European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com

e-ISSN: 2421-826X

DOI: 10.15405/epms.2022.10.63

ICONSPADU 2021
International Conference on Sustainable Practices Development and Urbanisation

A CLASSIFICATION OF HUMAN ERROR FACTORS IN UNINTENTIONAL INSIDER THREATS

Wan Basri Wan Ismail (a)*, Setyawan Widyarto (b)
*Corresponding author

(a) Faculty of Communication, Visual Art and Computing, University Selangor, Malaysia, wanbasri@unisel.edu.my
(b) Faculty of Communication, Visual Art and Computing, University Selangor, Malaysia, swidyarto@unisel.edu.my

Abstract

Most information security industry reports and works of literature agree that unintentional incidents occur because of human error. This error is one of the major distractions in the information security field. The most challenging in predicting and stopping unintentional insider threats is predicting human errors and human behaviour. This research aims to understand human error taxonomy, closely related to human error factors that pose a high risk of unintentional insider threats. Nine databases were searched using standardised and adapted search syntax to identify the relevant manuscripts published between 2000 and 2019. This paper has identified and classified organisational factors related to human error action. Fifty-two relevant articles were extracted and analysed. The scoping review outlines human error factors and mapping with human error taxonomy to understand these issues. The identification and classification will help employees and organisations deeply understand the importance of human error taxonomy and human error factors to prevent unintentional insider threats and improve their information security.

Keywords: Human error, human error taxonomy, unintentional insider threats

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

Human error in information security refers to human carelessness such as accidental disclosure of information, loss of data storage, and disposal of data that is not following procedures. Human error also arises due to the differences in skills, motivations, and knowledge between employees (Miyamoto & Takahashi, 2013). It is closely related to the work environment, organisation and job process that influence the behaviour of employees at work (Ganguly, 2011). According to industrial reports, more than 60% of data exfiltration is unintentional insider threats and the human factor of recognising insider attacks by unusual and suspicious behaviour (CyberEdge Group, 2020; Schulze, 2020; Shareth Ben, 2020).

Reason (1990) defines human error is as a failure to achieve the intended outcome in a planned sequence of mental or physical activities. The study also proposed a generic error modelling system (GEMS), categorising human error as 'slip' and 'mistakes'. Slips describe the inaccurate execution of the correct sequence of processes, while 'mistakes' represent situations where a person makes a wrong decision but executes it correctly. Thus 'mistakes' can be considered 'planning failures' and 'slips' as 'implementation failures' (Liginlal et al., 2009). The term 'mistakes' can be construed as intentional acts involving incorrect conceptual knowledge, incomplete knowledge, or incorrect action specifications.

On the other hand, malicious acts are intentional but intended to cause harm (Liginlal et al., 2009). This human failure cannot be eliminated because humans who mobilise and use equipment (technology) carry out actions (processes). Each individual has different behaviours, perceptions, and practices that can cause unintentional threats. Therefore, this study will look at the overall factors that pose unintentional threats to the organisation.

2. Problem Statement

Information leakage is an unauthorised transfer of data between external organisations. It is a widely known fact that humans are the weakest link in the security chain of any organisation (Boulton, 2017) against threats to information security. Although the equipment of the technology is sophisticated and meets the required criteria, the operation of the technology is dependent on humans. If humans fail to handle it properly, information security threats are remained (Aytes & Connolly, 2005).

Human error is the consequence; there is no single root cause for any error or mistake (Lush, 2017). Moreover, the human element makes it more difficult to predict, prevent, and even detect human error than machines. People perform with different capacities and are far from consistent, so the risk of human error cannot be eliminated. Therefore, a human error must be the investigation's starting point, not automatically its conclusion. Thus, a better understanding of human error factors can help an organisation apply appropriate information security protection to prevent unintentional insider threats.

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

3. Research Questions

Human error must be the investigation starting point, not automatically its conclusion. Therefore, the primary purpose of this study is to examine human error factors that cause information security threats. What are the human factors that relate to human error in information security?

4. Purpose of the Study

Understanding human error factors can be beneficial for an organisation to identify the roots of causes of unintentional human error. Applying human error research to classify human error factors will have two benefits. First, it will provide a framework to help organisations understand the human error factors that lead to human errors in their job tasks. The contribution of this paper can give guidance and help stakeholders identify and be more careful about social engineering threats based on their human errors' vulnerabilities.

