

# Cyber Security and Digital Threats in the Workplace: Evaluating the Imperative for OSHA Integration in to Employee Safety Standards in Malaysia

Farhana Akter  
School of Business and Social Sciences  
Albukhary International University  
Alor Setar, Malaysia

Yeasmin Akter  
School of Business and Social Sciences  
Albukhary International University  
Alor Setar, Malaysia

S M Asiful Islam Saky  
School of Computing and Informatics  
Albukhary International University  
Alor Setar, Malaysia

Norizan Azizan  
School of Business and Social Sciences  
Albukhary International University  
Alor Setar, Malaysia

**Abstract**—This study analyses cybersecurity techniques to improve employee safety within the framework of Occupational Safety and Health Administration (OSHA) requirements. As organizations focus more on digital infrastructure, the risks of cyber threats have risen, impacting both operational efficiency and employee well-being. The research project analyses and evaluates current cybersecurity measures, such as multi-layered security protocols and employee training, using qualitative interviews with representatives from nine companies. The findings demonstrate that companies implementing strong cybersecurity measures significantly decrease employee anxiety and stress about digital risks. Moreover, employees reported feeling safer and supported when their employers established effective cybersecurity methods, which created a culture of paying attention and awareness. In addition, the study highlights the psychological effects of cybersecurity responsibilities, suggesting that pressure to address digital risks can lead to higher mental health challenges for employees. As a result, the study recommends OSHA include digital security measures in its workplace safety standards to address these high risks. Despite its contributions, the study has limitations that focus on specific industries, which may disrupt the findings' generalization ability. Future studies must include a larger range of industries to gain a deeper knowledge of cybersecurity's impact on employee safety in different organizational situations. Overall, the findings emphasize the need for proactive cybersecurity measures to create a positive work environment. By bridging the gap between technological advancements in security and employee well-being, this study contributes to the increasing conversation on workplace safety in digital threats, emphasizing the need for robust legal structures that address both physical and digital threats.

**Keywords**—Cybersecurity; Digital Threats; OSHA Standards; Employee Safety; Workplace Safety.

## I. INTRODUCTION

Cybersecurity maintains digital systems, networks, and data against unauthorized entry, theft, and damage[1][2][3] including a range of approaches, techniques, and practices for securing sensitive information and avoiding cyber-attacks. In the workplace, cybersecurity is essential for protecting

company secrets and guaranteeing data confidentiality, integrity, and availability throughout its lifecycle[2], [4]. Furthermore, firewalls, encryption, safe passwords, and attack monitoring and detection systems are all vital elements of cybersecurity[3]. Cybersecurity plays a vital role in many sectors, including government, finance, healthcare, and education[1]. As cyber-attacks grow, businesses and individuals must be informed of new risks and take the appropriate steps[3]. Beyond that, digital hazards in the workplace have become an alarming issue, impacting both employee safety and productivity[5], [6]. According to a research highlight[1], these dangers include illegal observing, location tracking, and vulnerabilities in software has become a major challenge in terms of data protection and workplace safety. To address these mentioned challenges, digital health interventions have taken some steps in improving different kinds of health matters, particularly sleep, mental health, and physical activity levels[7]. In the construction industry, digital twin technology has emerged as an effective solution to enhance workforce safety by using advanced detecting and visualizing technologies[8]. However, the development sector has not completely implemented these improvements. As digital technologies develop, organizations have to incorporate comprehensive digital safety measures and workplace safety demands to protect employees from new hazards[9].

Cybersecurity attacks have become increasingly common and sophisticated in the digital era[10], posing serious risks including malware, ransomware, phishing, denial-of-service attacks, and data breaches in businesses and individuals[11]. For example, in May 2017, the WannaCry ransomware assault was a global cybersecurity disaster that had an important effect on healthcare systems, particularly in the UK's National Health Service (NHS)[12]. Hospitals and clinics lost access to patient records, which led to the cancellation of thousands of appointments and surgeries[13]. This attack revealed weaknesses in vital healthcare infrastructure, as malware disabled medical systems, harming patient care and causing major operational disruptions across targeted organizations.

This malware used Microsoft Windows vulnerabilities to encrypt users' data and demanded ransom payments for decryption[14]. The attack damaged around 230,000 devices in more than 150 countries, disrupting key services such as hospitals, businesses, and government institutions.

Furthermore, healthcare data is especially sensitive due to the importance of emergency interventions. The continuous application of older operating systems like Windows XP increased the NHS's vulnerability[15]. To reduce these threats, various countermeasures are used, such as firewalls, antivirus software, and intrusion detection systems[10], [11]. Additionally, organizations should invest in cybersecurity solutions, educate employees on best practices, and establish cyberattack response plans. Even as cyber risks grow, organizations and people must stay educated about emerging trends and take the required security precautions to secure their data[16]. On the other hand, Occupational Safety and Health (OSH) is a multidisciplinary profession that concentrates on identifying, preventing, and reducing workplace hazards for better worker health and well-being [17]. Furthermore, it includes research into global worker injury, disease, and death, as well as issues that influence workers' well-being throughout the world[18]. Occupational Safety and Health (OSH) seeks to attain optimal health and well-being in all work contexts, with measures reducing absenteeism by 27% and company healthcare costs by 26%[19]. The issue has grown in importance as a result of globalization and the COVID-19 pandemic, necessitating a global approach to occupational safety and health plans[18], [19]. OSH specialists are critical in safeguarding people, property, and the environment, in addition to managing safety issues across industries[20]. Despite their significance, work-related health issues still represent a huge burden, with millions of fatalities and accidents reported every year[19]. Furthermore, cybersecurity concerns in Malaysian workplaces have become more prevalent, especially since the development of remote work during the COVID-19 epidemic. According to studies, there has been an increase in many cybercrimes such as online phishing, virus distribution, fraud, and sexual harassment[21]. Malaysia has been recognized as the most vulnerable country in Southeast Asia to cyberattacks, needing enhanced safety precautions among government employees[22]. Technology, organizational, and human factors are three significant influences on cyber security protection in Malaysia[23]. To address these issues, the Malaysian government has taken numerous measures to enhance worker safety, including recent modifications to the Occupational Safety and Health Act (OSHA). These changes strive to widen legal requirements, add extra safeguards for dangerous material management, and enhance employee engagement in safety concerns[24].

