Copyright © 2023 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2023. Vol. 17(2): 112–132. DOI: 10.5281/zenodo.4766708
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Factors Effecting Cyber Incident Occurrence: Mediating Role of Cyber Incident Reporting Mechanism

Muhammad Awais Bhatti*[1]
Department of Management, School of Business,
King Faisal University, Al-Ahsa 31982, Saudi Arabia.

***Saima Jamil*[2]**
Department of Computer Sciences, Virtual University of Pakistan,
Peshawar Campus, Pakistan.

Abstract

The issue of Cyber security is of utmost importance for organisations, given that the presence of Cyber Incident occurrence presents significant vulnerabilities to the integrity and confidentiality of data. The present study aims to examine the factors that contribute to Cyber Incident occurrence and evaluate the efficacy of Cyber incident reporting mechanisms in mitigating such threats within a range of Saudi organisations. The study utilises quantitative methods to thoroughly investigate the phenomenon of cyber incident occurrence. Data was collected from a sample of 219 employees who held various positions and worked in different departments. Data was analyzed using Structural Equation Modelling (SEM) with Amos. The measurement instrument underwent thorough evaluation to establish its reliability and validity, thereby ensuring the credibility of the collected data. The study's results demonstrate multiple noteworthy direct and indirect impacts. The relationship between "Employee Training and Awareness," "Access Control & Monitoring," and "Insider Threat Detection & Reporting" indirectly influences the occurrence of Cyber incidents mediated by Cyber Incident Reporting Mechanisms. These findings highlight the significance of implementing effective reporting mechanisms to mitigate the frequency of Cyber incidents. The mediation effect of "Cyber Incident Reporting Mechanisms" is not supported in relation to "Organisational Innovativeness Culture" and "Employee Satisfaction." These findings demonstrate the intricate nature of these connections, suggesting that the presence of an innovative culture and high employee satisfaction may not directly influence the occurrence of Cyber incidents when reporting mechanisms are

[1] Associate Professor, Department of Management, College of Business,
King Faisal University, Al-Ahsa 31982, Saudi Arabia.

[2] Department of Computer Sciences, Virtual University of Pakistan,
Peshawar Campus, Pakistan. Email: Saima.Jamil@vu.edu.pk
* Corresponding Author Email: mbhatti@kfu.edu.sa

taken into account. The study also conducts a thorough evaluation of the measurement model fit, which indicates a strong fit across multiple indices, confirming the high quality and reliability of the measurement instrument. In conclusion, this study provides insights into the complex nature of Cyber Incident occurrence within Saudi organisations. This emphasises the importance of "Cyber Incident Reporting Mechanisms" in mitigating these threats and underscores the necessity for organisations to invest in employee training, access control, monitoring, and robust insider threat detection and reporting systems to enhance Cyber security. These insights offer valuable guidance for organisations seeking to protect their data and uphold a secure work environment amidst changing Cyber Incident occurrence.

Keywords: Access Control and Monitoring (ACM), Employee Satisfaction (ES), Cyber Incident Occurrence (CIO), Cyber Incident Reporting Mechanisms (CIRM) and Insider Threat Detection and Reporting (ITDR).

1. Introduction

The realm of Cybersecurity is perpetually expanding, thereby necessitating heightened attention to safeguarding sensitive data against a diverse range of malicious intrusions, which has emerged as a pressing priority for enterprises. The covert characteristics of Cyber Incident occurrence, which emanate from internal sources within an organisation as opposed to external origins, often receive less attention compared to the prevalence of external threats in discussions. In the present context, it has become imperative to acquire a comprehensive understanding, identify, and effectively mitigate the internal threats originating from within the organisation. This proposed study aims to conduct a thorough examination of the complex issue presented by Cyber Incident occurrence, delving into crucial factors that contribute to an organisation's susceptibility. This component comprises several factors, including Organisation Culture (OC), Employee Training and Awareness (ETA), Access Control and Monitoring (ACM), Employee Satisfaction (ES), Cyber Incident Occurrence (CIO), Cyber Incident Reporting Mechanisms (CIRM), and Insider Threat Detection and Reporting (ITDR).

The primary objective of the research presented is to propose a comprehensive approach for enhancing an organisation's security measures against Cyber Incident occurrence. The aforementioned objective will be achieved through the process of deconstructing the aforementioned components. The cultivation of Organisational Culture is a critical component of a successful security strategy, constituting one of its most significant facets. This study intends to explore the effectiveness of using Organisational Culture (OC) to cultivate a security-conscious mindset among employees as a means of mitigating Cyber Incident occurrence. During this period, there is an examination of ongoing employee training and awareness programmes, highlighting the significance of a competent and vigilant workforce. Access Control and Monitoring (ACM) is the initial defence mechanism against unauthorised access to sensitive data. This study examines various strategies for enhancing defence mechanisms to restrict access to an organization's digital infrastructure exclusively to authorised personnel.

Simultaneously, a study is being conducted to examine the impact of employee satisfaction (ES) on insider threat. This study explores the relationship between employee satisfaction and engagement and the reduced occurrence of internal security breaches. Understanding the mechanics of Cyber Incident Occurrence (CIO) is crucial for implementing effective preventative measures. Analysing past incidents provides valuable insights into potential vulnerabilities within an organisation. The proposed work also highlights the importance of Cyber Incident Reporting Mechanisms (CIRM), which aid in facilitating a prompt and coordinated response upon threat detection. The proposed task concludes with an investigation into the field of Insider Threat Detection and Reporting (ITDR).

Organisations can effectively mitigate internal threats by implementing advanced technologies and establishing transparent reporting channels, enabling proactive identification and management of potential risks. This investigation examines the impact of critical relationships on an organization's susceptibility to Cyber-attacks, with a specific emphasis on the mediating role of Cyber Incident Reporting Mechanisms (CIRM). This study highlights the interrelationships among Organisational Innovativeness Culture, Employee Training and Awareness, Access Control and Monitoring, Employee Satisfaction, and Insider Threat Detection & Reporting. This highlights the crucial role of CIRM in safeguarding organisations against the constant risk of Cyber incidents.

A threat refers to the possibility of undesirable outcomes resulting from a circumstance, capability, action, or event that has the potential to cause harm to a system or individual. Threats can arise from natural, accidental, or intentional causes. A threat is a widespread occurrence. Aslan et al. (2023) emphasises the growing concerns surrounding Cyber-attacks in Cyberspace and the necessity for innovative preventive measuresMathew (2023) highlights the growing concerns surrounding Cybercrime-as-a-Service (CaaS) and AI-enabled threats. The author emphasises the significance of monitoring online marketplaces and creating security tools as countermeasures against these threats. Gund and Jadhav (2023) examines security challenges in cloud computing and presents a taxonomy of threats and vulnerabilities. The objective is to offer guidance to cloud users and providers in enhancing their security practises.

