COVID- 19 pandemic - An Empirical Study on the Cybersecurity Behaviour of Healthcare Sectors and Employees

Harrison Stewart
Harrison Stewart Group
Germany
stewart@harrisonstewart.net

JDIM
Journal of Digital Information Management

ABSTRACT: *Earlier research by our team have focussed the multilayer SAM spiking neural network using training algorithms for implementing FPGA. In the current work we have outlined the utilization of SAM-based network for developing function approximation. We have deployed the spike coding model for the work. In the testing we have proved that the "interpolated XOR" and 3-polynominal function approximation of this SAM network. We found that the SAM network has the ability to perform these function approximations to high accuracy.*

Subject Categories and Descriptors: [K.6.5 Security and Protection] [J.3 LIFE AND MEDICAL SCIENCES]' Health

General Terms: Security, Cybersecurity, Pandemic period, COVID 19, Health Sciences

Keywords: Covid19, Cybersecuriy, Human Physiology, Organisational Culture, Cybersecurity Culture

Received: 11 June 2022, Revised 18 August 2022, Accepted 4 September 2022

Review Metrics: Review Scale: 0/6, Review Score: 4.9, Inter-reviewer consistency 86.2%

DOI: 10.6025/jdim/2022/20/4/115-130

1. Introduction

Healthcare leaders are investing in cyber security because of the new cyber threats that emerge daily (Fabisiak & Hyla, 2020). The sector has become a target for cyberattacks due to the high demand for patient data. The perceived significance of cybersecurity reflects how employees believe their motivation will improve cybersecurity in their organisation (Tsai & Tai, 2003). Technologies such as digitalisation and networking have become indispensable for all organisations, regardless of their size and characteristics, to gain a competitive advantage and satisfy consumers and partners (Stewart & Jürjens 2018). These commodities are driven by technology, which is also accompanied by various challenges, such as the rise of cybercrime (Stewart & Jürjens, 2018; Hu & Wang, 2018; Burns et al., 2019; Karumbaiah et al., 2016; Shahri et al., 2012).

Due to technological limitations in combating cybersecurity, the human factor has come to play a crucial role in these organisations, making them targets of cybercrime (Stewart & Jürjens 2017; Wash & Cooper, 2018). Various attacks exploit human weaknesses to obtain information and inflict harm on organisations. The most common tactics are phishing (Burda et al., 2020; Allodi et al., 2020; Burns et al., 2019), malware attacks, email spam (Hu & Wang, 2018; Chandra et al., 2016), password attacks and social engineering (Bullée & Junger, 2020; Bullée, 2017; Hadnagy. 2018). Attackers obtain employee information from websites and social networks for profiling, and craft emails with a legitimate look that contains a malicious link or attachment (Hu & Wang, 2018; Chandra et al., 2016; Agrawal & Singh, 2016). The temptation to click on such an email is powerful, which then leads to the installation of malware or spyware on the victim's computer (Burns et al., 2019; Wash & Cooper,

2018; Gupta et al., 2017). Factors such as curiosity and fear are some of the most critical factors that lead them to click on such emails (Acquisti, 2014; Wiederhold, 2014). There are some possible reasons for the increase in attacks on various organisations, including insufficient implementation of cybersecurity strategies, lack of or inadequate cybersecurity training, and adequate experience and resources (Wash & Cooper, 2018; Stewart & Jürjens 2017; Karumbaiah et al., 2016). Most organisations focus more on the technological factor and neglect the human factor (Stewart, 2021; Stewart & Jürjens, 2017; Sirur et al., 2018; Wash & Cooper, 2018; Asai & Perez, 2012).

With the improvement of network and internet technologies, cyber attacks on physical systems in various organisations through phishing, malware attacks, password attacks, and social engineering are becoming more common (Bullée & Junger, 2020; Hu & Wang, 2018; Hadnagy, 2018). The goal of these attackers is to spy on, manipulate, destroy and gain unauthorised access to data, leading to significant financial consequences and reputational damage (Cryptovision, 2021; Oliveira et al., 2017; Stewart & Jürjens, 2017). Various organisations are attacked every day with or without their knowledge (Hu & Wang, 2018; Liu & Moh 2016; Agrawal & Singh, 2016; Burda et al., 2020).

Several countries, academics, practitioners, industry conformists and government sectors have proposed various strategies to combat these attacks from a human per spective by addressing security awareness training and education methods. Despite all the internal measures taken by various organisations to protect information through security training and awareness, these efforts are insufficient considering the immense financial impact of cyber attacks on the organisations (Stewart & Jürjens, 2017; Karumbaiah et al., 2016). A survey by the digital association Bitkom showed that over 103 billion euros in damage were caused by cyber attacks in 2018/2019, and rose to 223 billion euros in 2020/21 in Germany (Cryptovision, 2021). This indicates that technical security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), network intrusion detection systems (NIDS), host intrusion detection systems (HIDS), or antivirus software are insufficient in today's world. As a result, the cyber threat has become unbearable for businesses, and all efforts to protect critical assets and maintain business continuity have become an impediment. Other researchers and organisations have proposed artificial intelligence and machine learning (Tewari et al., 2016; Grieco et al., 2016; Wu et al. 2017; Chernis and Verma 2018), but AI is still early.

To ward off and minimise such threats, companies offer security training to their employees (Chapple, 2019; Stewart & Jürjens 2017). This usually involves traditional integrated phishing training programmes and technologies that are often inefficient or unable to respond to modern, customised social engineering attacks (Bullée & Junger, 2020). Even though personnel are trained and educated about the dangers, most fatalities are caused by negligence and ignorance (Acquisti, 2014; Wiederhold, 2014; Agten et al., 2015). While some studies have suggested that workers who fall for such tactics ought to be punished, it has been observed that such sanctions create mental distortions in workers that adversely affect their work performance (Acquisti, 2014; Wiederhold, 2014).

This study addresses this issue by conducting a cybersecurity survey focusing on human versus cybersecurity risk in 20 healthcare centres in Germany. To this end, a survey is conducted at these companies to investigate how employees address cybercrime and how this affects the company. Therefore, this paper aims to identify vulnerabilities and technical risks associated with human action, identify areas of improvement for companies and propose a solution to the problem. It also addresses the security challenges companies face and offers cyber security education and awareness guidelines.

2. Literature Review

2.1 Cyber security - Human factor in an organization

Stewart & Jüjens (2017) showed how the human factor had been neglected in many organizations, leading to information security failures. Several studies have been conducted on information security policies (ISP) and compliance (Safa et al., 2016; Ifinedo, 2014) as a measure to increase employee security awareness, but the practical application of such policies present some challenges.

Despite the numerous studies that address the need for organizations to consider the potential benefits of reprehensible behaviour and individual standards and organizational conditions (Acquisti, 2014; Wiederhold, 2014; Agten et al., 2015; Karumbaiah et al., 2016), most fail to cover all elements of human conduct and social structure in the organization.

Human error and negligence are also considered the biggest threat to data security efficacy, making it a concern worth taking seriously (Agten et al., 2015; Wash & Cooper, 2018; Stewart & Jürjens 2017). The number and sophistication of cyber-attacks perpetrated by criminals have become a significant concern for organizations. It is possible to minimize these errors and negligence through awareness programmes encouraging individuals to adopt cybersecurity behaviours (Acquisti, 2014; Wiederhold, 2014).