The increasing cybercrime in Malaysia puts government employees in danger due to an inadequate level of cyber awareness. Despite modern security measures, strengthening training is essential for securing confidential information and decreasing threats. In addition, cybersecurity issues in Malaysian organizations boost employee stress, and mental health and safety. The lack of evaluation for these hazards in OSHA 1994 highlights the significance of digital threat management[25].

#### A. Research Objective

1. To investigate the effects of cybersecurity on employee safety.
2. To explore the impact of digital hazards on employee safety.
3. To analyze the relationship between OSHA standards and employee safety.

#### B. Research questions

1. What is the effect of cybersecurity on employee safety?
2. What is the impact of digital hazards on employee safety?
3. How is the relationship maintained between OSHA standards and employee safety?

#### C. Significance of the study

This study is significant because it analyses the vital connection between cybersecurity and employee safety under Occupational Safety and Health Administration (OSHA) regulations, as workplaces depend on digital technologies. As a result, the hazards linked to cyber threats that affecting both organizational productivity and employee well-being. By evaluating current cybersecurity policies and their effects on employee safety, this study emphasizes the importance of OSHA increasing its safety guidelines to include cybersecurity protections. The findings indicate that robust cybersecurity protocols can minimize employee stress and anxiety, promoting an extensive strategy for workplace safety that involves both physical and digital safeguards. This study teaches policymakers and business leaders about the value of complete regulatory frameworks that prioritise digital safety, resulting in a safer and more supportive work environment in an increasingly digitization world.

## II. LITERATURE REVIEW

#### A. Cybersecurity and Workplace Safety

Cybersecurity is sometimes seen as a wide expression allowing various meanings, because of its multidimensional character. It is usually described as a set of procedures, security measures, and controls aimed to protect systems and data from cyberattacks. However, cybersecurity goes beyond protecting information; it involves protecting the people who interact with it[26]. Cybersecurity experts also monitor security data, gather intelligence, use tools to protect sensitive information, investigate cybercrime, manage secure IT systems, and protect networks. Their work is highly collaborative, particularly in system procurement and development, where teams must analyze needs, design solutions, evaluate vendors, and help with system implementation[27]. Furthermore, recent studies indicate an increase in the occurrence and severity of cybersecurity threats across the world. There are Common risks include phishing, malware, ransomware, social engineering, and denial-of-service attacks[28]. Furthermore, the COVID-19 pandemic has increased weaknesses in cybersecurity as the world has turned to digital platforms for employment, education, and business, increasing dependency on vulnerable networks and systems[29]. Cybercriminals have benefited from these shortcomings and are targeting individuals and businesses for financial gain or access to private information[28]. The fast movement to remote employment has complicated the

cybersecurity landscape, presenting new difficulties to organizations[30]. This unexpected shift has increased cyber-risk profiles, with employees frequently making poor security decisions due to a lack of suitable remote access technology[31].

Malaysian employees are particularly concerned about cybersecurity and workplace safety. Management safety policies, coworker safety, and job security are all significant indicators of technical employees' compliance with safety measures[32]. Raising an understanding of procedural information security countermeasures improves protection motivation, which in turn enhances cybersecurity behaviors among employees[33]. Furthermore, the perception of severity, vulnerability, reaction efficacy, and self-efficacy influence the cybersecurity behavior of government employees[34]. The COVID-19 pandemic has raised cyberattacks, particularly within remote work, exposing employees to increased cybersecurity vulnerabilities. Malaysia reported 4,596 cybercrime scenarios in just the first four months of 2022[35]. Addressing these increasing threats necessitates a comprehensive approach that strengthens both cybersecurity and occupational safety regulations. This can be accomplished by targeted training, technology advancements, and establishing a culture of safety awareness, resulting in a secure and safe environment for Malaysia's growing workforce[36], [37].

#### B. Digital Threats Affecting Workplace Safety

While digital advances such as wearable gadgets, augmented/virtual reality, artificial intelligence, and navigation systems can improve safety in hazardous areas, but they present new threats[38]. These include illegal surveillance, location tracking, software crimes, phishing, ransomware, data breaches, social engineering, and denial of service attacks [39]. Besides that, integrating artificial intelligence into workplaces might boost productivity, but it may also worsen psychosocial concerns such as stress, prejudice, and job intensification due to increased monitoring and micromanagement capabilities[40]. Furthermore, the use of digital technologies can create both positive and bad workplace conditions, influencing employee well-being and safety[41]. Moreover, the digital era has enhanced unity but also boosted cybersecurity dangers in the workplace. Common risks include phishing, ransomware, data breaches, social engineering, and denial-of-service attacks[28], [42]. These concerns have grown in importance as remote work, cloud computing, and IoT technologies have become more popular[28], [43]. Journalists and human rights workers encounter extra threats, including illegal surveillance and GPS tracking[39]. Although ransomware attacks have become increasingly common, exploiting users remains the weakest link in cybersecurity[44]. These assaults often use social engineering techniques to trick victims into compromising their systems[45].

Phishing, social networks, and email are common attack vectors, with recently hired employees, those with limited cybersecurity awareness, and high-profile targets being more susceptible. Besides that, organizations often lack adequate cybersecurity preparedness, with employees using outdated

software, weak passwords, and lacking awareness of proactive prevention measures[43]. To mitigate these risks, experts recommend investing in cybersecurity solutions, educating employees on best practices, and developing response plans for cyberattacks[42]. A comprehensive approach that encompasses technical, preventive, and protective measures is necessary to address the evolving digital safety landscape[39].

#### C. Psychological and Physical Impacts of Cyber-attacks on Employees

Cyber-attacks can have an extensive psychological and physical impact on people and society. According to research, being a victim of cyber violence can cause desperation, stress, and loneliness, and also have a severe impact on physical and emotional well-being. Research[33] showed that procedural security countermeasure awareness increases protection motivation components, which in turn enhances cyberspace protective behavior. Furthermore, cyber-attacks and cyberbullying in Malaysian workplaces have significant psychological and physical effects on employees. Perceived severity, vulnerability, and self-efficacy all influence cybersecurity behavior among government personnel[34]. The rise of remote work during the COVID-19 pandemic has increased workplace cyberbullying, which can lead to post-traumatic stress disorder, psychiatric disorders, and even suicide[46]. Unequal power relations, anonymity, and cross-border connections are all factors that contribute to cyberbullying. The current legal framework in Malaysia is insufficient for handling cyberbullying, emphasizing the need for stronger legislation and management techniques[46]. Recent Malaysian research has highlighted the effects of cyberbullying on the mental health of healthcare employees and medical students. Hospital staff that experienced cyberbullying had weak positive relationships with depression ( $r=0.258$ ) and anxiety ( $r=0.276$ ) levels[47]. Similarly, medical students who were victims of cyberbullying were more likely to experience melancholy, anxiety, and stress[48]. During the COVID-19 pandemic, healthcare workers at Sarawak General Hospital encountered low levels of anxiety, stress, and depression, with female employees reporting considerably higher levels of worry and stress than male coworkers[49]. A study of emergency medical officers in Malaysian hospitals indicated that anxiety was the most prominent psychological disorder (28.6%), followed by depression (10.7%) and stress (7.9%), with male officers suffering considerably more anxiety than females[50].