Conversely, Lipner and Pescatore (2023) work is not pertinent to the research question or the subject matter of threats. Oruma and Petrović (2023) examines the security risks faced by social robots in public spaces within the context of 5G networks. The study specifically emphasises the vulnerabilities present in the wireless access network and communication equipment. In their study, Hammi, Zeadally, and Nebhen (2023) examines security threats within digital supply chains. The author discusses various attacks that specifically target different technologies employed in supply chains. Additionally, Hammi et al. (2023) puts forth countermeasures to mitigate these threats. Mady, Gupta, and Warkentin (2023) examines the impact of knowledge mechanisms on employees' perception of information security threats, emphasising the significance of personal relevance and factors that promote secure behaviour. Kiran, Nishmitha, and Priyanka (2023) examines security threats in cloud computing and suggests strategies to mitigate them, emphasising the importance of preserving data security and confidentiality.

Similarly, Aldulaimi, Abdeldayem, and Keir (2023) examines the development of Cybersecurity Culture within organisations, proposing a transition from a technical perspective to a socio-cultural one. The study highlights the importance of human resource management in conducting Cybersecurity awareness training. In an analysis, Kaur and Kaimal (2023) examines the security challenges and threats associated with cloud computing. She emphasises the importance of resolving data breach issues and addresses concerns regarding the storage of critical information in the cloud. Rauf, Mohsen, and Wei (2023) suggests a taxonomic categorization of Cyber Incident occurrence and highlights the importance of implementing sophisticated behavioural anomaly detection and automatic resilience measures. Yousef et al. (2023) examines the application of various machine learning techniques, such as supervised, unsupervised, and reinforcement learning, for the purpose of categorising insider threat behaviours.

Additionally, Al-Muntaser, Mohamed, and Tuama (2023) examines the application of file integrity monitoring for real-time intrusion detection in industrial control system workstations, with a particular emphasis on safeguarding user privacy. Villarreal-Vasquez et al. (2023) presents a novel anomaly detection framework utilising LSTM model for the identification of attack sequences in computer systems. The study showcases the framework's effectiveness in detecting Cyber Incident occurrence, exhibiting high performance. These papers emphasise the significance of comprehending and mitigating Cyber Incident occurrence using advanced detection methods, including behavioural anomaly detection, machine learning, file integrity monitoring, and sequence analysis. These papers offer valuable insights on the identification and mitigation of risks in the field of information security. Cârstea (2023) emphasises the significance of incorporating security requirements, such as preventing Cyber-attacks and monitoring DDoS attacks, in order to mitigate the consequences of information security incidents.

In his study, Öztürk, Koza, and Willer (2023) emphasises the importance of addressing human vulnerabilities in information security. Specifically, he suggests utilising social engineering penetration testing and providing training to employees to enhance their ability to identify and protect against social engineering threats. Bolek, Romanová, and Korček (2023) examines the risks encountered by e-business organisations and emphasises the necessity of implementing information security management systems to alleviate these risks. Nunes et al. (2023) highlights the information security concerns of financial auditors and offers ten recommendations to address these concerns. These recommendations encompass various areas such as mobile device usage, malware protection, and network security management.

2. Literature Review and Hypotheses

The ever-evolving field of organizational security uses the phrase "Cyber Incident occurrence" to refer to hazards that originate from within the company itself. This field is in a constant state of change. Internal dangers, as opposed to external dangers, are typically caused by workers, contractors, or other individuals within the organization who have access to sensitive information. The field of organisational security employs the term "Cyber Incident occurrence" to denote risks that arise internally within the company. This field experiences continuous evolution. Internal dangers, in contrast to external dangers, are commonly attributed to individuals such as workers, contractors, or other personnel within the organisation who possess authorised access to sensitive information. The strategy should encompass factors such as organisational culture awareness and the utilisation of advanced detection and reporting techniques.

On the other hand, Apau, Sedek, and Ahmad (2019) proposes the implementation of a Trusted Human Framework (THF) as a means to identify and prevent potential Cyber Incident occurrence. Saxena et al. (2020) highlights the importance of comprehending the characteristics of Cyber Incident occurrence and the difficulties associated with identifying and detecting them. According to Greitzer et al. (2019), it is crucial to take into account human behavioural factors when detecting and addressing Cyber Incident occurrence. In his study, Nicolaou, Shiaeles, and Savage (2020) investigates the application of bio-inspired models, particularly machine learning algorithms, for addressing Cyber Incident occurrence. These papers offer insights into diverse approaches and strategies for the identification and mitigation of risks within organisational settings.

According to Brown, Watkins, and Greitzer (2013), analysing electronic communication linguistically can help anticipate insider threat risks, offering early indications for proactive mitigation. Baracaldo and Joshi (2013) suggests an adaptive framework for risk management and access control that includes a risk assessment process to address Cyber Incident occurrence. Egli (2016) examines the risks associated with Cyber Incident occurrence to unstructured data and proposes effective risk mitigation strategies through the implementation of data governance. Enterprises face difficulties in enhancing their Cyber security to prevent and counter Cyber-attacks. However, there is a lack of comprehensive studies on the factors that influence organisations' awareness and preparedness in terms of Cyber Security.

Likewise, Pallas et al. (2013) found a positive relationship between an organization's innovativeness and the success of an innovation. Innovativeness is defined as having a strategic focus on innovations, extrinsic incentive, openness in communication, and management encouragement. Li and Liu (2022) found a positive correlation between corporate innovation culture and employees' innovative behaviour, with innovation self-efficacy serving as a mediating factor in this association. Elsayed et al. (2023) examined the influence of perceived psychological safety, error risk taking, and perceived organisational innovation climate on innovative work behaviour. The researcher found that error-taking plays a mediating role in the positive association between perceived psychological safety and innovative work behaviour.

Additionally, the perceived organisational innovation climate enhances this relationship. Mahajan (2010) highlighted the importance of event reporting systems for improving patient safety and facilitating the analysis of significant incidents. Benevento et al. (2023) examines the advantages and disadvantages of incident reporting systems (IRS) within the healthcare sector. The author emphasises the importance of enhancing operators' compliance with the IRS as a means to enhance the broader patient safety culture. Lecic et al. (2023) examines the role of an innovative climate in mediating the relationship between inventive behaviour and leadership, potentially impacting the occurrence of incidents. In conclusion, Elsamani, Mejia, and Kajikawa (2023) proposes a comprehensive conceptual framework that encompasses various factors that can impact the occurrence of incidents. This framework includes employee well-being and innovativeness as key components.

H1*: Cyber incident reporting mechanism mediates the relationship between organizational innovativeness culture and Cyber incident occurrence.*

The rising sophistication of Cyber-attacks poses a threat to the online security of organisations. Timely identification of such hazards is crucial for safeguarding organisations. Human perception can complement or surpass technology detection measures, especially in the case of advanced Cyberattacks like spear phishing. However, staff members have a limited usage of reporting tools. This study aims to expand the understanding of Cyber incident reporting behaviour by considering hedonic motives, specifically warm glow, in addition to the utilitarian incentives that previous research has primarily focused on in the field of Cyber security. This enables us to offer a more comprehensive comprehension of the subject matter. Volpentesta, Ammirato, and Palmieri (2011) found that information security managers' perception of risk was influenced by the existence of an information security policy and the reporting of incidents related to information security.