Phishing campaigns have also been used to analyze and evaluate human behaviour (Allodi et al., 2020; Burda et al., 2020; Karumbaiah et al., 2016). The act of sending a fraudulent message to induce a human victim to divulge confidential information is known as phishing. A successful phishing attack allows the attacker to install malicious software on the victim's computer (Diaz et al., 2018; Burns et al., 2019). Phishing attacks have been around since the dawn of the internet. The first effort to steal sensitive

data was made via the America Online (AOL) service in the mid-1990s. Phishing is a sophisticated strategy that uses social engineering tactics to persuade victims to act against their best interests. The most well-known phishing attacks are: Email Phishing, HTTPS Phishing, Spear Phishing, Whaling/CEO Fraud, Vishing, Smishing, Angler Phishing, Pharming, Pop-up Phishing, Clone Phishing, Evil Twin and Watering Hole Phishing. A deeper insight into these attacks can enable organizations to protect their users and their data more effectively, as these attacks target humans. Phishing emails have become increasingly influential and pose a more significant threat to society as their sophisticated approach tends to confuse victims regarding the legitimacy of such emails (Burda et al., 2020; Allodi et al., 2020; Hu & Wang, 2018). In both phishing emails and spear phishing, the visual illusion has shown to be a successful tactic (Teixeira et al., 2020; Rastenis et al., 2020), enhancing the impression of an email's legitimacy and making it difficult for targets to differentiate a legitimate email or website from a fake one. While phishing email targets many victims, spear phishing targets a single person by pretending to know the victim, making this phishing very effective (Allodi et al., 2020). Voice phishing or vishing, on the other hand, is a phishing attack carried out over the phone to trick a human victim into revealing confidential information.

As previously stated, social engineering techniques serve as a facilitator for phishing attacks (Bullée & Junger, 2020; Hadnagy, 2018; Bullée, 2017). Social engineering is a simple, induced, and manipulated process to obtain sensitive information from individuals. This facilitator poses a risk to all players in a company (Karumbaiah et al., 2016) and should be addressed through improvement initiatives.

Even though all of the 20 health centres in this study have adopted a holistic cybersecurity landscape (Tawileh et al., 2007), a survey performed for this study found that phishing attacks account for 80% of all cyber attacks, emphasizing the importance of human factors (Asai & Perez, 2012; Stewart & Jürjens 2017; Wash & Cooper, 2018).

2.2 Cyber security - Technological factor

Many anti-phishing simulators have been developed to prevent malicious emails from reaching the target user. These simulators have a URL-based control function and keyword evaluators. These keywords are stored in an existing database and determine the content of the email to block the entire email or delete all malicious attachments (Teixeira et al., 2020; Chandra et al., 2016; Sharma & Yadav, 2015). As already explained in section 2.1, phishing attacks are a major threat to any organization, and several comprehensive and efficient detection methods have been developed over the last decades. In this section, previous work on phishing simulators from 2015 to 2020 has been reviewed. However, these simulators can sometimes fail, leaving the end user to make strategic decisions. As mentioned earlier, machine learning and artificial intelligence approaches have been used to combat phishing attacks through numerous techniques, such as allow listing and blocklisting (Tewari et al., 2016).

A phishing website detector has been studied by Gupta et al. (2017), while Allodi et al. (2020) propose an anti-phishing simulator to warn users against exploiting fake websites or computers. Other studies on fuzzing have been conducted (Godefroid et al. 2017; Rajpal et al. 2017; Wang et al. 2017; She et al. 2018). Further studies on phishing detection have been conducted in e-banking using a fuzzy data mining strategy, while others propose anti-phishing detection (Kunju et al., 2019; Aleroud et al., 2017; Kiren et al., 2020; Rana et al., 2020; Justine et al., 2020; Simono et al., 2018; Jasper et al., 2019; Moul et al., 2019).

Wang et al. (2020) demonstrated a phishing prevention technique and suggested the implementation of optical character recognition on an Android mobile platform. Churi et al. (2018) presented a software prototype for phishing website detection. Eduardo et al. (2020) Conducted a systematic literature review on combating phishing attacks using recent machine learning approaches and highlighted three strategies to mitigate phishing attacks, namely: need for awareness, targeted blocklists, and machine learning. Amro (2018) & Aonzo (2018) studied phishing attacks on mobile devices, mitigation techniques and anti-phishing techniques and pointed out the shortcomings of anti-phishing techniques. Liu & Moh (2016) applied an Email filtering algorithm using email text as a keyword to perform complex word processing. The result showed 92.8% accuracy of their proposed algorithm.

Other researchers propose spam techniques and spam control algorithms to filter emails (Teixeira et al., 2020; Agrawal & Singh. 2016; Chandra et al., 2016; Sharma & Yadav, 2015). AlRashid et al. (2014) investigated the reduction of false positive emails by analyzing the behaviour of spam filters and revealed the various reasons for email failure. They developed an algorithm to facilitate email security on the recipient side. Tewari et al. (2016) proposed a machine-learning approach to predict whether an email is a spam.

Despite the various techniques and tools available to prevent phishing attacks, companies are still at risk of phishing attacks due to the negligence of their employees (Stewart & Jüjens, 2017; Agten et al., 2015). Stewart & Jürjens (2017) suggested that to combat cybersecurity, a the strategy should be developed that takes into account the interrelationship between technology, people and the organization concerned. Technical factors include defence mechanisms, human factors include perceptions of cyber security and its importance, security training and motivation, while organizational factors include information security policy, management, partners and strong leadership oversight, as well as the presence of compliance departments and a security culture.

In this context, this study shows that the integration of multiple measures has a positive impact on improving cybersecurity and that these measures should not be focused on a single department, but should be evenly distributed among employees in technical and non-technical positions, resulting in diversified knowledge within the organisation. In addition, trust plays a crucial role in cybersecurity awareness (Stewart, 2021; Pienta et al., 2020; Stewart & Jürjens, 2018; Stewart & Jürjens, 2017), and compliance with information security policies (ISPs) has been suggested in other studies (Safa et al., 2016; Ifinedo, 2014).

2.3 Cybersecurity - Security Awareness & Training

As alluded to in sections 2.1 and 2.2, technology alone cannot alleviate the risk of cyberattacks, making the consideration of the human factor a crucial element in all organisations (Stewart & Jürjens 2017). Despite sounding simple, attaining a good level of cybersecurity awareness is a challenge among employees today. Irrespective of the size of the organisation, all businesses struggle to train and educate their employees and the health centre is not exempt from this (Da Veiga & Martins, 2015; Shahri et al., 2012). The extent to which workers feel their motivation will improve cybersecurity in their organisation is reflected in their perceived adoption of cybersecurity. This highlights the importance of people being motivated to undertake cyber security training and awareness at a high level.

Although this study shows that employee negligence and errors play a significant role in cyber attacks, increasing security knowledge through sustained training from qualified specialists is a factor that contributes to a thriving cybersecurity culture (Da Veiga & Martins, 2015;

Shahri et al., 2012). Human actions are subject to uncertainty due to internal and external incentive factors. The extent of the organisation's cybersecurity culture initiatives and measures in its practical activities is proportional to its efforts to minimise employee error and negligence. Lack of cyber security training and education contributes to human vulnerabilities and thus risks. Security training and a security culture raise employees' awareness of cyber risks and strengthen their knowledge of cyber threats in terms of actions to take in specific situations. To improve cyber security awareness, organisations need to analyse the factors that influence employee participation in security programmes (Chapple, 2019; Eminagaoglu et al., 2009). This analysis should enable the organisation to review employee knowledge and the security training required to increase cybersecurity compliance adoption (Fabisiak & Hyla, 2020).

Furthermore, a strong security culture could address many of the underlying behavioural challenges to corporate data breaches (Vance, 2018; Wiederhold, 2014; Marsh & Microsoft, 2018). Developing cybersecurity skills involves overcoming digital threats using technology, policies, processes, cybersecurity training and awareness strategies that contribute immensely to enhancing overall security (Pienta et al., 2020; Stewart & Jürjens, 2017; Chapple, 2019; Karumbaiah et al., 2016; Thomas, 2018).