#### D. OSHA Regulation in Malaysia

The Occupational Safety and Health Act (OSHA) of 1994, based on the Australian Occupational Health and Safety Act of 1983, was introduced to minimize industrial accident rates in Malaysia. This legislation is based on the idea of self-regulation, requiring employers to comply with safety regulations out of self-interest rather than depending only on government consequences. Employers and employees must work together to guarantee workplace safety and prevent health and safety issues from being marginalized. Under OSHA 1994, the penalty for employers who fail to follow the established safety requirements was doubled to RM50,000, two years in



prison, or both. Errant employers could face RM1,000 fine, three months in prison, or both[51].

Recent OSHA modifications have significantly raised the penalties for breaches, emphasizing the significance of compliance. Notable changes include increasing the maximum fine for failing to guarantee employee safety, health, and welfare from RM50,000 to RM500,000. Furthermore, the maximum amount under Section 51 for general penalties has been raised from RM10,000 to RM100,000, with a daily fee for continuing offenses increasing from RM1,000 to RM2,000. The maximum fine for failing to comply with improvement or limitations orders has been increased from RM50,000 to RM500,000, with a fine of RM500 to RM2,000 for each day of noncompliance. Other important changes include doubling the penalties for failing to form a safety and health committee from RM5,000 to RM100,000 and increasing the maximum prison six months to one year. Furthermore, the fine for failing to designate a safety and health officer has been raised from RM5,000 to RM50,000. Overall, this legislative evolution is an important step towards enhancing workplace safety standards and promoting a safety-first culture in Malaysia's businesses[52].

Moreover, in Malaysia, the Department of Occupational Safety and Health (DOSH) under the Ministry of Human Resources is in charge of executing the 1994 occupational safety and health law[51][53]. The Occupational Health Unit oversees monitoring efforts. Hospitals and clinics under the Ministry of Health are responsible for notifying workers about workplace poisonings, infections, and injuries. Malaysia's Social Security Organization (SOCSO), also known as Pertubuhan Keselamatan Sosial (PERKESO), was established in 1971 to provide socioeconomic security to non-government employees[54][55]. The Employees Social Security Act of 1969 encourages all businesses to insure their employees for workplace diseases or injuries by contributing to SOCSO[56]. Data from SOCSO are more thorough than those acquired from Malaysia's Department of Safety and Health. Up to 2006, SOCSO employed 67% of Malaysia's total formal employment[38]. SOCSO offers employment injury insurance, disability compensation, rehabilitation programs, and certified training programs for disability assessment (CMIA)[57][58]. The government and business sectors both provide workers' compensation for injuries[59]. The Persons with Disability (PWD) Act of 2008 allows PWDs to gain a variety of benefits, particularly the right to special barrier-free access to public facilities. The Labour Department offers a number of vocational programs to help people with disabilities get jobs. SOCSO established the Return-To-Work (RTW) program in 2007 to help injured workers regain their full functional capacity at work. The RTW process is separated into four phases: off-duty, reentry, maintenance, and advancement. The Ministry of Human Resources manages the RTW programs[60].

### III. METHODOLOGY

This study explores the relationship between cybersecurity practices, digital threats, and employee safety in Malaysian workplaces, with an emphasis on the potential for integrating cybersecurity measures into OSHA standards. The methodology for this research combines qualitative data collection and analysis using NVivo to derive insights from industry interviews.

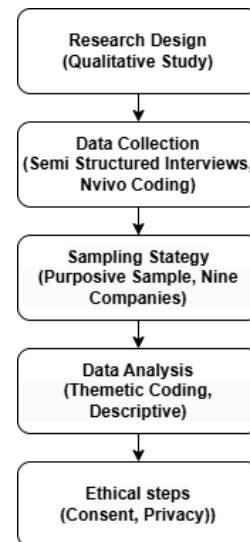


Fig. 1. Research Methodology

#### A. Research Design

A qualitative research approach was selected to gain in-depth insights into how organizations in Malaysia perceive and manage cybersecurity risks concerning employee safety. This approach enables a detailed understanding of company-specific cybersecurity practices, the psychological impact of digital threats on employees, and perspectives on regulatory changes involving OSHA standards. A cross-sectional study design was chosen to capture data from multiple organizations at a single point in time, offering a snapshot of current cybersecurity and safety practices.

#### B. Data Collection Methods

Data was collected via semi-structured interviews involving key personnel from various Malaysian companies, including IT managers, Human Resource professionals, and safety officers. These interviews explored three major areas: measures being employed in information security, employee stress due to digital threats, and the level of support for integrating cybersecurity into OSHA standards.

Prior to the research semi-structured interviews were conducted. Interviews were conducted with representatives from nine companies across different sectors, such as telecommunications, manufacturing, and digital services. Each interview lasted approximately 30-45 minutes which was conducted virtually and physically to accommodate participant schedules and maintain data security. Interview questions included topics like:

- The types of cybersecurity protocols currently in place.
- The psychological impact of cybersecurity threats on employees.
- Opinions on the potential for including cybersecurity in OSHA standards.

**Use of Nvivo 15 Software:** For the data analysis Nvivo 15 software was used. These interviews were first transcribed and then coded within Nvivo 15 to identify the emergence of specific themes, categorize responses, and underscore insights

within three primary areas of interest. In this regard, the usage of NVivo has been found quite helpful because it allows for easy coding and organization; thus, patterns in organizational practices, impacts on employees, and regulatory perspectives are identified.