Moreover, Eminağaoğlu, Uçar, and Eren (2009) conducted a case study that demonstrated the positive outcomes of information security awareness training. He highlighted the significance of human awareness in the efficacy of information security management programmes, specifically by emphasising the positive impact of information security awareness training. Liandani, Lubis, and Witjaksono (2020) found that self-attitude and self-cognitive factors significantly influence information security awareness. Parsons et al. (2014) developed the Human Aspects of Information Security Questionnaire (HAIS-Q) and found that comprehension of policy and procedures had a greater impact on attitude compared to self-reported behaviour. Riemenschneider, Burney, and Bina (2023) highlights the significance of psychological capital and organisational ideals in promoting behaviour that supports information security. Alfalah (2023) examines the impact of Cyber security perceptions on attitudes towards the use of a learning management system, with Internet security knowledge as a moderating factor.

H2*: Cyber Incident reporting mechanism mediates the relationship between Employee training awareness and Cyber incident occurrence.*

Information Systems (IS) research on managerial response to Cyber security breaches has mainly focused on external actions, such as customer redressal and crisis response. These areas are susceptible to impact due to the breach. A breach can indicate underlying systemic issues within the company. Merely addressing current problems through technical solutions and controls may hinder other managerial efforts to ensure future Cyber security. Information Security Risk Assessments (ISRA) are a valuable tool for identifying vulnerabilities that may have been overlooked following a breach. Although governance is emphasised in standards for these activities, it remains underexplored in information systems research, lacking empirical evidence to substantiate its role.

Correspondingly, Volpentesta et al. (2011) found that incident reporting and the existence of an information security policy were factors that influenced the perceived risk of information security incidents. Johnson (2002) emphasised the importance of creating effective queries and monitoring retrieval operations when considering the role of software tools in supporting incident reporting systems. According to Hazan (2016), incident reporting is crucial in healthcare settings. However, successful reporting is hindered by challenges such as system design issues and organisational culture difficulties. Mahajan (2010) highlighted the challenges related to incident reporting systems. The difficulties encompassed concerns about potential punitive measures and a lack of structured analysis and feedback for physicians. Rahman Jabin et al. (2023) highlights the deficiencies in digital incident reporting systems and the discrepancy between event reporting and investigation stages. Agbadiba and Maduagwu (2023) examines the impact of incident reporting on operational risk management and accident prevention in FPSO operations, highlighting the importance of behavioural change and the establishment of a safety culture.

H3*: Cyber Incident reporting mechanism mediates the relationship between access control & monitoring and Cyber incident occurrence.*

Companies may consider the suitability of an employee for a specific job in order to enhance the likelihood of successful and incident-free task execution. When assigning employees to tasks, it is feasible to consider variables such as the individual's familiarity with the task and the level of physical exertion required. The perceived risk of information security incidents was influenced by incident reporting and the presence of an information security policy, as indicated by the research conducted by Volpentesta et al. (2011). In a study conducted by Alaidaros and Albeedh (2022), an investigation was carried out to explore the relationship between job satisfaction and the information security of organisations.

The study specifically aimed to examine the impact of employee happiness on the overall state of information security within a company. In a study conducted by Bruno and Abrahão (2012), the objective was to examine the correlation between the frequency of incidents and the judgements rendered by operators in an information security centre. The researcher identified a notable correlation between the rate of occurrences and the quantity of incorrect positive judgements. The collective findings of these studies indicate that incident reporting methods may serve as a moderating factor in the relationship between employee happiness and the frequency of security incidents. In their study, Riemenschneider et al. (2023) examines the impact of corporate ideals on employee attitude and information security behaviour. They also explore the role of psychological capital as a mediator in this relationship. Al-refaei et al. (2023) proposes a model that utilises mediation and moderation to enhance service quality by considering factors such as work involvement, job satisfaction, and organisational commitment. This is achieved by prioritising three key factors.

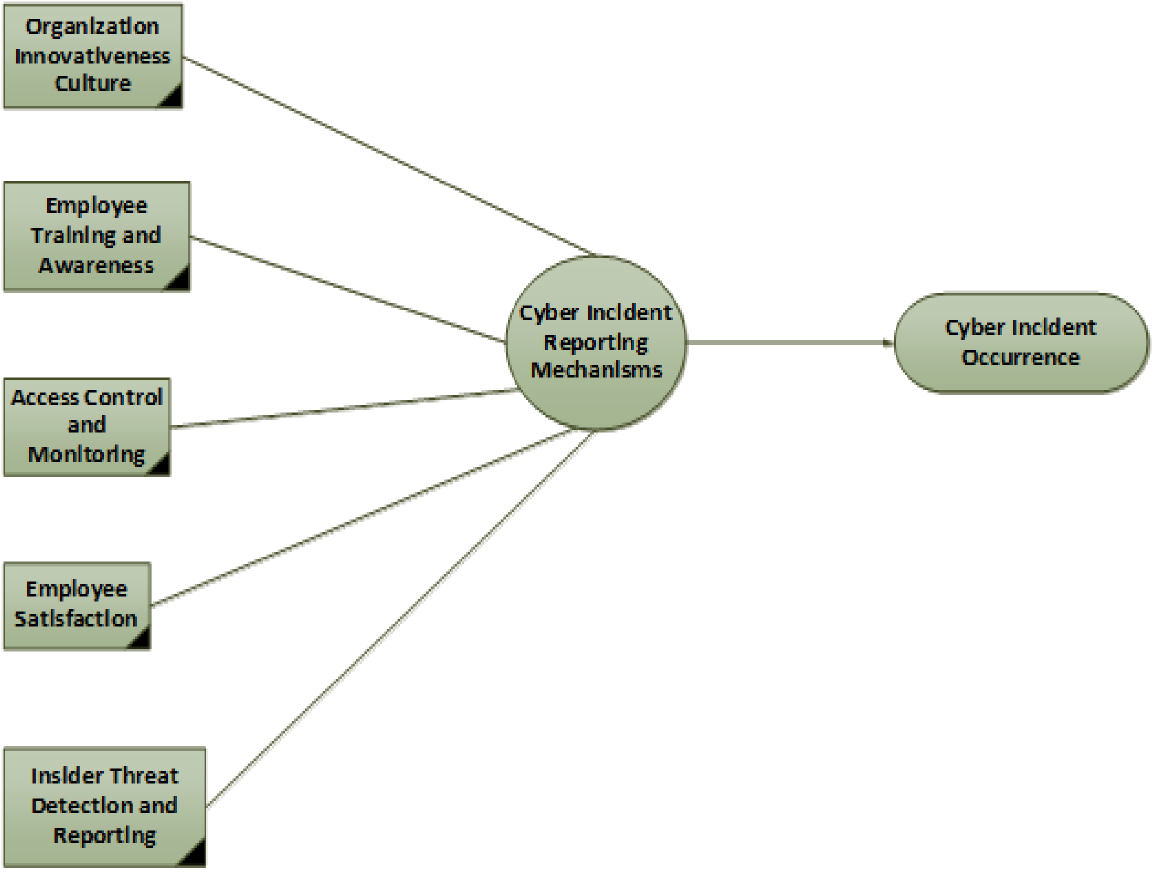
H4*: Cyber Incident reporting mechanism mediates the relationship between Employee satisfaction and Cyber incident occurrence.*

The effective governance of information security assets is a critical and intricate undertaking. The significance of ensuring security measures is heightened as businesses increasingly provide their customers with widespread access to information systems, coinciding with a rise in both the quantity and intricacy of security threats. To ensure effective management of information security, it is imperative to strategically allocate security resources across multiple domains. These domains encompass the prevention of attacks, the mitigation of vulnerabilities, and the deterrence of threats. This research offers assistance to managers in making informed security decisions through the evaluation of various security management strategies using a system dynamics model. The lens employed for the analysis of these strategies pertains to the costs associated with investment and security.