Organisations that underestimate the significance of adopting effective cybersecurity programmes are vulnerable to cyberattacks. Therefore, comprehensive security education and communication campaigns promote cybersecurity practices and behaviours. According to Stewart (2020),

Reference	Findings	Factor
Asai & Perez (2012) Stewart & Jürjens (2017) Wash & Cooper, (2018)	The human factor has been neglected in many organisations, leading to information security failures.	Human
Stewart (2021) Stewart & Jürjens (2018) Pienta et al. (2020)	Trust plays a crucial role in cybersecurity.	Human
Agten et al. (2015) Acquisti (2014) Wiederhold (2014)	Human error and negligence are also considered the biggest threat to cyber security efficacy.	Human
Chapple (2019)	Human error and negligence can be minimised through security awareness programmes.	Human
Allodi et al. (2020) Burda et al. (2020) Wash & Cooper (2018) Diaz et al. (2018) Burns et al. (2019)	Suggested phishing campaigns to be used to analyse and evaluate human behaviour	Human
Diaz et al. (2018) Beaudin (2017)	A successful phishing installs malicious software on the victim's computer.	Human

Reference	Findings	Factor
Bullée & Junger (2020) Hadnagy (2018) Bullée (2017)	Found out that social engineering techniques serve as a facilitator	Human
Teixeira et. (2020) Chandra et al. (2016) Sharma & Yadav (2015) Liu & Moh (2016)	Concluded that phishing emails and spear phishing, visual deception has proven to be a successful tactic in phishing attacks.	Human
Gupta et al. (2017)	Propose a phishing website detector	Technology
Kiren et al. (2020) Rana et al. (2020) Justine et al. (2020) Simono et al. (2018) Jasper et al. (2019) Kunju et al. (2019) Aleroud et al. (2017) Moul et al. (2019) Churi et al. (2020)	Propose an anti-phishing simulator to warn users against exploiting fake emails, websites or computers.	Technology
Amro (2018) Aonzo et al.(2018)	Propose a phishing Techniques in Mobile Devices	Technology
Liu & Moh (2016) Rastenis et al. (2020)	Propose Email filtering algorithm to filter emails before reaching the end-user. The result showed 92.8% accuracy of their proposed algorithm.	Technology
Agrawal & Singh (2016) Chandra et al. (2016) Sharma & Yadav (2015) Vyas et al. (2015) Thomas et al. (2014) Dhanaraj & Karthikeyani (2013)	Propose spam techniques and spam control algorithms to filter emails.	Technology
AlRashid et al. (2014)	Propose an algorithm to facilitate email security on the recipient side.	Technology
Tewari et al. (2016) Grieco et al. (2016) Wu et al. (2017) Chernis & Verma (2018)	Propose a machine learning approach to predict whether an email is spam or not.	Technology

Reference	Findings	Factor
Stewart & Jürjens (2017) Safa et al. (2016) Ifinedo (2014)	Organisations need to analyse the factors that influence employee participation in security programmes.	Organisation (Security Awareness Initiatives)
Stewart & Jürjens (2017) Chapple (2019) Karumbaiah et al. (2016)	Suggest that organisations should develop a strategy that takes into account the interrelationship between technology, people and the organisation concerned.	Organisation (Security Awareness Initiatives)
Stewart & Jürjens (2017) Stewart (2021)	Study shows that the integration of multiple measures has a positive impact on improving cybersecurity	Organisation (Security Awareness Initiatives)
Chapple (2019)	Cyber security training and measures should not be focused on a single department but should be evenly distributed among employees in technical and non-technical positions.	Organisation (Security Awareness Initiatives)
Safa et al. (2016) Ifinedo (2014)	Suggest compliance with information security policies, processes, cybersecurity training and awareness strategies.	Organisation (Security Awareness Initiatives)
Thomas (2018)	Suggest organisations to analyse the factors that influence employee participation in security programmes.	Organisation (Security Awareness Initiatives)
Marsh & Microsoft (2018) (Da Veiga & Martins, 2015)	Suggest a strong security culture to address many of the underlying behavioural challenges to corporate data breaches.	Organisation (Security Awareness Initiatives)
Wiederhold (2014) Vance et al. (2018)	Suggest factors such as knowledge, experience, attitudes, skills, beliefs and perceptions can influence behaviour.	Organisation (Security Awareness Initiatives)
Stewart & Jürjens (2017) Sirur et al. (2018) Wash & Cooper, (2018); Asai & Perez (2012).	Suggest a sustained training over time to prevent security attrition.	Organisation (Security Awareness Initiatives)
Fabisiak & Hyla (2020)	Suggest stakeholder engagement and support.	

Reference	Findings	Factor
Nurse (2018) Nurse et al. (2011 Furnell & Thomson (2009) Stewart & Jürjens (2017)	Suggest stakeholder engagement and support.	Organisation (Security Awareness Initiatives)
Da Veiga & Martins (2015)	Suggest cybersecurity improvement must be holistically aligned with the organisation's mission and promote the cyber security culture and employees knowledge.	Organisation (Security Awareness Initiatives)
Chapple (2019)	The degree of effectiveness of a cybersecurity awareness programme facilitates the evaluation of behaviour.	Organisation (Security Awareness Initiatives)
Eminağaoğlu et al. (2009) Fabisiak & Hyla (2020) Vance et al. (2018)	Suggest security culture alignment of security training with the organisation's mission, resources, cyber threat intelligence.	Organisation (Security Awareness Initiatives)

Table 1. Summary of literature

various factors such as knowledge, experience, attitudes, skills, beliefs and perceptions can influence behaviour. On the other hand, an individual's perceived attitude can be achieved through encouragement. Hence, organisations need to encourage their employees to participate in security programmes. Training and encouragement should be sustained over time to prevent security attrition (Thomas, 2018) and must be incorporated with work processes and human factors (Stewart, 2017). Moreover, the necessary awareness-raising or behavioural change is not based on security warnings alone. Sending various threat alerts to staff via email is no guarantee that they will read or comply with the issue. Instead, the focus should be on practical training and communication consistent with the organisation's mission and resources.

Cybersecurity improvement must be holistically aligned with the organisation's mission and promote the corporate culture (Da Veiga & Martins, 2015; Tawileh et al., 2007). This strategy may adversely impact the perceived significance of cybersecurity knowledge. The messages and the campaigns to raise security awareness must be tailored to the target group. The degree of effectiveness of a cybersecurity awareness programme facilitates the evaluation of behaviour. Therefore, security culture (Da Veiga & Martins, 2015), alignment of security training with the organisation's mission, resources, cyber threat intelligence and stakeholder engagement are all critical factors for a thriving security awareness culture.

Table 1 summarises the above studies, which conclude that, in addition to organisation culture and leadership, employee error and negligence are among the factors that must be considered to prevent cyber attacks.

3. Case Study & Hypothesis Derivation

This case study looks at 20 health centres that were victims of cyber attacks in the early days of Covid-19. All of the companies have tried without success to raise staff security awareness. The study analyses the current state and tries to identify common challenges. The cyber threat to organisations, businesses and governments worldwide has become a significant issue. This issue needs to be adequately addressed in the context of the 20 health centres in Germany whose focus is on cybercrime targeting staff and having a significant impact on their business. All 20 healthcare centres aim to increase the number of highly skilled workers to increase their competitiveness. However, there is also a need to increase the commitment to promoting continuous security awareness among employees and within the centres themselves. Despite this, all 20 healthcare leaders are willing to increase their spending on cybersecurity. However, with evolving threats being uncovered daily, identifying where an organisation should better invest its budget is challenging. High demand for patient data and frequently outdated systems constitute why healthcare is now the biggest target of cyber-attacks. The healthcare centres in this study store an incredible amount of confidential patient data worth a lot of money to hackers. As technology plays along, innovation has become a big focus at the 20 healthcare centres, where medical devices such as X-ray machines, insulin pumps and defibrillators play a crucial role. Here, the medical devices are connected to the internet, which provides more entry points for attacks. In addition, staff need to access the data remotely, which opens up further opportunities for attack. This attack is based on the remote connection of new devices to the network, as not all devices are secure. All organisations have implemented various protection mechanisms such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS) and antivirus software, but have still been victims of cyber attacks. This