**Interview protocol:** The interview schedule was designed with a set of open-ended questions to gather comprehensive insights into participants' views on integrating cybersecurity and digital threat management into OSHA (Occupational Safety and Health Administration) standards within Malaysian workplaces. The questions aimed to explore participants' experiences with workplace cybersecurity measures, their perceptions of current safety standards, and the perceived importance of governmental policies in safeguarding against digital threats. Sample questions included:

1. How does your company protect employees from cyber threats like hacking or data breaches?
2. How have digital threats affected employees in your company?
3. How can cyberattacks lead to stress or mental health issues for employees?
4. How does your company ensure both employee safety and data security?
5. How should safety regulations (like OSHA) include protections against digital threats?
6. How do you train employees to spot and avoid cyber threats like phishing or ransomware?
7. How do you handle the challenges of keeping employees safe from cyber threats?
8. How would including cybersecurity rules in workplace safety standards help employees?
9. How should the government enforce cybersecurity rules in the workplace?
10. How do you see workplace safety evolving with the rise of digital threats?

#### C. Sampling Strategy

A purposive sample approach was utilized to identify organizations that are likely to have developed cybersecurity policies since they operate in industries with greater digital security needs, such as banking, telecommunications, and government services. The selection criteria assured a diverse range of viewpoints, notably on cybersecurity's influence on employee safety. Aside from that, the research included participants from nine firms, offering a comprehensive assessment of current workplace procedures and attitudes concerning cybersecurity.

#### D. Data Analysis

All interviews were transcribed and imported into NVivo15 for analysis. Transcripts were coded thematically, with a focus on cybersecurity practices, employee safety and stress, and support for OSHA integration. Three major themes were pre-defined for coding: (1) Cybersecurity Measures on Employee Safety, (2) Digital Threats on Employee Well-being, and (3) OSHA Standards and Employee Safety. Thematic analysis was conducted to identify patterns within each theme. This process

involved organizing the data into sub-themes to capture nuanced insights, such as the psychological impact of digital threats, role-based access controls, and continuous employee training on digital security. Quantitative coding percentages were also applied to measure coverage, allowing for a more detailed understanding of the emphasis each company placed on the different aspects of cybersecurity.

#### E. Ethical Considerations

Ethical considerations were prioritized throughout the study to ensure participant privacy and confidentiality. Every participant was given a document that explained the aim of the research, the protocols for processing data, and their ability to withdraw from the study at any point in time to provide informed consent. Furthermore, in order to preserve sensitive information for the purpose of the research, the names of companies and the identities of individual employees were anonymized. This was done in particular with regard to cybersecurity methods and procedures. Moreover, in order to preserve the integrity of the data and protect anonymity, all of the data, including transcriptions and recordings of interviews, were kept in a safe location and only the study team had access to them.

#### F. Limitations

This qualitative research, using purposeful sampling, may not reflect the wider industrial context. Participants from industries possessing substantial digital assets may prioritize cybersecurity more than those from other sectors. The swiftly changing cybersecurity environment may make some conclusions time-sensitive due to the ongoing emergence of new threats and technology.

#### G. Company Selection Justification

This research identified nine companies: Bigledger Sdn Bhd, Kode Digital Expert, Kollect, KONE Elevator (M) Sdn Bhd, Pinnacle, Nestlé, Tectiera, Zero-day Security, and the ICT Department of Albukhary International University. The selection of these organizations was purposeful, and intended to include a variety of viewpoints across sectors with distinct digital safety issues, including digital services, manufacturing, telecommunications, consumer products, and education. Every firm has instituted cybersecurity protocols, rendering it essential to examine how OSHA regulations can integrate digital safety into employee protection frameworks. This selection provides a comprehensive examination of how several Malaysian sectors are now addressing digital threats, along with insights on the prospective advantages of integrating cybersecurity into OSHA safety regulations. The varied range of companies facilitates a comprehensive understanding of industry-specific strategies and their effectiveness in mitigating cybersecurity threats and enhancing overall workplace safety.

### IV. FINDINGS

According to the research findings, it is clear that all companies under analysis have set cybersecurity policies that enhance positive change to the safety and welfare of their employees by addressing the risks posed by digital threats. They also promote a higher awareness of proper behavior on the Internet among employees. The analysis was conducted using NVivo software. The analysis highlights company-specific strategies, the psychological impact of digital threats on employees, and strong support for integrating cybersecurity within OSHA standards.

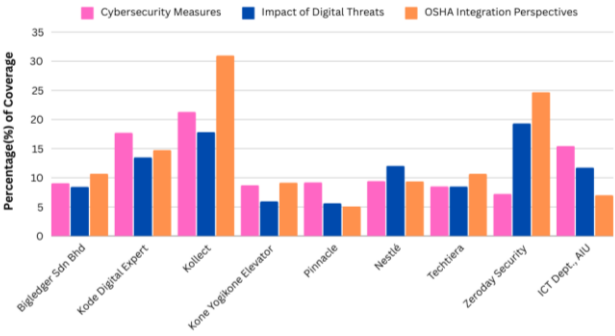


Fig. 2. Percentage Coverage of Cybersecurity Themes Across Companies

A. Cybersecurity Protocols and Impact on Employee Safety

TABLE I. IMPACT OF CYBERSECURITY ON EMPLOYEE SAFETY

Company	Cybersecurity on Employee Safety	Percentage of Coverage
Bigledger Sdn Bhd	Implements multi-layered security protocols (e.g., firewalls, intrusion detection) and regular training to enhance safety awareness and reduce stress.	9.07%
Kode Digital Expert	Uses strong security software, and two-step login systems, and conducts regular updates and training on cyber threat identification.	17.72%
Kollect	Prioritizes employee training on phishing, password security, and network monitoring, which helps reduce anxiety about digital threats.	21.32%
Kone Elevator	Enforces a code of conduct for data security, role-based access control, and continuous employee training on recognizing cyber threats.	8.72%
Pinnacle	Uses multi-factor authentication and regular cybersecurity training to reduce stress associated with handling sensitive data.	9.21%
Nestlé	Employs advanced threat detection systems, routine security audits, and practical cybersecurity training to reinforce digital safety.	9.45%
Techiera	Adopts zero-trust architecture and multi-factor authentication to minimize employee anxiety about data leaks and cyber threats.	8.52%
Zeroday Security	Uses a multi-layered security approach and provides mental health resources to help employees manage stress from cyber threats.	7.25%
ICT Departme nt, Albukhary Internatio nal University (AIU)	Employs strict cybersecurity protocols, including firewalls, multi-factor authentication, and network monitoring; provides regular training and empowers employees to report issues.	15.46%

Result: This research indicates that all companies and organizations have strong cybersecurity policies in place, according to analysis, such measures effectively reduce stress related to cyber threats and are beneficial for company employees as these contribute positively to both employee safety and well-being; This implies that precaution, sensitization, and rigorous security procedures make employees have believed in the organization to deal with digital threats.