5. Research Methods

In order to discover the relationship between human error activities, human error factors, and human error taxonomy, a scoping review has been used to retrieve related articles. This study only has reviewed the relevant articles to identify the human error that can cause unintentional insider threats in an organisation. The methodological review was conducted using the framework Arksey and O'Malley (2005) proposed in conjunction with the improvements recommended by Levac et al. (2010). This approach has four phases: identification, screening, eligibility, and result from the review process. The study was gathered using nine pertinent databases with pre-existing keywords to capture relevant literature, as shown in Table 1 broadly. Several rounds of trial and error are attempted to obtain the relevant article with appropriate terms are strung together with Boolean Operator ([AND] and [OR])**.**

Table 1. Database and Keywords used in Scoping Review

Database	Keyword used
Science Direct / IEEE / Scopus / Web of Science / ProQuest / ACM / Emerald / Taylor Francis / Springer	Unintentional insider threat, accidental insider threat, human error, careless, negligent, accidental, slips, lapse, organisation factors, human error factor, information security, information leakage, data breach, data loss, data exfiltration

As shown in Table 2, the inclusion and exclusion criteria were applied to review English eligibility records published from January 2000 to December 31, 2019.

Table 2. Inclusion and Exclusion Criteria

Criteria	Inclusion	Exclusion
Human Error	●Papers that focus on human error factors and describe human error classifications ●Papers that focus on information security factors that relate to organisation factors. ●Papers that provide human error and human mistakes issues on information security.	●Papers not related to human error in information security ●Papers that focus on intentional insider threats

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

The full texts of the selected articles were read, and the relevant data was extracted into a standardised data extraction table. The extracted data items included the source of the articles, title, author, year of publication, type of publication, important findings, and recommendations. The selected articles from databases were categorised based on identified themes to capture the relevant items related to the research question. The results of the literature search on the identification phase are 3742 records. The process was discovered through the selected databases before the deduplication step. These records were screened, unduplicated, and assessed for eligibility. Subsequently, only 52 articles were selected for inclusion in the review (see Figure 1).

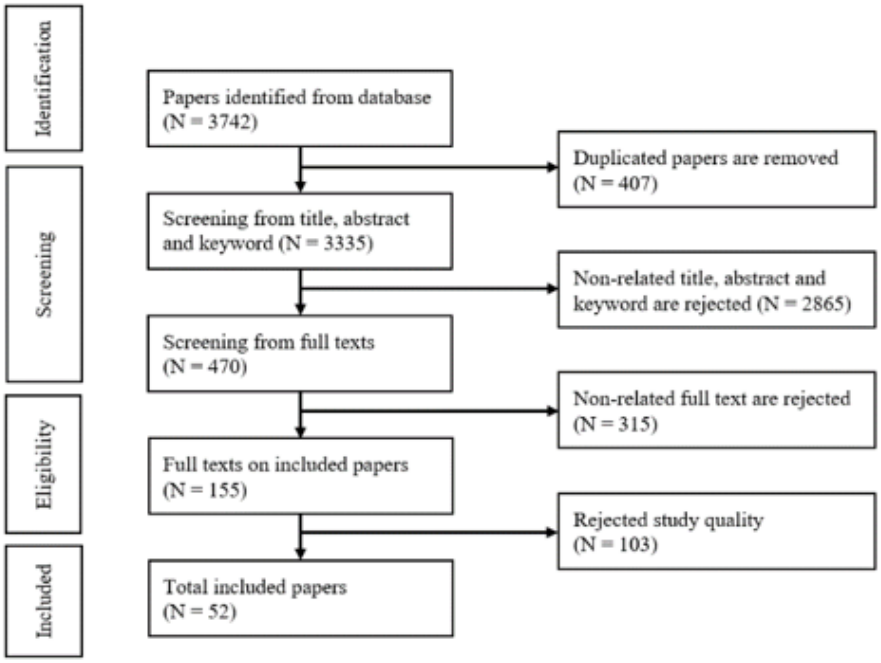

Figure 1. The study selection process by PRISMA guidelines

The total numbers of articles related to human errors in information security based on the selection process are 52 articles. Furthermore, analysis of these articles led to the development of two domains of research: the human factor and the organisation factor. However, each main domain of the human factor consists of a subdomain: careless, negligent, accidental, slips, lapse, mistake, and human error. Meanwhile, a few sub-domains for organisation factors are shown in Appendix 1.

6. Findings

There are many causes of human error issues. Figure 2 represents the extracted data from literature and classifies it into two main components of unintentional insider threat: human error and organisation factors. These two elements are closely related to each other. Furthermore, the analysis of 52 articles also justified 14 elements of organisation factors that contribute to human error, as shown in Figure 2. The highest percentage is awareness (44%), training (40%), and policy enforcement (35%). Other factors contributing to human error are management support, budget, organisation culture and good communication among colleagues. For instance, individual skills performance and errors will be affected

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

when the tasks are too complicated, such as workflow process, unsuitable equipment, an unconducive work environment, irregular work procedures, and ineffective communication with colleagues. Similarly, management factors include lack of resources such as staffing, finance, unorganised planning and work processes, lack of training for employees, lack of emphasis on culture and information security awareness associated with rule-based, knowledge-based human error.