is evident in both research and much of the business literature, which highlights the need for organisations to introduce or embed security awareness training as a method of preventing cybercrime and protecting corporate assets (Stewart & Jürjens, 2017; Sirur et al., 2018; Wash & Cooper, 2018; Asai & Perez, 2012). While there is some evidence that commitment to security training is a core part of corporate culture and identity; there is little evidence of such commitment from management and even some employees in the 20 health sectors. Moreover, strategies to create such commitment among management and executives, who could have easily transferred their willingness to employees, are not readily apparent. The problems encountered by the 20 health centres are based on their current methods of promoting security education and training, together with the flexibility with which the term 'security awareness training' is used in day-to-day operations. This can also be explained by the evolving misperception of security in the workplace, which encourages ineffective security education and training. The 20 health centres in this study have yet to cultivate a culture focused on employee security behaviour. This culture should have encompassed the features and structures of the procedures that provide the framework for their security programmes. The organisations' current strategy does not provide insight into their training outcomes and cybersecurity culture. Therefore, the characteristics and processes that signify a commitment to continuous security training for all employees and the creation or maintenance of a cybersecurity culture within the organisations must be further identified and explored.

	Factors	Items	Hypothesis
H1	*Cyber Threat Intelligence*	***CTI***	*Improving staff intelligence of cyber threats through knowledge and training will not protect an organisation from cyber attacks.*
H2	*Cybersecurity Trust & Self-efficacy*	***CTSE***	*Cybersecurity trust & self-efficacy has no positive influence on the perceived significance of cybersecurity and raises cybersecurity culture.*
H3	*Perceived Cyber Security Significant*	***PS***	*High levels of perceived significance of cybersecurity awareness and training cannot influence employees to motivate cybersecurity behaviours.*
H4	*Cyber Security Behaviour*	***CB***	*The perceived significance of cybersecurity does not positively impact cybersecurity behaviour.*

Table 2. Organisation cyber security hypothesis

Despite all the technical strategies that the organisations have put in place to defend against cyber threats fell victim to a cyber attack in 2020 during the COVID era. This was due to staff being busy with COVID patients, which prevented them from even learning about the latest threats such as phishing attacks (Agrawal & Singh, 2016; Chandra et al., 2016; Sharma & Yadav, 2015; Vyas et al., 2015; Thomas et al., 2014; Dhanaraj & Karthikeyani, 2013; Teixeira et., 2020), leaving IT specialists with the task of protecting an entire hardware network from attack. The forensic experts tasked with investigating the causes of the data breach at the 20 health centres concluded that the primary cause was a phishing attack.

At this stage, it is clear that technology alone cannot prevent cybercrime, which is why the human factor makes an important contribution (Stewart & Jürjens 2017). Although human actions are unpredictable and considered the weakest link in the security chain, most of these mistakes and negligence could be corrected through continuous and strategic security awareness training and education by qualified specialists or the security manager (Nurse, 2018; ENISA, 2019; Nurse et al., 2011; Furnell & Thomson, 2009). Therefore, management should not only invest in technical devices to mitigate cyber attacks but also adopt a strategy to reduce the weaknesses of their employees and make them aware of information security (Nurse, 2018; Furnell & Thomson, 2009). This awareness should improve their threat intelligence and educate them on security measures and actions to take in case of threat events. In the next section of this study, the staff of the 20 health centres will be analysed.

3.1 Hypothesis

Employees who work in an environment where cybersecurity is a high priority are more likely to develop effective cybersecurity habits. Creating a culture of cybersecurity requires ongoing training to keep the concepts fresh in employees' minds. Organisations should invest in their employees' cyber literacy and additional training to familiarise them with cyber threat alerts. This is an investment in the company's success and employee retention. Employees can master the rapidly evolving technology surrounding them through cyber security training and cyber threat intelligence. Employees who are not forced or motivated to learn are allowed to live in their

comfort zones and do things their way, posing a threat to the organisation. The following hypothesis is proposed in the study.

H1: Improving staff intelligence of cyber threats through knowledge and training will not protect an organisation from cyberattacks.

The human aspect is critical for any organisation and remains the weakest link in the chain of all defence systems. In this research, it is hypothesised that the human element is a source of facilitation for cyber-attacks. Data breaches in companies are primarily due to employee negligence, including management, employees and external partners, which means that companies have not adopted good policies and measures to improve the cyber security of their employees.

Although data leaks attributed to human error, trust, security awareness training, and long-term sustainability can improve an organisation's cybersecurity culture. Hence, continuous training on cyber security issues is necessary to keep staff updated. Cybersecurity awareness and training programmes must support the organisation's business needs and be relevant to the organisation's culture and mission (ENISA, 2019; Santos-Olmo et al., 2016; Dojkovski et al., 2007) to avoid security fatigue (Furnell & Thomson, 2009). A robust cybersecurity culture is critical to the employee behavioural challenges that underpin security failures in organisations. Hence trust & self-efficacy in cyber security behaviours, such as privacy in internet use and computer protection, will promote employees' awareness of cyber security. Furthermore, perceived security awareness is based on high cyber security self-efficacy. The study puts forward the following hypothesis.

H2: Cybersecurity trust & self-efficacy has no positive influence on the perceived significance of cybersecurity and raises cybersecurity culture.

When employees are confronted with the issue of cybersecurity, they perceive its significance more strongly. In other words: When employees learn about cybersecurity, they have a more favourable opinion of cybersecurity. Numerous research studies have examined perceived importance as one of the elements that influence a person's desire to perform a behaviour (Stewart, 2021; Stewart & Jürjens, 2017; Pajares and Graham, 1999). Employees' perception of the value of cybersecurity training programs plays a vital role in increasing their incentive to participate in and complete such programs (Tasi & Tai, 2003).

According to Eccles & Wigfield (2002), individual motivation is positively related to the value or relevance of an object or activity. Based on these assumptions, the perceived value of cybersecurity awareness and training programmes among employees is critical in evaluating training programmes. It increases motivation to participate in the training programmes with positive results. The study hypotheses the following:

H3: High levels of perceived significance of cybersecurity awareness and training cannot influence employees to motivate cybersecurity behaviours.

The essential elements that influence individuals' behaviour are their understanding, skills and awareness of cyber security, as well as their perceptions, beliefs and views (Arksey & O'Malley, 2005; Amankwa et al., 2015). However, the appropriate incentives needed to enhance security behaviour still need to be discovered. Such behaviour ought to take into account the ever-changing strategies that hackers use to target users (Nurse, 2018, Iuga et al., 2016; Amankwa et al. 2015). The study hypotheses the following:

H4: The perceived significance of cybersecurity does not positively impact cybersecurity behaviour.

Despite all the initiatives on employee training, it is necessary to examine the impact of industry standards on cybersecurity maturity. While organisations that adhere to an industry certification such as (ISO27000 Family, PCI, HIPAA, FIPPA, SOX, SOC, NIS, NIST, etc.) can take advantage of this to improve cybersecurity education and training for their employees, non-compliant organisations may not feel obligated to allocate resources for employee training. The study hypotheses the following:

H5: Compliance with an industry-standard improves employees' perceived cyber security and behaviour.

The issue of the human aspect as a possible source of cyber-attacks in healthcare facilities is examined based on the above five hypotheses. According to the research, the human element needs to be improved to achieve a successful level of cyber security. Neglecting staff engagement in cybersecurity development can lead to inadequate programmes and activities. The research model and definitions are presented in Table 2 and Figure 2.

The notion that regulatory compliance translates to security is a frequent misconception. Organisations that adhere to an industry standard are more likely to see employee training as a prerequisite for improving security culture than those that do not. Although "compliant" is not synonymous with security, many organisations have developed a misconception about the differences between security and compliance. This serious misperception remains regardless of the legal norm at hand.

