

Comparing Table 2 to Table 1 from the organizational aspect study, we can see that both tables aim to summaries the responses given by IT experts from six different firms.

Table 2: Interviewees' responses on technological aspects, together with the underlying themes

No	Questions	Firm 1	Firm 2	Firm 3	Firm 4	Firm 5	Firm 6
9	System logs analysis	PTT	**CWA**	PTT	PTT	**CWA**	PTT
10	Inventory list	NGL	**CWA**	PTT	NGL	**CWA**	NGL
11	System backups	PTT	**CWA**	PTT	PTT	**CWA**	PTT
12	Antivirus threat analysis	HUWA	**CWA**	HUWA	LOR, PTC	**CWA**	HUWA
13	Advanced password rules	PTT	**CWA**	PTT	PTT	**CWA**	PTT
14	Internet firewall rules	PTT	**CWA**	PTT	PTT	**CWA**	PTT

The log analysis is performed in all the six companies but their recurrence and methods differ from company to company. When it comes to the frequency of log analysis, Companies 3 and 6 perform it once a week but also more frequently if it is needed. In Company 1, the log analysis is limited to be done only once a week, in Company 4, on an occasional basis, while in Company 2 it is conducted three times a week but if it is known that there is a new tread in the cyber space, it is done more often. The only company that performs the log analysis on a daily basis is Company 5. IT professionals in Companies 1, 3, 4 and 6 analyze the logs manually while in Company 2, besides the manual log analysis, there are automatic e-mail notifications about the error logs that IT professional 2 receives in his electronic mail account. IT professional in Company 5 also receives the error logs in his e-mail account but immediately performs the analysis of them when they are received. Additionally, he explains that he divides the system logs into three groups, namely error, debug and information that help him to perform their analysis hierarchically.

Complete and up to date inventory list of hardware and software exists in 50% of sampled companies. That is, the Companies 2, 3 and 5 have such a list but the rest of them do not. IT professional 3 states that he has such a list and that it is always updated. In Company 2 the media access control addresses of hardware devices are tracked through the system logs. The IT professional from Company 5 provided the most thorough answer. He explains that the list is always up to date and it is used for the purposes such as to replace old fashioned hardware with the new one, to keep the software license always up to date and to authorize the company's hardware and software in their information system. As aforementioned, Companies 1, 4 and 6 do not have such a list but IT professionals from these companies provided different reasons for this. IT professional 1 says that he creates the hardware authorizations while installing the new devices, IT professional 4 agrees that such a list should be created but guesses that the lack of responsibility may be the reason of not having it. Finally, IT professional from Company 6 does not provide any reason for not possessing the list but admits that it is a good idea to have one created.

System backup is the activity that is performed by all the six IT professionals. More specifically, Companies 1, 2 and 4 back up their data on a daily basis while IT professional from Company 2 added that beside the daily backup, all the company's data are backed up twice a week. In Companies 3 and 5, the complete data backup is done once a week with addition that in Company 5, this activity is also performed on a regular daily basis. IT professional 6 stated that all the data created on a daily basis are saved at two places at the same time i.e. at two hard discs but all the company's data are saved every night. There is a different length when it comes to data storage. Company 1 stores the backed-up data for a month, Company 3 never deletes them and Company 4 stores its data until the next backup. Company 5 stores its data for ten and Company 6 for three years. However, in Company 2 the daily data are stored for two years but the complete backed up data is preserved until the next backup. In the case of data damage, IT professionals 1, 2, 3, 4 and 5 can retrieve their data minimally after from 20 minutes until 2 hours. More specifically, Companies 1 and 3 can retrieve their data after 1 hour, Company 4, from 20 to 25 minutes, Company 2, after 30 minutes and Company 5 can restore its data after one-to-two-hour time. According to IT professional 6, this process takes quite a time which is data retrieval after from 4 to 6 hours.

Psychological Aspect Analysis

Analyzing the responses of the interviewees to six questions is the empirical data analysis of the psychological component. Two sets of questions comprise the six-question test. Among IT workers, is there a general degree of guilt or shame proneness? That's the goal of the first series of questions. On the other hand, the second set of questions is designed to determine whether IT workers are more likely to feel guilty or ashamed, as it covers both the construction of cyber security and its aftermath.

The summary of the responses from IT experts is shown in Table 3 below; it is formatted similarly to Tables 1 and 2.