B. Digital Hazard Impact on Employee Safety

TABLE: II. IMPACT OF DIGITAL THREATS ON EMPLOYEE SAFETY

Compan y	Digital Threats on Employee Safety	Percentage of Coverage
Bigledger Sdn Bhd	Digital threats create a heightened need for vigilance, adding stress, particularly with advanced phishing tactics.	8.45%
Kode Digital Expert	Increased digital threats cause unease about data safety and add workload in the event of a security incident.	13.51%
Kollect	Enhanced security measures increase vigilance, yet add to stress and burnout risk due to continuous adherence to protocols.	17.84%
Kone Elevator	Educates employees on identifying phishing and other cyber threats, mitigating risks to financial and personal data.	5.93%
Pinnacle	High sensitivity of data handled increases employee stress, necessitating frequent cybersecurity education.	5.60%
Nestlé	Unchecked digital threats impact productivity, requiring constant employee vigilance to assure safety.	12.06%
Techiera	Cyber threats disrupt workflows and increase anxiety; mental health support is provided to ease stress.	10.56%
Zeroday Security	Elevated cybersecurity responsibilities add stress; continuous training mitigates the psychological impact.	19.35%
ICT Departme nt, Albukhar y Internatio nal Universit y (AIU)	Digital threats increase awareness and responsibility, yet add stress, particularly due to phishing scams and the potential compromise of personal/professional data.	11.76%

Result: Digital threats increase stress and conscientiousness among employees, particularly those dealing with confidential information. This leads to the necessity for consistent cybersecurity training and mental health support and counseling services to counteract the psychological impact of digital safety responsibilities. Employees are thus more aware of the risks posed by digital technology but they undergo increased pressure to meet security demands on the technology to keep their working place secure from any sort of cyberattacks.

### C. OSHA Standards and Employee Safety

TABLE: III. OSHA STANDARDS AND EMPLOYEE SAFETY

Company	OSHA Standards and Employee Safety	Percentage of Coverage
Bigledger Sdn Bhd	Advocates integrating digital safety within OSHA standards, recommending regular cybersecurity training and clear incident protocols.	10.70%
Kode Digital Expert	Suggests that digital safety should be treated similarly to physical safety standards for better employee protection.	14.76%
Kollect	Strongly supports expanding OSHA to include cybersecurity as part of workplace safety, promoting comprehensive employee protection.	31.00%
Kone Elevator	It recommends that OSHA mandate regular cybersecurity audits, data protection protocols, and employee training.	12.69%
Pinnacle	Emphasizes a need for formal cybersecurity standards as part of workplace safety to protect employees effectively.	24.71%
Nestlé	Proposes OSHA guidelines to include cybersecurity practices to safeguard data and ensure employee safety.	9.38%
Techtiera	Endorses OSHA's inclusion of cybersecurity for protecting digital safety in remote and on-site work environments.	10.68%
Zeroday Security	Recommends mandatory cybersecurity training, audits, and clear OSHA guidelines for digital safety in the workplace.	24.71%
ICT Department , Albukhary International University (AIU)	Supports integrating cybersecurity in safety standards to ensure organizations prioritize employee protection in both physical and digital domains.	7.03%

Result: According to the data shown above, the opinions of the companies surveyed are highly favorable toward integrating cybersecurity issues into OSHA standards. This would make structured guidelines and mandate cybersecurity practices in a way that would enhance the overall safety of the employees with recommendations that focus not only on safety from physical harm but also cyber harm.

### V. DISCUSSION

This research investigates the influence of cybersecurity practices in the protection of employees at the Malaysian workplace and the possibility of incorporating cybersecurity into the OSHA objective. Results suggest that cybersecurity measures, employee stress, and the demand for legal protection in the online environment are correlated.

#### A. Interpretation of Findings and Comparison with Previous Research

The study confirms that all companies in the sample use multiple layers of protection including firewalls, multiple-factor authentication (MFA), and the use of updated software. The current framework correlates with the ideas highlighted by [42], [61] in that, an enhanced system of security is necessary to prevent unauthorized access and data breaches. An opportunity for employee training appeared in companies as an interesting aspect since cybersecurity awareness seems to be a constant requirement in the contemporary business environment[39]. However, apart from these technical measures, there are psychological effects of digital threats. Researchers have mentioned that managing cybersecurity threats affects mental health as well as employees' stress levels[34], [46]. This study reaffirms the findings of prior studies in emphasizing that cybersecurity is not just a technological problem, but a business issue as well, largely due to employees' stress and anxiety over security threats and the need for protection against them. The results also reveal a high level of approval for including cybersecurity under OSHA regulations, reflecting comparability to trends in worldwide regulation of workplace security. The regulatory bodies can respond to some of the new digital risks that are evolving in the Workplace Safety Issuers environment[28]. Bodies like Albukhary International University (AIU) ICT Department and Bigledger Sdn Bhd its part said that implementing the OSHA guidelines for Cybersecurity would aid in the formulation of cybersecurity policies as a structured extension of physical safety.

#### B. Broader Implications

It emerged from the study that integrating cybersecurity into OSHA standards could play a transformative role in enhancing workplace safety and well-being. For organizations, this approach would emphasize the importance of proactive cybersecurity that creates a structured culture of vigilance where employees feel supported and protected. The focus on employee training can be explained by the fact that cybersecurity is logistical in terms of technology and people, which states that the "human element" is vital in effective cybersecurity strategies[62]. In the broader context of workplace safety, these findings suggest that cybersecurity training and awareness could become as foundational as physical safety training, particularly in sectors heavily reliant on digital infrastructure and for industries that are dependent on digital assets. By formalizing digital safety practices, OSHA could support companies in establishing consistent, high-level cybersecurity standards. It will enable organizations to prioritize digital protections without compromising employee well-being or operational efficiency.



### C. Study Limitations and Future Research Directions

Despite its contributions, this study has the following limitations. The sample is representative and diverse at the same time but might seem insufficient when investigating organizations in various industries. This may become also a limitation of the study since different industries may have different levels of integration of the digital environment and related risks including cyber threats. Further research can be extended to a broader range of sectors and organizations: therefore, the findings of the present study can be considered as an attempt to provide a more generalized picture of the role of cybersecurity in the protection of employees' safety. Additionally, although this paper shows how cybersecurity responsibilities affect mental health, it does not measure the psychological effects of digital threats. Exploratory research can now be conducted on how the above preoccupations evolve over a long period, impacting employee well-being, as pointed out by [34], [46]. Further research into the long-term effects of digital threats on mental health would provide a richer perspective on the relationship between cybersecurity and employees' welfare. Another area for future exploration involves a study regarding the evaluation of the practical feasibility of implementing cybersecurity into OSHA standards. New technologies can provide good solutions for occupational safety but may require industry-specific adaptations to some extent [38]. Research that investigates how different industries can adapt OSHA cybersecurity standards could be beneficial for both policymakers and organizations looking to enhance digital safety.