This research project aims to illuminate more than just the training programs and processes deployed in organisations. It examines additional aspects of an organisation's surroundings that contribute to the pervasiveness of a learning culture or demonstrate the commitment to supporting continuous learning inside a company. It also includes case studies of businesses establishing a cybersecurity culture at various stages.

$H5_a$	*Industry standards do not raise staff awareness of cyber security.*
$H5_b$	*Perceived Cyber Security Significance are not influenced by Industry standards.*
$H5_6$	*Staff awareness of cyber security are not influenced by an Industry standards*
$H5_d$	*Employee cyber security culture is not influenced by Industry standards.*
$H5_e$	*Environmental factors do not influence cyber security significance among employee*

Table 2A. Industrial compliance and human factor

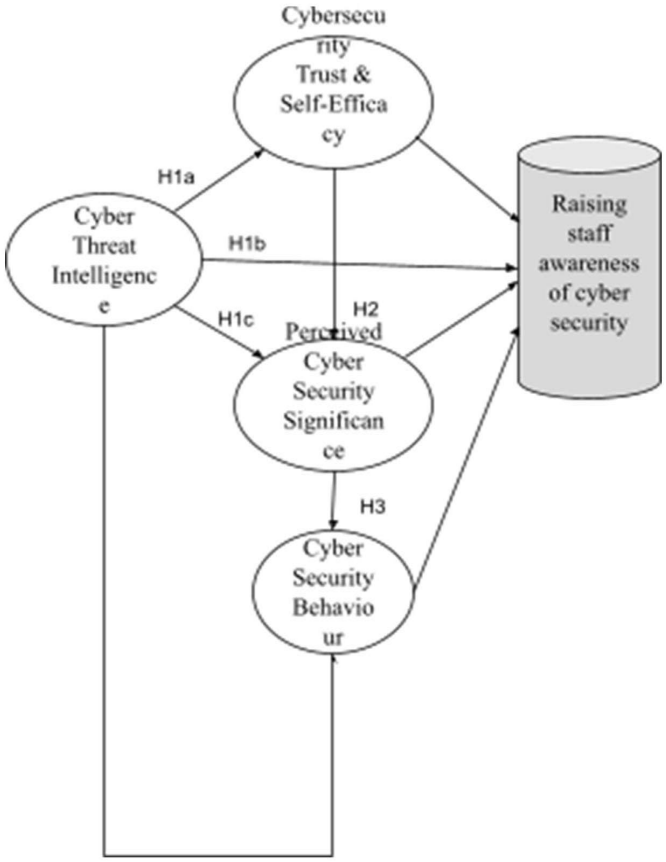

Figure 1. Proposed Research Model - Raising Staff awareness of Cybersecurity in Health Centers

This research project aims to illuminate more than just the training programs and processes deployed in organisations. It examines additional aspects of an organisation's surroundings that contribute to the pervasiveness of a learning culture or demonstrate the commitment to supporting continuous learning inside a company. It also includes case studies of businesses establishing a cybersecurity culture at various stages.

4. Methodology

The purpose of this research was to find the most influential factors affecting the human the component in improving cybersecurity knowledge among healthcare workers by using various regression models to test hypotheses and conduct a comprehensive analysis of the results. We began by using referenced databases to search for articles on cybersecurity, and an empirical study was conducted in 20 healthcare organisations in the US to obtain the correlations needed for the analysis of this study.

4.1 Data Collection (Research design and Sample)

Data were collected using a standardised online questionnaire with open and closed questions. A survey was selected to collect the necessary quantitative and qualitative data. A pilot test was first carried out with several

respondents to test the questionnaire. The actual survey was then conducted between March and May 2021. A total of 20 health centres that have experienced a data breach during the early stages of COVID-19 were contacted by email. Thus, 20 companies received the link to the online survey, and all 20 companies answered the questions with a response rate of 19,9%. The companies were asked to fill in a closed and open questionnaire. The questions were designed with the topics discussed in Section 2 in mind, such as security culture, security awareness and training, motivation, perceived cybersecurity adoption, tools, and how their current compliant standards impact their company's cybersecurity adoption, awareness, usage and perceived benefits of cybersecurity resilience. The data were analysed using Excel and SPSS.

4.2 Measures of Construct

Previous research measures and the constructs developed in this study are used to validate measurement errors in the context of cyber security. The actions of trust & self-efficacy were derived from the educational psychology literature on cyber security (Bandura et al., 1996; Choi, Fuqua, & Griffin, 2001), while the measures of the perceived significance of cyber security to employees were derived from Pajares and Graham (1999). The established steps were modified to reflect the current state of cyber security. Other constructs have been derived from this study. The PLS graph is used in this paper to ascertain the validity of the constructs and the structural coefficients.

5. Findings and Discussion

To test the hypotheses, different regression models were used depending on the scale level of the dependent variables. In the following section, the correlations of the variables processed in the study are presented. As shown in Table 1, each hypothesis was given a dependent construct. For H1, the conditional construct is cyber threat intelligence, which describes employees' ability to be informed about current cyber threats, e.g., phishing email threats. Trust & self-efficacy denotes H2 and refers to employees' confidence and ability to perform behaviours required to achieve specific goals. Employees' trust & self-efficacy is a measure of their confidence and trust in their ability to control their motivation, behaviour and social culture. Perceived cyber security significance denotes H3. Here, according to perceived importance, employees are asked to rank the significance of cybersecurity training and if the activity is important in preventing mistakes and negligence. For H4, the dependent construct is cybersecurity behaviour, which describes employees' behaviour in protecting their computer from viruses (e.g. not falling for phishing attempts and updating anti-virus software), including internet browsing security, passport security, social engineering and phishing threats. All four constructs were measured on a five-point Likert scale from "1" very low to "5"= very high. Partial Least Square (PLS) is then used to test the model to specify both the relationships between constructs and the measures underlying each construct (Lohmöller, 1989; Wold, 1982).

Except H5, which was 0.5971 out of 15 reflective indicators, the loadings of Hi, H2, H3, and H4 were all above the threshold of 0.6 (Chin, 1998 a) (Table 2).

Consequently, the reliabilities of the individual items of H1, H2, H3 and H4 are acceptable. The composite reliabilities varied from 0.778 (Cyber security trust & self-efficacy) to 0.900.

(Cyber threat intelligence), both of which are above the recommended acceptable value of 0.7 (Fornell & Larcker, 1981), indicating that the measurement model ensures construct-level reliability. Table 3 shows the composite reliability indices. By comparing the average variance extraction (AVE) between constructs to test discriminant validity, it was found that all AVEs for the latent variables measured by the reflective indicators are above the required minimum value of 0.5 and that the square root of the AVE for each construct is greater than the correlations with the other constructs. This result shows that the measurement model ensures discriminant validity (Chin, 1998b). The detailed AVE and correlation coefficients between the constructs are shown in Table 3.

Based on the Fornell-Larcker criterion, the measure of discriminant validity proposed as the square root of the AVE of each construct can be used to determine discriminant validity if the value is greater than the other correlation in the diagonal. For example, Table 3 shows that the constructs PS of CTSE, CTI and CB have square roots of 0.534, 0.451, 0.890 and 0.534, respectively, i.e. these values are more significant than the correlation value of the respective column. Thus, the result shows that the discriminant validity is well established, as shown in Table 3. The parsimony index (PCFI = .83) indicates that the model fits as shown in Table 4, including the essential parameters identified in the hypothesis. In this work, the CMIN is not within the required (Chau, 1997), but still between 0.05 and 0.08 and can be considered a suitable model fit (MacCallum et al., 1996).