Table 3: Interviewees' responses on psychological aspects, together with the underlying themes

No	Questions	Firm1	Firm2	Firm3	Firm4	Firm5	Firm6
9	System logs analysis	PTT	**CWA**	PTT	PTT	**CWA**	PTT
10	Inventory list	NGL	**CWA**	PTT	NGL	**CWA**	NGL
11	System backups	PTT	**CWA**	PTT	PTT	**CWA**	PTT
12	Antivirus threat analysis	HUWA	**CWA**	HUWA	LOR, PTC	**CWA**	HUWA
13	Advanced password rules	PTT	**CWA**	PTT	PTT	**CWA**	PTT
14	Internet firewall rules	PTT	**CWA**	PTT	PTT	**CWA**	PTT

CONCLUSIONS

We all know that small and medium-sized firms (SMEs) are the lifeblood of the global economy, but we also know that they are much more susceptible to cyber-attacks than large corporations. Understanding the impact of organizational, technical, and psychological factors on cyber security for small and medium-sized enterprises (SMEs) was the overarching goal of this master's dissertation, which aimed to shed fresh light on the topic. Looking at it through the eyes of IT experts reveals a lack of understanding of the organizational, technical, and psychological factors affecting SMEs. In general, cyberattacks on SMEs are more common than on big firms, and this thesis supported two claims about this phenomenon. The first is that small and medium-sized enterprises (SMEs) don't put enough money into cyber security (Rodriguez and Martinez, 2013).

REFERENCES

1. Blanksma-Ceta, A., & Konings F. (2017). National Cybersecurity Awareness Survey. Retrieved June 28, 2020, from https://www.alertonline.nl/media/

2. Bongiovanni, I. (2019). The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education. Computers & Security, 86, 350-357.

3. Boundy, A.& Levy, E., (2021, February 18). Staying Safe Online Guide. Netsafe, A Providing Free Online Safety Advice in New Zealand. Retrieved March 18, 2021.

4. Brown, C. F., Demaray, M. K., Tennant, J. E., & Jenkins, L. N. (2017). Cyber Victimization in High School: Measurement, Overlap with face-to-face Victimization, and Associations with Social–emotional Outcomes.*School Psychology Review*, 46(3), 288-303.

5. Bruijn, H. De, & Janssen, M. (2017). Building cybersecurity awareness : The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

6. Burley, Diana & Bishop, Matt & Kaza, Sidd & Gibson, David & Hawthorne, Elizabeth & Buck, Scott. (2017). *ACM Joint Task Force on Cybersecurity Education.* 683-684. https://doi.org/10.1145/3017680.3017811.

7. Cabero-Almenara, J., Romero-Tena, R., & Palacios-Rodriguez, A. (2020). Evaluation of Teacher Digital Competence Frameworks Through Expert Judgement: the Use of the Expert Competence Coefficient. *Journal of New Approaches in Educational Research*, 9(2), 275-293. https://doi.org/10.7821/naer.2020.7.578

8. Caena F, Redecker C. (2019) Aligning teacher competence frameworks to 21st century challenges: The case for the European Digital Competence Framework for Educators (DigcompeDu). *European Journal of Education*, 54,356–369. https ://doi.org/10.1111/ejed.12345

9. Cartelli, Antonio. (2020). Frameworks for Digital Competence Assessment: Proposals, Instruments and Evaluation. *Proceedings of Informing Science & IT Education Conference, USA* 561-574. https://doi.org/10.28945/1274

10. Cassie, Hague. & Sarah, Payton (2020) *Digital Literacy across the Curriculum* (a Futurelab handbook) FutureLab. Retrieved May 1, 2019, from https://www.nfer.ac.uk/publications/futl06/futl06.pdf

11. Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cybersecurity*, 5(1), https://doi.org/10.1093/cybsec/tyz001.2092011

12. Chaowakeeratiphong, T., & Wongnaya, S. (2020). Guidelines to Develop Digital Citizenship of Students at the Faculty of Education, Kamphaeng Phet Rajabhat University. *The Golden Teak: Humanity and Social Science Journal*, 26(4), 72-85.

13. Chapman, J. (2019,). *How safe is your data? Cyber-Security in Higher Education*, Retrieved June 28,2020 from https://www.Note-12-Paper-April-2019-How-safe-is-your-data.pdf

14. Chen, Y., & He, W. (2023). Security risks and protection in online learning: A survey. *The International Review of Research in Open and Distributed Learning*, 14(5). https://doi.org/10.19173/irrodl.v14i5.1632

15. Chetty, P. (2021, October 18). *How to Graphically Test Normality*? Knowledge Tank. Retrieved February 22, 2022, from https://www.projectguru.in/