According to Ismaila and Adeleke (2023), there have been a lot of improvements in finding Cyber Incident occurrence recently. He does this by carefully looking at the metadata related to the techniques used to find these threats. This review is predicated on a comprehensive literature search. The purpose of this publication is to establish a benchmark for researchers engaged in the development of novel detection methodologies. In his study, Wang (2008) examines the correlation between the dissemination of information pertaining to information security and the subsequent impact of information security incidents. Based on the research findings, the emergence of new disclosures pertaining to information security risk factors has the capacity to mitigate the repercussions of incidents on stock prices. This observation underscores the importance of devising effective methods for disclosure.

As per Natarajan and Hossain (2004), it is advocated that the intelligence community should adopt social network surveillance as a means to mitigate the various risks associated with individuals within the organisation. Rauf et al. (2023) presents a comprehensive classification system for Cyber Incident occurrence, focusing primarily on advanced techniques such as behavioural anomaly detection and automatic resilience. In their study, Rahman Jabin et al. (2023) conducts an evaluation of healthcare quality concerns pertaining to digital incident reporting systems.

H5*: Cyber Incident reporting mechanism mediates the relationship between insider threat detection & reporting and Cyber incident occurrence.*


Organization Innovativeness Culture
Employee Training and Awareness
Access Control and Monitoring
Employee Satisfaction
Insider Threat Detection and Reporting
Cyber Incident Reporting Mechanisms
Cyber Incident Occurrence

3. Methodology

The research employed quantitative methodologies to offer a comprehensive perspective on the phenomenon. A total of 219 employees from diverse sectors in Saudi Arabia were included in the sample for data collection. The selection of participants aimed to ensure a comprehensive representation of various roles, levels of seniority, and departments across their respective organisations. The presence of diverse perspectives facilitated a thorough comprehension of the dynamics surrounding Cyber Incident occurrence. A structured questionnaire was created to assess Cyber Incident occurrence, drawing from existing literature and expert opinions. The questionnaire consisted of sections that examined individual attitudes, behavioural patterns, and organisational factors related to Cyber Incident occurrence.

The researchers used Likert-scale questions to measure responses, enabling quantitative analysis. Data was collected via online surveys distributed to the chosen participants. The survey questionnaire aimed to collect data regarding employees' perceptions, experiences, and observations regarding Cyber Incident occurrence. Anonymity was ensured to promote truthful and open responses from participants. Statistical software was utilised to conduct quantitative data analysis. The researchers computed descriptive statistics, such as means, frequencies, and percentages, in order to provide a summary of the participants' responses. In order to identify significant correlations and patterns within the data Structural Equation Modelling (SEM) with Amos were utilised.

The analysis identified several factors that contribute to Cyber Incident occurrence, such as employee dissatisfaction, inadequate security protocols, limited employee awareness, and insufficient monitoring mechanisms. These findings offer valuable insights into the difficulties organisations encounter when addressing Cyber Incident occurrence.

Table 1. Measurement Scales

“Organization Innovativeness Culture	**References**
1. Innovativeness_1: Managers have courage to make innovation and take risk.	Ernest Chang and Lin (2007)
2. Innovativeness_2: Managers actively lead the staff to grow and innovate.	
3. Innovativeness_3: Managers have vision and insights to create new business opportunities.	
4. Innovativeness_4: Employees always have to face challenges and they can learn and grow from the challenges.	
5. Innovativeness_5: Your company pays attentions to the uniqueness of employees and encourages the innovation from employees.	
6. Innovativeness_6: Your company is willing to take risks, and it is indeed an ambitious and energetic organization.	
Employee Training and Awareness	Zhou et al. (2019)
1. In organization normally there is employee training provided on computer network privacy and security AND mobile device privacy and security	
2. In organization normally there is HIPAA training, which includes instructional material tailored for telehealth privacy and security, provided at least on an annual basis, for all staff that use the telehealth system	
3. In organization normally there are the risks of social media connections (e.g. risks of inadvertent linking of patients via social media as a result of using mobile devices with downloaded social media accounts on the device) discussed with all users of the telehealth system	
Access Control and Monitoring	
1. In organization normally there is Authentication/Access Control	
2. In organization normally there is proper user authentication (username, passwords, fingerprinting, PINs, and security questions) established before logging into the telehealth session	
3. I normally use strong passwords (uppercase, lowercase, minimum length, special symbols, digits, etc.) to access the telehealth system	
4. In organization normally there is there an inactivity time out function available on the telehealth system that requires re-authentication to access the system after the timeout period has ended	
5. In organization normally there is unauthorized viewing of patient information prevented by applying access controls (e.g., role-based, user-based, context-based access controls)	
6. In organization normally there are all of the smart devices (smartphones, tablets, smartwatch etc.) that are used in telehealth sessions, password protected and encrypted	
Employee Satisfaction	
1. I am satisfied with the information security practices.	Montesdioca and Maçada (2015)
2. I am satisfied with the information security training.	
3. I am satisfied with the information security policy.	
4. Overall, I am satisfied with the information security.	
Cyber Incident Occurrence	Lynch (2022)

1. In organization I use multi-factor authentication (MFA) 2. In organization I enforce a current privileged user policy and regularly audit user privileges 3. In organization I regularly run phishing attack simulations to ensure your colleagues are trained to look for signs of fraud 4. In organization I enforce your security policy controls in your cloud-managed data repositories 5. In organization I use an analytics tool to study past Cyber Incident occurrence and build profiles to define unusual user activities	
Incident Reporting Mechanisms	
1. In organization, no recognised reporting mechanism in place 2. In organization, a reporting process in place but not well known or used. 3. In organization, a reporting mechanism is in place and used by most butstill has challenges in its use 4. In organization, a well understood processes with majority completing theprocess as described 5. In organization, second nature to staff on how to report.	Humphrey (2017)
Insider Threat Detection and Reporting	
1. In organization normally there are anti-malware alerts 2. In organization normally there are blacklisted files detected ('hacker tools') 3. In organization normally there is (Attempt of) disabling anti-malware tools 4. In organization normally there has been attempted to escalation of privileges 5. In organization normally user attempts to print or copy confidential documents 6. In organization normally there is abnormally large number of software errors 7. In organization normally there is unidentified device is attached (USB, CD-ROM) 8. In organization normally there is failed login attempts 9. In organization normally there are different users (attempting to) log in from the same workstation 10.In organization normally there are user logs into a desktop workstation outside working hours 11.In organization normally there is lack of log messages or monitoring data"	Kont et al. (2015)

4. Reliability and Validity

Table 2 presents the factor loadings, reliability, and convergent validity for the constructs in the study. The key findings for each construct are as follows:

The organization's culture demonstrates good reliability (CR: 0.761), convergent validity (AVE: 0.564), and strong internal consistency (α: 0.784). Employee Training and Awareness also shows acceptable reliability (CR: 0.701), convergent validity (AVE: 0.541), and strong internal consistency (α: 0.841). Access Control and Monitoring exhibit's good reliability (CR: 0.733), convergent validity (AVE: 0.597), and strong internal consistency (α: 0.799). Employee Satisfaction demonstrates strong reliability (CR: 0.768), convergent validity (AVE: 0.600), and sound internal consistency (α: 0.739). Cyber Incident Occurrence displays good reliability (CR: 0.749), convergent validity (AVE: 0.588), and strong internal consistency (α: 0.744). Cyber Incident Reporting Mechanisms show acceptable reliability (CR: 0.710), supported convergent validity (AVE: 0.509), and sound internal consistency (α: 0.728). Insider Threat Detection and Reporting reveals good reliability (CR: 0.700), established convergent validity (AVE: 0.537), and strong internal consistency (α: 0.785). These findings collectively indicate that the measurement instrument is robust and valid, as it reliably and accurately assesses the factors associated with Cyber Incident occurrence in the study.