The bootstrap resampling method was used to evaluate the structural model and test the path coefficients' significance. The path coefficient method was first introduced before (Wright, 1918) to relate the correlation coefficients in multiple systems to the functional relationships between variables. Chin (1998b) recommended that 0.20 and above 0.30 are ideal for standardised path coefficients. The p-value is set to 0.05. Therefore, the path coefficients were developed in this study at 0.20 and above. 0.30. In the end, the result showed the significance of the path coefficients from CTSE to PS and from PS to CB, as well as the path coefficients from CTSE to PS and from PS to CB. Although the impact of Cyber Threat Intelligence on employees' behaviour was not empirically supported in this study. Thus H1 is rejected. H5 is also dismissed, as compliance with a standard has no significant impact on employee behaviour in terms of perceived cybersecurity. The results of the hypothesis tests are summarised in Figure 2. Trust is essential in this study as it counteracts

	PS	*CTSE*	CTI	CB	Composite Reliability	AVE
PS	**1.000**	**0.370**	**-0.321**	**0.263**	**0.763**	**0.534**
CTSE		**1.000**	**0.221**	**0.096**	**0.653**	**0.451**
CTI			**1.000**	**0.111**	**0.868**	**0.890**
CB				**1.00**	**0.793**	**0.534**

Table 3. Correlations , composite & AVE of latent variables

Fit Measures	Values Proposed	Values Observed
CMIN (χ2/df)	≤ 4.0	2.77
Normed Fit Index	≥ .86	0.87
Parsimony adjusted to CFI	-	0.89
Tucker-Lewis Index	≥ .86	0.89
Comparative Fit Index	≥ .86	0.93
Root mean square error of approximation	≤ .09	0.05

Table 4. Final Confirmatory Factor Analysis Model for our Model Fit

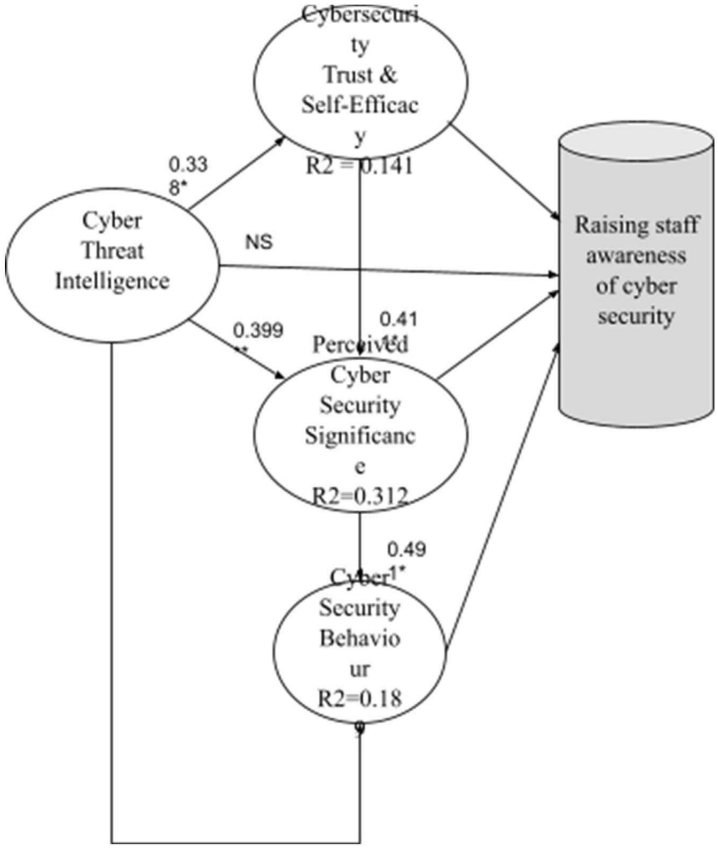

Figure 2. Proposed Research Model Fit- Raising Staff awareness of Cybersecurity in Health Centers

the risk and uncertainty associated with new, exploratory or innovative behaviours. This study has provided practical evidence that trust improves employees' cybersecurity behaviours.

After analysing the model fit, our empirical results conclude that all four constructs significantly influence employees' cybersecurity awareness, with three constructs being more important. In this regard, the results suggest a 1% level of power, and the empirical results indicate that employees are more likely to change their cybersecurity beliefs when they trust themselves. The results in this paper confirm that the influence of compliance with an industry standard has no direct or indirect impact on employees' cybersecurity perceptions.

4.1 Univariate Analysis

Considering the results obtained in this study, as shown in Table 3, there is sufficient evidence to support the rejection of H2, H3 and H4 as they all affect employee behaviour towards cyber security, as there is a strong correlation between self-efficacy and trust. The results reject H5a, H5b, H5c, H5d and H5e with a confidence level of 99%.

5. Limitations

This study is limited to 20 health centres in Germany, which means that the results of this the analysis may not be the same in other countries, demographic characteristics, cultures and additional factors. Therefore, the study focused on trust & self-efficacy, behaviour, cyber threat intelligence and perceived cybersecurity.

6.Conclusion & Future Work

In connection with the topic of the influence of human threats on cyber security in health centres, the responses of 20 hospitals in Germany were analysed. The results show that compliance with an industry standard or security awareness training does not influence employees' perception of cyber security or change their behaviour. Rather, high cyber security trust & self-efficacy and cyber threat intelligence will impact employees' attitudes towards cyber security, such as how they handle phishing emails, vishing calls, software security updates, antivirus updates and their social media behaviour. These two factors will then highlight their role in the cybersecurity chain, which will also affect their perceived significance of cybersecurity and the impact of their negligence on the company. This can be achieved through sustained motivation, communication, group sessions and one-to-one meetings that allow employees to address cyber security issues, their shortcomings and their cyber security challenges.

In the other areas, no difference was found between standard-compliant and non-standard-compliant, with almost half of the companies in this study adhering to a specific industry standard. In addition, informal variables such as trust play an essential role in developing a cybersecurity culture. The combination of confidence & self-efficacy and perceived cybersecurity, as well as cyber threat intelligence, has a significant impact on individuals and increases cybersecurity awareness and significance. In addition, employees may need to be made aware of what constitutes risky security behaviour for a company, so sharing information about cyber threats may influence security behaviour.

Trust is a crucial driver for this work as it helps to reduce the sense of risk and uncertainty associated with cyber security behaviours. Trust can improve an individual's understanding of the characteristics of a particular technology and its impact on their behaviour. In this study and previous literature, emphasis has been placed on cybersecurity training and awareness-raising for employees in areas such as phishing and social engineering. However, training alone can only improve cybersecurity culture if addressing the psychological backgrounds of employees that foster their negligence and mistakes or security fatigue. The 20 companies in this study had implemented various cybersecurity training, but they needed more to protect them from cyberattacks.

As a rule of thumb, this study shows that simply training employees will not prevent cyber attacks. Therefore, improving employees' perception of cyber security, sustained training and continuous individual assessment are the driving forces that can improve their security posture. Furthermore, compliance does not convey the security, so integrating information security management systems such as the ISO family does not necessarily impact employee behaviour. As mentioned earlier, this study was conducted in Germany and may have different implications for other health centres in other countries.

This study highlights the relevance of further research on cybersecurity in health centres, especially in this day and age when healthcare organisations are faced with advancing digitalisation.

References

[1] Acquisti, H. (2014), “Privacy in electronic commerce and economics of immediate gratification”, ACM Press, 2004, pp. 21-29; B.K. Wiederhold, “The role of Psychology in Enhancing Cybersecurity”, Cyberpsychology, Behavior and Social Networking, Mary Ann Liebert Inc. Publishers, New Rochelle, pp. 1-2.

[2] Agten, P., Joosen, W., Piessens, F., Nikiforakis, N. (2015),” Seven Months’ Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse. In Network and Distributed System Security Symposium. Internet Society.

[3] Aleroud, A., Zhou, L. (2017), “Phishing environments, techniques, and countermeasures: A survey,” Computers & Security, vol. 68, pp. 160 – 196.

[4] Allodi, L., Chotza, T., Panina, E., Zannone, N. (2020) ,”The need for new anti-phishing measures against spear-phishing attacks”, IEEE Security & Privacy, 18(2):23–34.