### VI. RECOMMENDATIONS AND CONCLUSION

This study underscores the importance of cybersecurity measures in promoting a safe and supportive workplace, particularly in digital-intensive environments. Findings indicate a strong alignment between robust cybersecurity protocols and reduced employee stress, highlighting the potential benefits of extending OSHA standards to encompass digital threats. The proactive approach to cybersecurity evident in the companies surveyed, including AIU ICT Department and Kollect, points to a growing need for regulatory frameworks that address both physical and digital safety in the workplace. The study recommends that companies continue to invest in comprehensive cybersecurity training and mental health resources for employees responsible for managing digital security. These initiatives suggested a holistic approach to digital safety that can improve employee resilience against cyber threats while maintaining operational security. Future regulatory guidelines could support these efforts by providing consistent standards that organizations can adopt, enhancing overall workplace safety, and fostering a culture where both physical and digital security are prioritized.

In conclusion, the integration of cybersecurity within OSHA standards would represent an essential evolution in workplace safety, reflecting the modern challenges faced by digitized industries. This study highlights the significance of cybersecurity as a multidimensional concept encompassing

technology, mental health, and regulatory oversight. A structured regulatory approach to cybersecurity within workplace safety frameworks would enable organizations to better protect employees from the dual pressures of physical and digital threats, ultimately leading to safer and more resilient work environments.

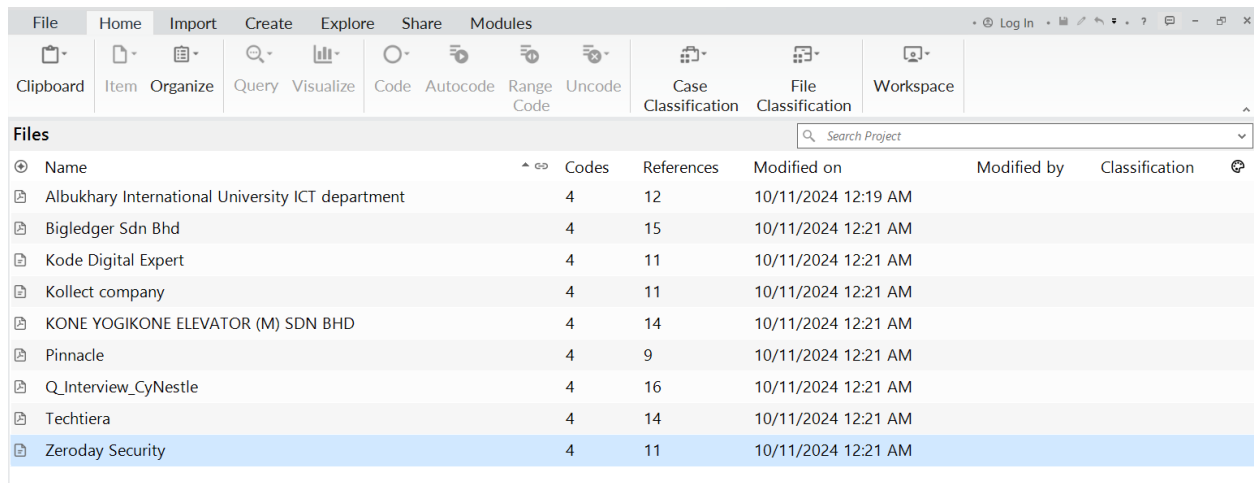
### REFERENCES

- [1] Ujjwal Rao, "Overview of Cyber Security," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 47–51, Apr. 2023, doi: 10.48175/ijarsct-9470.
- [2] Prof. Aarti R. Naik, "Cybersecurity in Business," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 367–374, Mar. 2024, doi: 10.48175/ijarsct-15764.
- [3] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the top five evolving threats in cybersecurity: an in-depth overview," *Mesopotamian journal of cybersecurity*, vol. 2023, pp. 57–63, 2023.
- [4] D. A. Bajpai, "International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT)," *International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT)* (April 01, 2024). *International Journal of Advanced Research in Science, Communication and Technology*, 0 [10.48175/ijarsct-16987], 2024.
- [5] P. N. Akpa, "PW 0348 Innovative solutions on the effects of emerging risks related to occupational safety and health arising from digitalization of work," 2018, BMJ Publishing Group Ltd.
- [6] F. Costantino, A. Falegnami, L. Fedele, M. Bernabei, S. Stabile, and R. Bentivenga, "New and emerging hazards for health and safety within digitalized manufacturing systems," *Sustainability*, vol. 13, no. 19, p. 10948, 2021.
- [7] A. Howarth, J. Quesada, J. Silva, S. Judycki, and P. R. Mills, "The impact of digital health interventions on health-related outcomes in the workplace: a systematic review," *Digit Health*, vol. 4, p. 2055207618770861, 2018.
- [8] L. Hou, S. Wu, G. Zhang, Y. Tan, and X. Wang, "Literature review of digital twins applications in construction workforce safety," *Applied Sciences*, vol. 11, no. 1, p. 339, 2020.
- [9] M. J. Kuczabski, "Threats associated with digital technology in the workplace," 2021.
- [10] A. Sleem, "A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age," *Journal of Cybersecurity & Information Management*, vol. 10, no. 2, 2022.
- [11] A. Tamrakar and B. Patra, "CYBERSECURITY THREATS AND COUNTERMEASURES: A REVIEW," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 9, no. 3, pp. 1400–1404, 2018.
- [12] J. Tully, J. Selzer, J. P. Phillips, P. O'Connor, and C. Dameff, "Healthcare challenges in the era of cybersecurity," *Health Secur*, vol. 18, no. 3, pp. 228–231, 2020.
- [13] I. G. Cohen, S. Hoffman, and E. Y. Adashi, "Your money or your patient's life? Ransomware and electronic health records," 2017, American College of Physicians.
- [14] L. J. Trautman and P. C. Ormerod, "Wannacry, ransomware, and the emerging threat to corporations," *Tenn. L. Rev.*, vol. 86, p. 503, 2018.
- [15] A. O'Dowd, "Major global cyber-attack hits NHS and delays treatment," May 15, 2017. doi: 10.1136/bmj.j2357.
- [16] S. Preetha, P. Lalasa, and R. Pradeepa, "A comprehensive overview on cybersecurity: threats and attacks," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 10, no. 8, pp. 98–106, 2021.
- [17] P. A. Schulte, G. Delclos, S. A. Felknor, and L. C. Chosewood, "Toward an expanded focus for occupational safety and health: a commentary," *Int J Environ Res Public Health*, vol. 16, no. 24, p. 4946, 2019.
- [18] T. P. Fuller, "Introduction to Global Occupational Safety and Health," in *Global Occupational Safety and Health Management Handbook*, CRC Press, 2019, pp. 1–17.
- [19] J. L. Lu, "Occupational Safety and Health amid the Global Pandemic," *Acta Med Philipp*, vol. 56, no. 1, 2022.