Table 3 presents the results of discriminant validity, where the squared correlations between constructs are shown below the diagonal. The diagonal values, representing the Average Variance Extracted (AVE) for each construct, exceed the squared correlation values, indicating strong discriminant validity. This suggests that the constructs are separate and do not have significant overlap in their measurement. In summary, the study's measurement instrument exhibit's high reliability, satisfactory convergent validity, and robust discriminant validity. These findings establish the reliability and credibility of the data gathered and examined in relation to Cyber Incident occurrence within organisational settings.

Table 1. Factor Loadings Reliability, Convergent Validity

	CR	**AVE**	**A**
Organization Culture (OC)	0.761	0.564	0.784
Employee Training and Awareness (ETA)	0.701	0.541	0.841
Access Control and Monitoring (ACM)	0.733	0.597	0.799
Employee Satisfaction (ES)	0.768	0.600	0.739
Cyber Incident Occurrence (CIO)	0.749	0.588	0.744
Cyber Incident Reporting Mechanisms (CIRM)	0710	0.509	0.728
Insider Threat Detection and Reporting (ITDR)	0.700	0.537	0.785

Table 2. Discriminant Validity

	1	**2**	**3**	**4**	**5**	**6**	**7**
OC	**0.56**						
ETA	0.47	**0.58**					
ACM	0.34	0.49*	**0.61**				
ES	0.24**	0.14**	0.47*	**0.50**			
CIO	0.40*	0.22**	0.58	0.24**	**0.57**		
CIRM	0.39**	0.37	0.51*	0.33**	0.43*	**0.54**	
ITDR	0.44*	0.19*	0.27**	0.38*	0.28*	0.17**	**0.501**

Note: values of AVE on diagonal higher than squared correlations values. † p < 0.100; * p < 0.050; ** p < 0.010; *** p < 0.001

4.1 Model Testing:

Summary of Measurement *Model Fit*

The findings are as follows.

- **CFI (Comparative Fit Index):** The Comparative Fit Index (CFI) score of 0.92 surpasses the acceptable threshold of 0.90, suggesting that the measurement model exhibits favourable fit in comparison to a null model.
- **AGFI (Adjusted Goodness of Fit Index):** The model's fit is considered acceptable, as it exceeds the baseline threshold of 0.80, with a score of 0.84.
- **RMSEA (Root Mean Square Error of Approximation):** The RMSEA value of 0.018 falls below the suggested threshold of 0.08, suggesting that the measurement model demonstrates a favourable fit with the collected data.
- **CMIN/df (Chi-Square/degrees of freedom):** The model demonstrates good fit with a value of 2.31, which falls below the established threshold of 3. This indicates a reasonable chi-square statistic.
- **TLI (Tucker-Lewis Index) and IFI (Incremental Fit Index):** The TLI and IFI scores are 0.95 and 0.93, respectively, exceeding the acceptable threshold of 0.90. This provides additional evidence supporting the strong fit of the measurement model.

In summary, the aforementioned explanation suggests that the measurement model demonstrates a strong fit with the data, as evidenced by several fit indices surpassing the recommended thresholds. This outcome instils confidence in the overall quality of the measurement model.

Summary of Structural Model Fit

The results are as follows:

- **CFI (Comparative Fit Index):** The Comparative Fit Index (CFI) score of 0.94 surpasses the acceptable threshold of 0.90, indicating that the structural model exhibits a favourable fit in comparison to a null model.
- **AGFI (Adjusted Goodness of Fit Index):** The model's fit, indicated by a score of 0.85, is deemed satisfactory as it exceeds the minimum threshold of 0.80, which serves as the baseline.
- **RMSEA (Root Mean Square Error of Approximation):** The RMSEA value of 0.011 falls below the commonly recommended threshold of 0.08, suggesting that the structural model exhibits a favourable fit with the observed data.
- **CMIN/df (Chi-Square/degrees of freedom):** With a value of 1.24, the structural model fits well as it is below the threshold of 3, suggesting a reasonable chi-square statistic.
- **TLI (Tucker-Lewis Index) and IFI (Incremental Fit Index):** The TLI and IFI scores, which are 0.95 and 0.94 respectively, surpass the acceptable threshold of 0.90. This provides additional evidence supporting the strong fit of the structural model.

In conclusion, the previous information suggests that the structural model demonstrates a strong alignment with the data, as evidenced by multiple fit indices exceeding the recommended thresholds. This instils confidence in the integrity of the structural model and its appropriateness for examining the interrelationships among constructs.

4.2 Direct and Indirect Hypothesis

These findings suggest the following:

- Each of the independent variables (Organization Culture, Employee Training and Awareness, Access Control and Monitoring, Employee Satisfaction, and Cyber Incident Occurrence) has a significant direct positive effect on "Cyber Incident Reporting Mechanisms," indicating that improvements in these variables contribute to enhanced reporting mechanisms for Cyber incidents.
- The significant impact of indirect effects, which encompass the combined influence of both direct and indirect pathways, underscores the crucial role of these variables in facilitating the implementation of Cyber incident reporting mechanisms.
- The presence of effective ''Cyber incident reporting mechanisms'' has a direct and positive impact on the occurrence of Cyber incidents. This correlation supports the idea that implementing strong reporting mechanisms can contribute to a decrease in the frequency of Cyber incidents.

In general, the analysis of direct and indirect effects underscores the intricate connections between these variables, underscoring their interdependence in influencing the efficacy of Cyber incident reporting mechanisms within the examined context.

Table 4. Summary of Effects

Variables	Direct Effects	Indirect Effects	Total Effects
Organization Culture → Cyber Incident Reporting Mechanisms	0.314	0.497	0.811
Employee Training and Awareness → Cyber Incident Reporting Mechanisms	0.388	0.499	0.887
Access Control and Monitoring → Cyber Incident Reporting Mechanisms	0.146	0.379	0.525
Employee Satisfaction → Cyber Incident Reporting Mechanisms	0.136	0.441	0.577
Cyber Incident Occurrence → Cyber Incident Reporting Mechanisms	0.247	0.501	0.748
Cyber Incident Reporting Mechanisms → Cyber Incident Occurrence	0.397	----	0.397

Table 5 below provides the summary of the acceptance/rejection status of all the hypotheses of the study in accordance with the results presented in Table 7 above.