[5] AlRashid, H., AlZahrani, R., ElQawasmeh, E. (2014), "Reverse of e-mail spam filtering algorithms to maintain e-mail deliverability," 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Bangkok, pp. 297-300.

[6] Amankwa, E., Loock, M., Kritzinger, E.(2015),"Enhancing information security education and awareness: Proposed characteristics for a model", In: 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). pp. 72–77. IEEE.

[7] Amro, B. (2018), "Phishing Techniques in Mobile Devices," arXiv, pp. 27–35, 2018, doi: 10.4236/jcc.2018.62003.

[8] Aonzo, S., Merlo, A., Tavella, G., Fratantonio, Y. (2018),"Phishing attacks on modern android," Proc. ACM Conf. Comput. Commun. Secur., pp. 1788– 1801, 2018, doi: 10.1145/3243734.3243778.

[9] Arksey, H., O'Malley, L.(2005),"Scoping studies: towards a methodological framework", International journal of social research methodology 8(1), 19–32.

[10] Asai, T., Perez, J. L. C. (2012), "Human-related problems in information security faced by Japanese, British and American overseas companies because of cultural differences", China-USA Business Review, Vol. 11, No. 1, Pp 86-101.

[11] Beaudin, K. (2017)," The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches", New Dir. Institutional Res. 2017, 2016, 37–48.

[12] Bullée, J-W H., Junger, M. (2020), "Social Engineering, Springer Nature", Berlin, 2020, pp. 1-28. Bullée, J.-W. (2017), "Experimental social engineering: investigation and prevention. PhD thesis, University of Twente, 2017.

[13] Burda, P., Chotza, T., Allodi, L., Zannone, N. (2020)," Testing the Effectiveness of Tailored Phishing Techniques in Industry and Academia: a Field Experiment", In International Conference on Availability, Reliability and Secu rity. ACM.

[14] Burns, A., Johnson, M., Caputo, D. (2019), "Spear Phishing in a Barrel: Insights from a Targeted Phishing Campaign", Journal of organisational Computing and Electronic Commerce.

[15] Chapple, M. (2019), "Four ways to measure security success," SearchSecurity. [Online]. Available: https://searchsecurity.techtarget.com/tip/Four-ways- to-measure-security-success. [Accessed: 10-Sep-2020].

[16] Chandra, J. V., Challa, N., Pasupuleti, S.K. (2016),"A practical approach to E-mail spam filters to protect data from advanced persistent threat," 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, pp. 1-5.

[17] Chau, P. Y .K. (1997), "Reexamining a model for evaluating information center success using a structural equation modeling approach", Decision Sciences, 28(2), 309-334. doi:10.1111/j.1540-5915.1997.tb01313.x.

[18] Chernis, B., Verma, R.(2018),"Machine Learning Methods for Software Vulnerability Detection", In: Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics ACM. 2018. p. 31–9.

[19] Chin, W. W. (1998)," The partial least squares approach to structural equation modeling", In G. A. Marcoulides (Ed.), Modern methods for business research (pp. 295–358). Mahwah: Lawrence Erlbaum.

[20] Churi, T., Sawardekar, P., Pardeshi, A., Vartak, P. (2017),"A secured methodology for anti-phishing," Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017, vol. 2018- Janua, pp. 1–4, 2018, doi: 10.1109/ICIIECS.2017.8276081.

[21] Cryptovision. (2021), "223 billion euros in damage caused by cyberattacks on German companies" https://www.cryptovision.com/en/223-billion-euros-in-damage-caused-by-cyberattacks-on-ger man-companies/"

[22] Da Veiga, A., Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Computers & Security, vol. 49, pp. 162–176.

[23] Dhanaraj, S., Karthikeyani, V. (2013), "A study on E-mail image spam filtering techniques," 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, Salem, pp. 49-55.

[24] Diaz, A., Sherman, A.T., Joshi, A. (2018), "Phishing in an Academic Community: A Study of User Susceptibility and Behavior", arXiv 2018. arXiv: 1811.06078.

[25] Dojkovski, S., Lichtenstein, S., Warren, M.J.(2007),"Fostering Information Security Culture in Small and Medium Size Enterprises", An Interpretive Study in Australia. In: ECIS. pp. 1560–1571.

[26] Eccles, J.S., Wigfield, A. (2002), "Motivational beliefs, values, and goals [Learning and performance in educational settings]", Annual Review Psychology, 53, 109-132.

[27] Eduardo, B., Fuertes, W., Sanchez, S., Sanchez, M. (2020), "Classification of Phishing Attack Solutions by Employing Deep Learning Techniques", A Systematic Literature Review", vol. 152. Springer Singapore.

[28] Eminagaoglu, M., Uçar, E. & Eren, S. (2009),"The positive outcomes of information security awareness training in companies – A case study", Information Security Tech. Report, Elsevier pp. 223-229.

[29] ENISA. (2019), "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity"- (2019), https://www.enisa.europa.eu/publications/cybersecurity-cultureguidelines-behavioural-aspects -of-cybersecurity/ (Accessed 11-September-2020)

[30] Fabisiak, L., Hyla, T. (2020), "Measuring cyber security awareness within groups of medical professionals in Poland", Proceedings of the 53rd Hawaii International Conference on System Sciences, pp. 3871-3880.

[31] Fornell, C. G., Larcker, D. F. (1981), "Evaluating struc-

tural equation models with unobservable variables and measurement error", Journal of Marketing Research, 18(1), 39–50.

[32] Furnell, S., Thomson, K.L. (2009)," Recognising and addressing 'security fatigue'", Computer Fraud & Security 2009(11), 7–11.

[33] Godefroid, P., Peleg, H., Singh, R.(2017)," Learn&Fuzz: Machine learning for input fuzzing", In: 2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE; 2017. p. 50–9.

[34] Grieco, G., Grinblat, G.L., Uzal, L., Rawat, S., Feist. J., Mounier, L.(2016)," Toward Large-Scale Vulnerability Discovery using Machine Learning. In: Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. ACM; 2016. p. 85–96.

[35] Gupta, B., Tewari, Jain, A.K., Agrawal, D. P. (2017),"Fighting against phishing attacks: state of the art and future challenges," Neural Computing and Applications, vol. 28, no. 12, pp. 3629–3654.

[36] Hadnagy, C. (2018) ,"Social Engineering", The Science of Human Hacking. Wiley. Hu, H., Wang, G. (2018),"End-to-End Measurements of Email Spoofing Attacks" In USENIX Security Symposium, pages 1095–1112. USENIX Association.

[37] Ifinedo, P. (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Inf. Manag., vol. 51, no. 1, pp. 69–79, Jan. 2014.

[38] Iuga, C., Nurse, J.R.C., Erola, A.(2016),"Baiting the hook: factors impacting susceptibility to phishing attacks", Human-centric Computing and Information Sciences 6(1), 8.

[39] Jasper, G., Kathrine, W., Praise, P. M., Rose, A. A., Kalaivani, E. C. (2019),"Variants of phishing attacks and their detection techniques," Proc. Int. Conf. Trends Electron.

[40] Informatics, ICOEI 2019, no. Icoei, pp. 255–259, 2019, doi: 10.1109/ICOEI.2019.8862697. Jensen, M., Dinger, M., Wright, R., Thatcher, T. (2017), "Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems, 34(2):597–626.

[41] Karumbaiah, S., Wright, R.T., Durcikova, A., Jensen, M. L. (2016), " Phishing training: A preliminary look at the effects of different types of training", In Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, pages 1–10.

[42] Kunju, M. V., Dainel, E., Anthony, H. C., Bhelwa, S. (2019), "Evaluation of phishing techniques based on machine learning," 2019 Int. Conf. Intell. Comput. Control Syst. ICCS 2019, no. Iciccs, pp. 963–968, 2019, doi: 10.1109/ICCS45141.2019.9065639.