- [20] C. D. Reese, *Occupational safety and health: fundamental principles and philosophies*. Crc Press, 2017.
- [21] N. K. Tharshini, F. H. Mas'ud, and Z. Hassan, "Level of cybercrime threat during the outbreak of COVID-19 pandemic: A study in Malaysia,," *International Journal of Academic Research in Business and Social Sciences*, vol. 12, no. 5, pp. 40–51, 2022.
- [22] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks," *Information*, vol. 13, no. 9, p. 413, 2022.
- [23] C. S. Ganesh and R. Krishnan, "A review of occupational injury research in Malaysia," *Med J Malaysia*, vol. 71, no. Suppl 1, pp. 100–104, 2016.
- [24] K. Anwar and M. Syafiq, "Amendment to Occupational Safety and Health Act (OSHA): Relevant changes," Available at SSRN 4497209, 2023.
- [25] R. Azmi, S. N. S. Ahmad, and B. A. M. Kamil, "Mental health issues at workplace: An overview of law and policy in Malaysia and United Kingdom (UK)," *Health N Hav*, vol. 5, pp. 316–329, 2020.
- [26] C. P. Rodrigues and P. Ochôa, "Cybersecurity and personal data: which aspects influence safety in the workplace," 2022.
- [27] R. Houston, "Thriving Cybersecurity Professionals: Building a Resilient Workforce and Psychological Safety in the Federal Government," University of Pennsylvania, Pennsylvania, 2019.
- [28] I. Mukhopadhyay, "Cyber threats landscape overview under the new normal," in *ICT Analysis and Applications*, Springer, 2022, pp. 729–736.
- [29] Z. ALsaed and M. Jazzar, "Covid-19 age: Challenges in cybersecurity and possible solution domains," *J Theor Appl Inf Technol*, vol. 99, no. 11, pp. 2648–2658, 2021.
- [30] T. Ahmad, "Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity," Available at SSRN 3568830, 2020.
- [31] K. Curran, "Cyber security and the remote workforce," *Computer Fraud & Security*, vol. 2020, no. 6, pp. 11–12, 2020.
- [32] C. Subramaniam, F. M. Shamsudinb, and A. S. I. Alshuaibic, "Investigating employee perceptions of workplace safety and safety compliance using PLS-SEM among technical employees in Malaysia," *Journal of Applied Structural Equation Modeling*, vol. 1, no. 1, pp. 44–61, 2017.
- [33] N. Humaidi and S. H. A. Alghazo, "Procedural information security countermeasure awareness and cybersecurity protection motivation in enhancing employee's cybersecurity protective behaviour," in *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, 2022, pp. 1–10.
- [34] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks," *Information*, vol. 13, no. 9, p. 413, 2022.
- [35] S. A. Mim, R. Rahman, M. R. Al Asif, K. F. Hasan, and R. Khondoker, "Cybersecurity Attacks and Vulnerabilities During COVID-19," in *International Conference on Advanced Information Networking and Applications*, Springer, 2023, pp. 532–545.
- [36] J. B. H. Yap, K. P. H. Lee, and C. Wang, "Safety enablers using emerging technologies in construction projects: empirical study in Malaysia," *Journal of engineering, design and technology*, vol. 21, no. 5, pp. 1414–1440, 2023.
- [37] N. A. Amirah, W. I. Asma, S. Muda, and A. Amin, "Operationalisation of safety culture to foster safety and health in the Malaysian Manufacturing Industries," *Asian Soc Sci*, vol. 9, no. 7, p. 283, 2013.
- [38] J. E. Doodoo, H. Al-Samarraie, A. I. Alzahrani, M. Lonsdale, and N. Alalwan, "Digital Innovations for Occupational Safety: Empowering Workers in Hazardous Environments," *Workplace Health Saf*, vol. 72, no. 3, pp. 84–95, 2024.
- [39] J. R. Henrichsen, M. Betz, and J. M. Lisosky, *Building digital safety for journalism: A survey of selected issues*. UNESCO Publishing, 2015.
- [40] P. V Moore, "Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management," Springer, pp. 292–315, 2019.
- [41] M. J. Kuczabski, "Threats associated with digital technology in the workplace," 2021.
- [42] A. Sleem, "A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age,," *Journal of Cybersecurity & Information Management*, vol. 10, no. 2, 2022.
- [43] H. T. Woldemichael, "Emerging Cyber Security Threats in Organization," *International Journal of Scientific Research in Network Security and Communication*, vol. 7, no. 6, pp. 7–10, 2019.
- [44] P. L. Gallegos-Segovia, J. F. Bravo-Torres, V. M. Larios-Rosillo, P. E. Vintimilla-Tapia, I. F. Yuquilima-Albarado, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," in *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, IEEE, 2017, pp. 1–6.
- [45] W. Fuertes et al., "Impact of social engineering attacks: A literature review," *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*, pp. 25–35, 2022.
- [46] W. R. W. Rosli, S. N. Ya'cob, M. H. A. Bakar, and M. S. M. Bajury, "Governing the risks of cyber bullying in the workplace during the era of COVID-19," *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, vol. 6, no. 10, pp. 334–342, 2021.
- [47] A. N. A. T. S. Thurai Singam and N.-A. Abdullah, "Cyber Bullying among Hospital Staff and its Influence on Mental Health and Professionalism," *International Journal of Academic Research in Business and Social Sciences*, vol. 12, no. 9, Sep. 2022, doi: 10.6007/ijarbss/v12-i9/14076.
- [48] M. H. L. Lee, M. Kaur, V. Shaker, A. Yee, R. Sham, and C. S. Siau, "Cyberbullying, social media addiction and associations with depression, anxiety, and stress among medical students in Malaysia," *Int J Environ Res Public Health*, vol. 20, no. 4, p. 3136, 2023.
- [49] S. S. Kiat et al., "Psychological symptoms among healthcare workers handling COVID-19 patients," *Med. J. Malays*, vol. 76, pp. 138–144, 2021.
- [50] S. N. Yahaya, S. F. A. Wahab, M. S. B. Yusoff, M. A. M. Yasin, and M. A. A. Rahman, "Prevalence and associated factors of stress, anxiety and depression among emergency medical officers in Malaysian hospitals," *World J Emerg Med*, vol. 9, no. 3, p. 178, 2018.
- [51] A.-R. Abdul-Aziz and A.-A. Hussin, "Construction safety in Malaysia: A review of industry performance and outlook for the future," *Journal of Construction Research*, vol. 4, no. 02, pp. 141–153, 2003.
- [52] K. Anwar and M. Syafiq, "Amendment to Occupational Safety and Health Act (OSHA): Relevant changes," Available at SSRN 4497209, 2023.
- [53] R. Hassan, A. R. Ismail, N. K. Makhtar, and N. Jusoh, "Improving occupational safety and health (OSH) enforcement among employers in manufacturing sector in Kelantan," in *AIP Conference Proceedings*, AIP Publishing, 2021.
- [54] A. B. L. Abas, A. R. B. M. Said, M. A. B. A. Mohammed, and N. Sathiakumar, "Occupational disease among non-governmental employees in Malaysia: 2002-2006," *Int J Occup Environ Health*, vol. 14, no. 4, pp. 263–271, 2008.
- [55] A. B. L. Abas, D. A. R. B. Mohd Said, M. A. B. Aziz Mohammed, and N. Sathiakumar, "Fatal occupational injuries among non-governmental employees in Malaysia," *Am J Ind Med*, vol. 56, no. 1, pp. 65–76, 2013.
- [56] R. R. R. Shaharuddin, L. A. Mutalib, and H. Hashim, "The concept of rights and protection to employees: A comparative overview," *International Journal of Islamic Thought*, vol. 4, p. 58, 2013.
- [57] M. A. B. A. Mohammed, "The Return to Work Programme in Malaysia-investing in people," *International Journal of Disability Management*, vol. 9, p. e8, 2014.
- [58] E. P. H. Cheong, "Developing the Social Security Organisation (SOCO) of Malaysia's RTW case management system," *International Journal of Disability Management*, vol. 9, p. e44, 2014.
- [59] D. Appel and P. S. Borba, "Costs and Prices of Workers' Compensation Insurance," in *Workers' Compensation Insurance Pricing: Current Programs and Proposed Reforms*, Springer, 1988, pp. 1–17.
- [60] C. S. Ganesh and R. Krishnan, "A review of occupational injury research in Malaysia," *Med J Malaysia*, vol. 71, no. Suppl 1, pp. 100–104, 2016.
- [61] Prof. Aarti R. Naik, "Cybersecurity in Business," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 367–374, Mar. 2024, doi: 10.48175/ijarsct-15764.
- [62] L. A. Jones, "Unveiling Human Factors: Aligning Facets of Cybersecurity Leadership, Insider Threats, and Arsonist Attributes to Reduce Cyber Risk," *SocioEconomic Challenges*, vol. 8, no. 2, pp. 44–63, 2024.