5. Result of Analyses and Hypotheses

The findings of the analyses and hypotheses testing are displayed in Table 5, which focuses on evaluating the mediating effect of "Cyber Incident Reporting Mechanisms" on the associations between different independent variables and "Cyber Incident Occurrence." The findings are as follows:

- **H1** - Cyber Incident reporting mechanism mediates the relationship between organizational innovativeness culture and Cyber incident occurrence: This hypothesis is rejected as the p-value is 1.01, which is above the significance level of 0.05. The t-value of 1.34 is also below the threshold of 1.96, indicating that the mediation effect is not supported.
- **H2** - Cyber Incident reporting mechanism mediates the relationship between Employee training awareness and Cyber incident occurrence: This hypothesis is accepted, with a p-value of 0.014, which is below the significance level of 0.05. The t-value of 2.97 exceeds the threshold of 1.96, indicating that the mediation effect is supported.
- **H3** - Cyber Incident reporting mechanism mediates the relationship between access control & monitoring and Cyber incident occurrence: This hypothesis is accepted, with a p-value of 0.011, below the significance level of 0.05. The t-value of 3.54 surpasses the threshold of 1.96, supporting the mediation effect.
- **H4** - Cyber Incident reporting mechanism mediates the relationship between Employee satisfaction and Cyber incident occurrence: This hypothesis is rejected, as the p-value is 0.87, exceeding the significance level of 0.05. The t-value of 1.22 is below the threshold of 1.96, indicating that the mediation effect is not established.
- **H5** - Cyber Incident reporting mechanism mediates the relationship between insider threat detection & reporting and Cyber incident occurrence: This hypothesis is accepted, with a p-value of 0.016, below the significance level of 0.05. The t-value of 4.57 exceeds the threshold of 1.96, supporting the mediation effect.

In short, the results show that "Cyber Incident Reporting Mechanisms" act as a link between "Employee Training and Awareness," "Access Control and Monitoring," and "Insider Threat Detection and Reporting" when it comes to "Cyber Incidents." However, the presence of a mediation effect between "Organisational Innovativeness Culture" and "Employee Satisfaction" is not substantiated. The aforementioned findings offer valuable insights into the intricate interconnections among the variables under examination and their influence on the frequency of Cyber incidents within the specific context that was investigated.

Table 5. Hypothesis Testing

	Hypotheses	P-value	t-value	Accept or reject
H1	Cyber Incident reporting mechanism mediates the relationship between organizational innovativeness culture and Cyber incident occurrence.	1.01	1.34	**Rejected**
H2	Cyber Incident reporting mechanism mediates the relationship between Employee training awareness and Cyber incident occurrence.	0.014	2.97	**Accept**
H3	Cyber Incident reporting mechanism mediates the relationship between access control & monitoring and Cyber incident occurrence.	0.011	3.54	**Accept**
H4	Cyber Incident reporting mechanism mediates the relationship between Employee satisfaction and Cyber incident occurrence.	0.87	1.22	**Rejected**
H5	Cyber Incident reporting mechanism mediates the relationship between insider threat detection & reporting and Cyber incident occurrence.	0.016	4.57	**Accept**

p-value <0.05 (Hair et al., 2007), t-value > 1.96 (Bhatti & Sundram Kaiani, 2015)

6. Discussion

This study examines the relationships between different organisational factors, namely Organisation Culture (OC), Employee Training and Awareness (ETA), Access Control and Monitoring (ACM), Employee Satisfaction (ES), and Insider Threat Detection and Reporting (ITDR), and the occurrence of Cyber Incidents (CIO). Furthermore, researchers conducted an investigation into the mediating function of Cyber Incident Reporting Mechanisms (CIRM) within these associations. These results offer significant insights for organisations seeking to enhance their Cybersecurity strategies and address the issue of Cyber Incident occurrence.

Also, this study highlights the significant importance of Cyber Incident Reporting Mechanisms (CIRM) as an intermediary in particular relationships, particularly those involving Employee Training and Awareness (ETA), Access Control and Monitoring (ACM), and Insider Threat Detection and Reporting (ITDR). However, it is important to note that the influence of additional organisational factors, such as Organisation Culture (OC) and Employee Satisfaction (ES), may not be as extensively mediated by CIRM in terms of mitigating the frequency of Cyber incidents. The thorough comprehension of the interconnections among these variables and their moderation by CIRM provides organisations with a more intricate strategy for enhancing their Cyber security endeavours.

The second hypothesis suggested that the mediating role of CIRM would be evident in the relationship between Employee Training and Awareness (ETA) and the Chief Information Officer (CIO). The acceptance of this hypothesis indicates that CIRM functions as a mediator in the association between ETA and CIO. This suggests that the implementation of comprehensive employee training and awareness programmes, coupled with the establishment of streamlined reporting mechanisms, can contribute to a decrease in the probability of Cyber incidents.

The third hypothesis stated that the mediating role of CIRM would be evident in the relationship between Access Control and Monitoring (ACM) and the Chief Information Officer (CIO). The hypothesis was found to be supported, suggesting that CIRM serves as an effective mediator in the relationship between ACM and CIO. This highlights the significance of not only implementing robust access control and monitoring protocols but also establishing a dependable reporting system to address and minimise Cyber incidents. The fourth hypothesis proposed that the mediating role of CIRM would be evident in the relationship between Employee Satisfaction (ES) and CIO. The rejection of this hypothesis indicates that there is no substantial mediation effect of CIRM on the relationship between employee satisfaction and the CIO.

The presence of effective reporting mechanisms is crucial in conjunction with employee satisfaction in order to effectively mitigate the occurrence of Cyber incidents. The fifth hypothesis suggests that the relationship between Insider Threat Detection and Reporting (ITDR) and the Chief Information Officer (CIO) would be influenced by the presence of CIRM. The acceptance of this hypothesis suggests that CIRM functions as a mediator in the association between ITDR and CIO. This suggests that the presence of effective mechanisms for identifying and reporting Cyber Incident occurrence is of utmost importance in mitigating the frequency of Cyber incidents within an organisation.

In brief, the findings of this study underscore the significant importance of Cyber Incident Reporting Mechanisms (CIRM) in moderating the associations between specific organisational factors and the occurrence of Cyber incidents. The integration of robust reporting mechanisms, in conjunction with elements such as comprehensive employee training and awareness programmes, as well as access control and monitoring measures, can play a pivotal role in mitigating the likelihood and impact of Cyber incidents. Nevertheless, the research also emphasises that the influence of additional variables, such as Organisational Culture and Employee Satisfaction, may not be as significantly moderated by CIRM in reducing Cyber incidents.

7. Implications:

This research enhances the theoretical comprehension of the significance of Cyber Incident Reporting Mechanisms (CIRM) within the realm of Cyber security. This study elucidates the role of CIRM in facilitating the connections between different organisational factors and the occurrence of Cyber incidents, emphasising its crucial function as a mediator between organisational practices and the mitigation of such incidents. The findings of the study indicate that the influence of organisational factors on the occurrence of Cyber incidents is not consistent across all factors. Through the analysis of the mediating effect of CIRM, this study differentiates between factors such as Employee Training and Awareness (ETA) and Access Control and Monitoring (ACM), which demonstrate significant mediation, and factors such as Organisation Culture (OC) and Employee Satisfaction (ES), which display less pronounced mediation.