[43] Liu, P., Moh, T.S. (2016), "Content Based Spam E-mail Filtering," 2016 International Conference on Collaboration Technologies and Systems (CTS), Orlando, FL, pp. 218-224.

[44] Lohmöller, J.-B. (1989),"Latent variable path modeling with partial least squares", Heidelberg: Physica.

[45] MacCallum, R.C., Browne, M.W., Sugawara, H.M. (1996), "Power Analysis and Determination of Sample Size for Covariance Structure Modeling ", Psychological Methods, 1:130–49.

[46] Marsh & Microsoft. (2018),"By the Numbers: Clobal Cyber Risk Perception Survey", 2018, PwC, Managing risks and enabling growth in the age of innovation. 2018 Risk in Review Study, 2018.

[47] Moul, K. A. (2019),"Avoid phishing traps," Proc. ACM SIGUCCS User Serv. Conf., no. August 2017, pp. 199–208, 2019, doi: 10.1145/3347709.3347774.

[48] N. Agrawal, N., Singh, S. (2016),"Origin (dynamic blacklisting) based spammer detection and spam mail filtering approach," 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), Moscow, pp. 99-104.

[49] Nurse, J.R.C. (2018),"Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In: et al., A.S. (ed.) The Oxford Handbook of Cyberpsychology.

[50] Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K. (2011), "Trustworthy and effective communication of cybersecurity risks: A review. In: Workshop on Socio-Technical Aspects in Security and Trust (STAST)", pp. 60–68. IEEE (2011) 40. OAS: Cybersecurity Awareness Campaign Toolk

[51] Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., Ebner, N. (2017)," Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing", In Conference on Human Factors in Computing Systems, page 6412–6424. ACM.

[52] Pienta, D., Tams, S. & Thatcher, J.B. (2020),"Can Trust be Trusted in Cybersecurity?", Proceedings of the 53rd Hawaii International Conference on System Sciences pp 4264-4273.

[53] Rajpal, M., Blum, W., Singh, R. (2017)," Not all bytes are equal: Neural byte sieve for fuzzing"-; 2017 Nov 9; 1–10.

[54] Rastenis, J., Ramanauskaite, S., Janulevicius, J., ? Cenys, A., ? Slotkiene, A., Pakrijauskas, K. (2020), "E-mail-based phishing attack taxonomy," Appl. Sci., vol. 10, no. 7, pp. 1–15, 2020, doi: 10.3390/app10072363.

[55] Santos-Olmo, A., S´anchez, L., Caballero, I., Camacho, S., Fernandez-Medina, E.(2016),"The importance of the security culture in smes as regards the correct management of the security of their assets", Future Internet 8(3), 30.

[56] Shahri, A. B., Ismail, Z., Rahim, N. Z. A. B . (2012), "Security effectiveness in health information system:

through improving the human factors by education and training", Australian J*ournal of Basic and Applied Sciences*, 6, 226-233.

[57] Sharma, A. K., Yadav, R. (2015), "Spam Mails Filtering Using Different Classifiers with Feature Selection and Reduction Technique," *2015 Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, pp. 1089-1093.

[58] She, D., Pei, K., Epstein, D., Yang, J., Ray, B., Jana, S. (2019),"NEUZZ: Efficient Fuzzing with Neural Program Smoothing", *IEEE Symposium on Security & Privacy*; 2019, 89(46). p. 38.

[59] Sohrabi, N., Von Solms, R., Furnell, S., Elizabeth, P., and Africa, S. (2016), "Information security policy compliance model in organisations," *Comput. Secur.*, vol. 56, pp. 1–13.

[60] Stewart, H. (2020), "Information Technology and Cyber Security Unplugged": The interrelationship between Human Technology and Cyber Crime Today (English Edition), Rohhat LTD" 2020.

[61] Stewart, H., and Jürjens, J. (2017), "Information security management and the human aspect in organizations", Information & Computer Security, vol. 25, no. 5, pp. 494–534. https://doi.org/10.1108/ICS-07-2016-0054

[62] Stewart, H. (2021), "The hindrance of cloud computing acceptance within the financial sectors in Germany", Information and Computer Security, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-01-2021-0002

[63] Stewart, H. and Jürjens, J. (2018), "Data security and consumer trust in FinTech innovation in Germany", Information and Computer Security, Vol. 26 No. 1, pp. 109-128. https://doi.org/10.1108/ICS-06-2017-0039

[64] Tandale, K.D., Pawar, S.N. (2020),"Different Types of Phishing Attacks and Detection Techniques: A Review." 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC). IEEE, 2020.

[65] Tawileh, A., Hilton, J., McIntosh, S. (2007),"Managing information security in small and medium sized enterprises: A holistic approach", In: ISSE/SECURE 2007 *Securing Electronic Business Processes*, pp. 331–339. Springer.

[66] Teixeira da Silva, J., Alkhatib, A., Tsigaris, P. (2020)," Spam emails in academia", *Issues and costs. Scientometrics* 2020, 122, 1171–1181.

[67] Tewari, A., Jain, A.K., Gupta, B .B. (2016), "Recent survey of various defense mechanisms against phishing attacks," *Journal of Information Privacy and Security*, vol. 12, no. 1, pp. 3–13.

[68] Thomas, J. (2018),"Individual Cyber Security: Empowering Employees to Resist Spear Phishin to Prevent Identity Theft and Ransomware Attacks", *International Journal of Business and Management, Canadian Center of Science and Education*, Richmond Hill, pp. 1-24.

[69] Thomas, J., Raj, N. S.,Vinod, P. (2014),"Towards filtering spam mails using dimensionality reduction methods," 2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), Noida, pp. 163-168.

[70] Tsai, W.C., Tai, W.T.(2003)",Perceived importance as a mediator of the relationship between training assignment and training motivation", Personnel Review, 32(1/2), 151-163.

[71] Vance, A., Jenkins,J.L., Anderson, B.B., Bjornn, D.K., Kirwan, C.B. (2018), "Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments", MIS Quarterly, Management Information Systems Research Center, Minneapolis, pp. 355-380.

[72] Vyas, T., Prajapati, P., Gadhwal, S. (2015), "A survey and evaluation of supervised machine learning techniques for spam e-mail filtering," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, pp. 1-7.

[73] Wang, J., Chen, B., Wei, L., Liu, Y. (2017),"Skyfire: Data-Driven Seed Generation for Fuzzing", In: 2017 IEEE Symposium on Security and Privacy (SP). *IEEE*; 2017. p. 579–94.

[74] Wang, Y., Liu, Y., Wu, T., Duncan, I.(2020), "A Cost-Effective OCRImplementation to Prevent Phishing on Mobile Platforms," Int. Conf.Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2020, 2020, doi:10.1109/CyberSecurity 49315.2020.9138873.

[75] Wash, R., Cooper, M. M. (2018), "Who Provides Phishing Training? Facts, Stories, and People Like Me", In Conference on Human Factors in Computing Systems, page 1–12. ACM.

[76] Wiederhold, B.K. (2014), "The role of Psychology in Enhancing Cybersecurity", Cyberpsychology, Behavior and Social Networking, Mary Ann Liebert Inc. Publishers, New Rochelle, pp. 1-2.

[77] Wold, H. (1982)," Soft modeling: the basic design and some extensions", In K. G. Jöreskog & H. Wold (Eds.), Systems under indirect observations: part II (pp. 1–54). Amsterdam: North-Holland.

[78] Wright, P. G. (1928),"The tariff on animal and vegetable oils", 347 pp. The Macmillan Co., New York. Wright, S., 1918-On the nature of size factors. *Genetics* 3: 367-374.

[79] Wu, F., Wang, J., Liu, J., Wang, W. (2017),"Vulnerability detection with deep learning",, In: 2017 3rd *IEEE International Conference on Computer and Communications (ICCC)*; 2017. p. 1298–302.