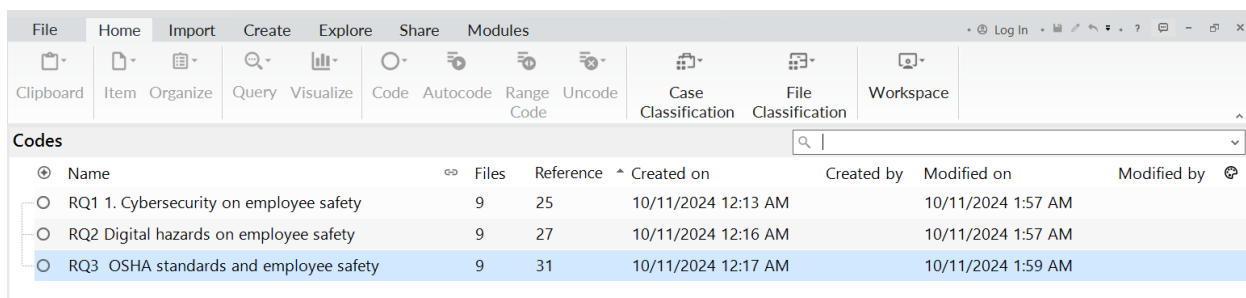
# APPENDIX



The screenshot shows the Nvivo 15 Software interface with the 'Files' table selected. The table lists various files and their associated codes and references. The 'Files' table has columns: Name, Codes, References, Modified on, Modified by, and Classification. The data is as follows:

Name	Codes	References	Modified on	Modified by	Classification
Albukhary International University ICT department	4	12	10/11/2024 12:19 AM		
Bigledger Sdn Bhd	4	15	10/11/2024 12:21 AM		
Kode Digital Expert	4	11	10/11/2024 12:21 AM		
Kollect company	4	11	10/11/2024 12:21 AM		
KONE YOGIKONE ELEVATOR (M) SDN BHD	4	14	10/11/2024 12:21 AM		
Pinnacle	4	9	10/11/2024 12:21 AM		
Q_Interview_CyNestle	4	16	10/11/2024 12:21 AM		
Techtiera	4	14	10/11/2024 12:21 AM		
Zero day Security	4	11	10/11/2024 12:21 AM		

Fig. 3. Research Data Analysis Using Nvivo 15 Software



The screenshot shows the Nvivo 15 Software interface with the 'Codes' table selected. The table lists various codes and their associated files and references. The 'Codes' table has columns: Name, Files, Reference, Created on, Created by, Modified on, and Modified by. The data is as follows:

Name	Files	Reference	Created on	Created by	Modified on	Modified by
RQ1 1. Cybersecurity on employee safety	9	25	10/11/2024 12:13 AM		10/11/2024 1:57 AM	
RQ2 Digital hazards on employee safety	9	27	10/11/2024 12:16 AM		10/11/2024 1:57 AM	
RQ3 OSHA standards and employee safety	9	31	10/11/2024 12:17 AM		10/11/2024 1:59 AM	

Fig. 4. Research Key Objectives Analysis Using Nvivo 15 Software