The findings can be used by organisations to prioritise and improve their employee training and awareness programmes. By acknowledging the intermediary function of CIRM, organisations can implement training programmes that not only impart knowledge to employees but also enable them to confidently and proficiently communicate potential Cyber threats. The research highlights the significance of incorporating robust access control and monitoring systems alongside effective reporting mechanisms. Organisations have the option to allocate resources towards the adoption of advanced access control technologies and real-time monitoring tools, in conjunction with the implementation of streamlined reporting procedures, as a means to effectively mitigate Cyber incidents. Organisations can enhance their insider threat mitigation strategies by recognising the influence of CIRM in facilitating the connection between Insider Threat Detection and Reporting (ITDR) and the incidence of Cyber incidents. It is imperative to establish measures that guarantee employees possess comprehensive knowledge regarding the identification and reporting of Cyber Incident occurrence and to ensure that these reports are promptly addressed and acted upon.

8. Limitations and Future Research Directions:

The study's findings may be limited in terms of generalizability. The study was conducted within a specific organisational context, and its findings may not be universally applicable to all industries or organisational settings. The study's reliance on self-reported data may introduce biases. Future research could improve by incorporating both self-reporting and objective data sources to enhance the validity of the study. The study does not consider temporal fluctuations in the associations. Longitudinal studies offer valuable insights into the temporal evolution of relationships.

Future research should consider examining various industries and organisational sizes to determine the generalizability of the findings in different contexts. Longitudinal research can examine the evolving relationships between organisational factors, CIRM, and Cyber incident occurrence, taking into account the dynamic nature of Cyber security threats. Studying the relationship between organisational policies, governance structures, and CIRM can enhance our comprehensive comprehension of the Cyber security landscape. Studying the influence of CIRM and organisational factors on Cyber incident occurrences across different cultures and regions can offer valuable insights into global Cyber security practices.

In conclusion, this study offers significant theoretical and practical insights regarding the role of Cyber Incident Reporting Mechanisms (CIRM) in the field of Cyber security. Despite its limitations, future research can expand on these findings to improve our understanding of how organisations can effectively address Cyber threats and enhance their Cyber security.

9. Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant 5093]'.

References

Agbadiba, I., & Maduagwu, D. N. (2023). Impact of Incident Reporting on Operational Risk Management and Accident Prevention in FPSO Operations in Nigeria. *SPE Nigeria Annual International Conference and Exhibition*, D021S010R006. https://doi.org/10.2118/217174-MS

Al-Muntaser, B., Mohamed, M. A., & Tuama, A. Y. (2023). Real-Time Intrusion Detection of Insider Threats in Industrial Control System Workstations Through File Integrity Monitoring. *International Journal of Advanced Computer Science and Applications, 14*(6), 326-333. https://doi.org/10.14569/IJACSA.2023.0140636

Al-refaei, A. A., Ali, H. B., Ateeq, A. A., & Alzoraiki, M. (2023). An Integrated Mediating and Moderating Model to Improve Service Quality through Job Involvement, Job Satisfaction, and Organizational Commitment. *Sustainability, 15*(10), 7978. https://doi.org/10.3390/su15107978

Alaidaros, H., & Albeedh, S. (2022). Towards Studying the Relationship between Job Satisfaction and Organizations' Information Security. In *2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE)* (pp. 1-6). IEEE. https://doi.org/10.1109/ITSS-IoE56359.2022.9990932

Aldulaimi, S. H., Abdeldayem, M. M., & Keir, M. Y. A. (2023). Formulating the Cyber Security Culture in Organizations: Proposing and Arguing Insights. *International Journal of Professional Business Review, 8*(5), e01660. https://doi.org/10.26668/businessreview/2023.v8i5.1660

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences, 10*(4), 136-144. https://doi.org/10.21833/ijaas.2023.04.017

Apau, M. N., Sedek, M., & Ahmad, R. (2019). A Theoretical Review: Risk Mitigation Through Trusted Human Framework for Insider Threats. In *2019 International Conference on Cybersecurity (ICoCSec)* (pp. 37-42). IEEE. https://doi.org/10.1109/ICoCSec47621.2019.8970795

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security, 39*, 237-254. https://doi.org/10.1016/j.cose.2013.08.001

Benevento, M., Nicolì, S., Mandarelli, G., Ferorelli, D., Cicolini, G., Marrone, M., Dell'Erba, A., & Solarino, B. (2023). Strengths and weaknesses of the incident reporting system: An Italian experience. *Journal of Patient Safety and Risk*

Management, 28(1), 15-20. https://doi.org/10.1177/25160435221150568

Bhatti, M. A., & Sundram Kaiani, V. P. (2015). *Business research: quantitative and qualitative methods* (1st ed.). Pearson Singapore.

Bolek, V., Romanová, A., & Korček, F. (2023). The Information Security Management Systems in E-Business. *Journal of Global Information Management, 31*(1), 1-29. https://doi.org/10.4018/JGIM.316833

Brown, C. R., Watkins, A., & Greitzer, F. L. (2013). Predicting Insider Threat Risks through Linguistic Analysis of Electronic Communication. In *2013 46th Hawaii International Conference on System Sciences* (pp. 1849-1858). IEEE. https://doi.org/10.1109/HICSS.2013.453

Bruno, T., & Abrahão, J. (2012). False alarms and incorrect rejections in an information security center: correlation with the frequency of incidents. *Work, 41*(Supplement 1), 2902-2907. https://doi.org/10.3233/WOR-2012-0542-2902

Cârstea, C. (2023). Methods of Identifying Vulnerabilities in the Information Security Incident Management Process. *Romanian Military Thinking,* (1), 128-145. https://doi.org/10.55535/RMT.2023.1.7

Egli, M. C. (2016). *Mitigating the risks of insider threat on unstructured data through data governance*. University of Oregon Applied Information Management. http://hdl.handle.net/1794/21963

Elsamani, Y., Mejia, C., & Kajikawa, Y. (2023). Employee well-being and innovativeness: A multi-level conceptual framework based on citation network analysis and data mining techniques. *Plos one, 18*(1), e0280005. https://doi.org/10.1371/journal.pone.0280005

Elsayed, A. M., Zhao, B., Goda, A. E.-m., & Elsetouhi, A. M. (2023). The role of error risk taking and perceived organizational innovation climate in the relationship between perceived psychological safety and innovative work behavior: A moderated mediation model. *Frontiers in Psychology, 14*, 1042911. https://doi.org/10.3389/fpsyg.2023.1042911

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report, 14*(4), 223-229. https://doi.org/10.1016/j.istr.2010.05.002

Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial management & data systems, 107*(3), 438-458. https://doi.org/10.1108/02635570710734316

Greitzer, F. L., Purl, J., Leong, Y. M., & Sticha, P. J. (2019). Positioning your organization to respond to insider threats. *IEEE Engineering Management Review, 47*(2), 75-83. https://doi.org/10.1109/EMR.2019.2914612

Gund, N. S., & Jadhav, A. A. (2023). Cloud Computing Security: Threats and Countermeasures. *International Journal of Advanced Research in Science, Communication and Technology, 3*(5), 517-523. https://doi.org/10.48175/IJARSCT-11678

Hair, J. F., Money, A. H., Samouel, P., & Page, M. (2007). Research Methods for Business. *Education + Training, 49*(4), 336-337. https://doi.org/10.1108/et.2007.49.4.336.2

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys, 55*(14s), 1-40. https://doi.org/10.1145/3588999

Hazan, J. (2016). Incident reporting and a culture of safety. *Clinical Risk, 22*(5-6), 83-87. https://doi.org/10.1177/1356262216682893

Humphrey, M. (2017). *Identifying the critical success factors to improve information security incident reporting* (Doctoral Dissertation, Cranfield University).

http://dspace.lib.cranfield.ac.uk/handle/1826/12739

Ismaila, I., & Adeleke, N. D. (2023). Systematic Literature Review and Metadata Analysis of Insider Threat Detection Mechanism. *International Journal of Computer Science and Mobile Computing, 12*(4), 60-88. https://doi.org/10.47760/ijcsmc.2023.v12i04.007

Johnson, C. (2002). Software tools to support incident reporting in safety-critical systems. *Safety Science, 40*(9), 765-780. https://doi.org/10.1016/S0925-7535(01)00085-6

Kaur, M., & Kaimal, A. B. (2023). Analysis of Cloud Computing Security Challenges and Threats for Resolving Data Breach Issues. In *2023 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCCI56745.2023.10128329

Kiran, T. S. R., Nishmitha, S. N. S., & Priyanka, G. (2023). Security Threats and Measures to Overcome in Superior Cloud. *i-manager's Journal on Cloud Computing, 10*(1), 1. https://doi.org/10.26634/jcc.10.1.19239

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2015). *Insider threat detection study*. NATO CCD COE, Tallinn. https://ccdcoe.org/library/publications/insider-threat-detection-study

Lecic, M. S., Milic, B., Visnjic, R., & Culibrk, J. (2023). Leadership, Innovative Behavior and the Case of Innovative Climate&mdash;When the Mediator Becomes the Mediated. *Behavioral Sciences, 13*(1), 40. https://doi.org/10.3390/bs13010040

Li, Z., & Liu, L. (2022). The impact of organizational innovation culture on employees' innovation behavior. *Social Behavior and Personality: an international journal, 50*(12), 1-10. https://doi.org/10.2224/sbp.11934

Liandani, P., Lubis, M., & Witjaksono, W. (2020). Exploring the Relationship of Individual Indicator as the Critical Factor in Information Security Awareness. In *Selected Papers from the 1st International Conference on Islam, Science and Technology, ICONISTECH-1 2019, 11-12 July 2019, Bandung, Indonesia*. EAI. http://dx.doi.org/10.4108/eai.11-7-2019.2297836

Lipner, S., & Pescatore, J. (2023). Updates, Threats, and Risk Management. *Communications of the ACM, 66*(5), 21-23. https://doi.org/10.1145/3587826

Lynch, B. (2022, Sep 30). *The 5-Question Test to Assess Your Readiness to Manage Insider Threats*. Imperva. https://www.imperva.com/blog/the-5-question-test-to-assess-readiness-to-manage-insider-threats

Mady, A., Gupta, S., & Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. *Information Systems Journal, 33*(4), 790-841. https://doi.org/10.1111/isj.12424

Mahajan, R. P. (2010). Critical incident reporting and learning. *BJA: British Journal of Anaesthesia, 105*(1), 69-75. https://doi.org/10.1093/bja/aeq133

Mathew, A. (2023). Cybercrime-as-a-Service & AI-Enabled Threats. *International Journal of Computer Science and Mobile Computing, 12*(1), 28-31. https://doi.org/10.47760/ijcsmc.2022.v12i01.004

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security, 48*, 267-280. https://doi.org/10.1016/j.cose.2014.10.015

Natarajan, A., & Hossain, L. (2004). Towards a Social Network Approach for Monitoring Insider Threats to Information Security. In H. Chen, R. Moore, D. D. Zeng, & J. Leavitt (Eds.), *Intelligence and Security Informatics* (pp. 501-507). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-25952-7_41

Nicolaou, A., Shiaeles, S., & Savage, N. (2020). Mitigating Insider Threats Using Bio-Inspired

Models. *Applied Sciences, 10*(15), 5046. https://doi.org/10.3390/app10155046

Nunes, A., Pais, M., Mikaela, K., & Soares, B. H. (2023). The concerns of financial auditors with Information Security: 10 recommendations to consider. In *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE. https://doi.org/10.23919/CISTI58278.2023.10211295

Oruma, S. O., & Petrović, S. (2023). Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey. *IEEE Access, 11*, 63205-63237. https://doi.org/10.1109/ACCESS.2023.3288338

Öztürk, A., Koza, E., & Willer, M. (2023). Social Engineering Penetration Testing within the OODCA Cycle – Approaches to Detect and Remediate Human Vulnerabilities and Risks in Information Security. *Human Factors in Cybersecurity*.

Pallas, F., Böckermann, F., Goetz, O., & Tecklenburg, K. (2013). Investigating organisational innovativeness: Developing a multidimensional formative measure. *International Journal of Innovation Management, 17*(04), 1350009. https://doi.org/10.1142/S1363919613500096

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Rahman Jabin, M. S., Steen, M., Wepa, D., & Bergman, P. (2023). Assessing the healthcare quality issues for digital incident reporting in Sweden: Incident reports analysis. *DIGITAL HEALTH, 9*. https://doi.org/10.1177/20552076231174307

Rauf, U., Mohsen, F., & Wei, Z. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. *Journal of Cyber Security and Mobility, 12*(2), 221–252. https://doi.org/10.13052/jcsm2245-1439.1225

Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023). The influence of organizational values on employee attitude and information security behavior: the mediating role of psychological capital. *Information & Computer Security, 31*(2), 172-198. https://doi.org/10.1108/ICS-10-2022-0156

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics, 9*(9), 1460. https://doi.org/10.3390/electronics9091460

Villarreal-Vasquez, M., Modelo-Howard, G., Dube, S., & Bhargava, B. (2023). Hunting for Insider Threats Using LSTM-Based Anomaly Detection. *IEEE Transactions on Dependable and Secure Computing, 20*(01), 451-462. https://doi.org/10.1109/TDSC.2021.3135639

Volpentesta, A. P., Ammirato, S., & Palmieri, R. (2011). Investigating effects of security incident awareness on information risk perception. *International Journal of Technology Management, 54*(2/3), 304-320. https://doi.org/10.1504/IJTM.2011.039317

Wang, T.-W. D. (2008). Reading the disclosures with new eyes: bridging the gap between information security disclosures and incidents. In *Proceedings of the 9th Annual Information Security Symposium* (pp. 1-1). https://dl.acm.org/doi/abs/10.5555/2789054.2789094

Yousef, R., Jazzar, M., Eleyan, A., & Bejaoui, T. (2023). A Machine Learning Framework & Development for Insider Cyber-crime Threats Detection. In *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 1-6). IEEE. https://doi.org/10.1109/SmartNets58706.2023.10215718

Zhou, L., Thieret, R., Watzlaf, V., DeAlmeida, D., & Parmanto, B. (2019). A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and validation. *International journal of telerehabilitation, 11*(1), 3-14. https://doi.org/10.5195/ijt.2019.6276