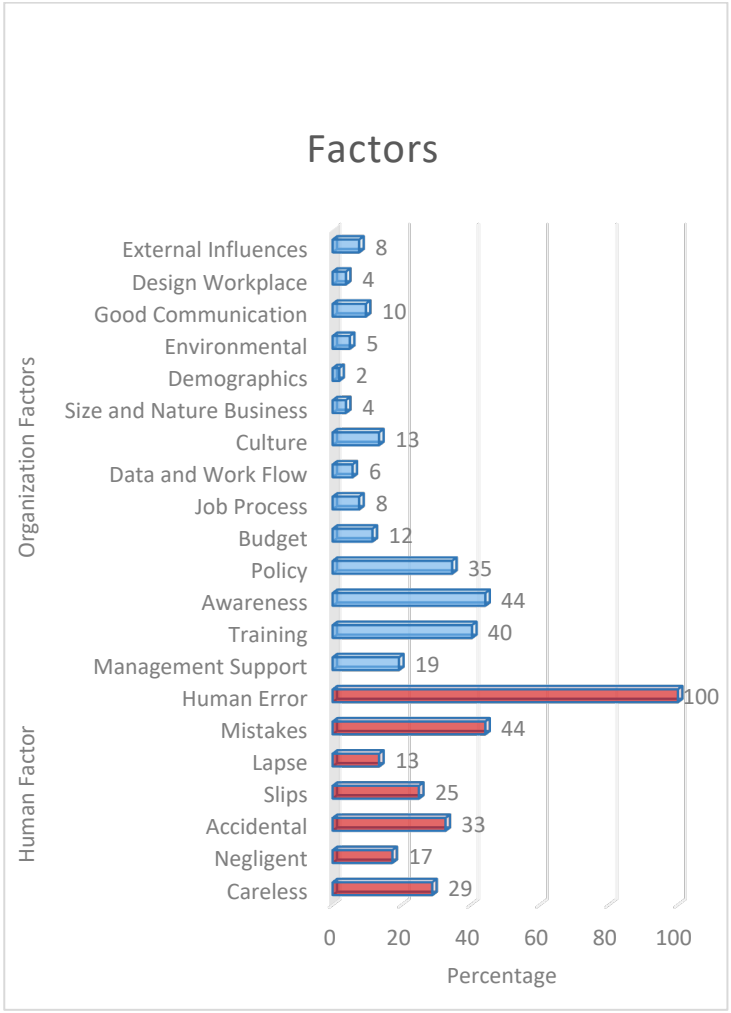

Figure 2. Organisation Factors and Human Errors

6.1. Human Error Taxonomy

Several works of literature have shown that there are three different types of human error: 'mistakes', 'slips' and 'lapse' (Selvik & Bellamy, 2020), leading causes of information leakage (Shu et al., 2016). However, the findings in Figure 3 shows that some terms of human error used in many articles are mistakes (27%), accidental(20%), careless(18), slips (16%), negligent (11%) and lapse (8%). Even the accidental, careless, and negligent keywords are not officially categorised under types of human error, but the terms refer to unintentional insider threats (Gerić & Hutinski, 2007; Munshi et al., 2011).

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

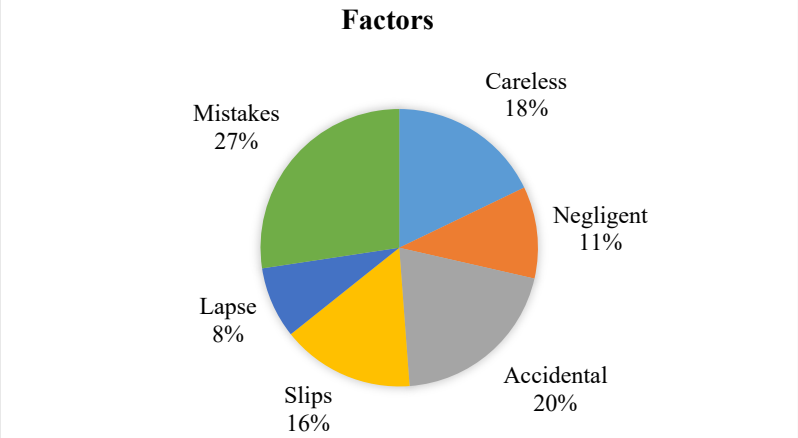

Figure 3. Types of Human Error

Therefore, the summary of human error taxonomy is shown in Figure 4. Human error is divided into two types of action; thinking and action errors. Action error is associated with familiar tasks requiring bit attention which are referred 'slip' and 'lapse'. Slip frequently performed physical action that goes wrong such as rearranging data input into a process control interface. Meanwhile, lapse is a short-term memory lapse; that fails to perform a required action, such as missing a crucial step in a safety procedure.

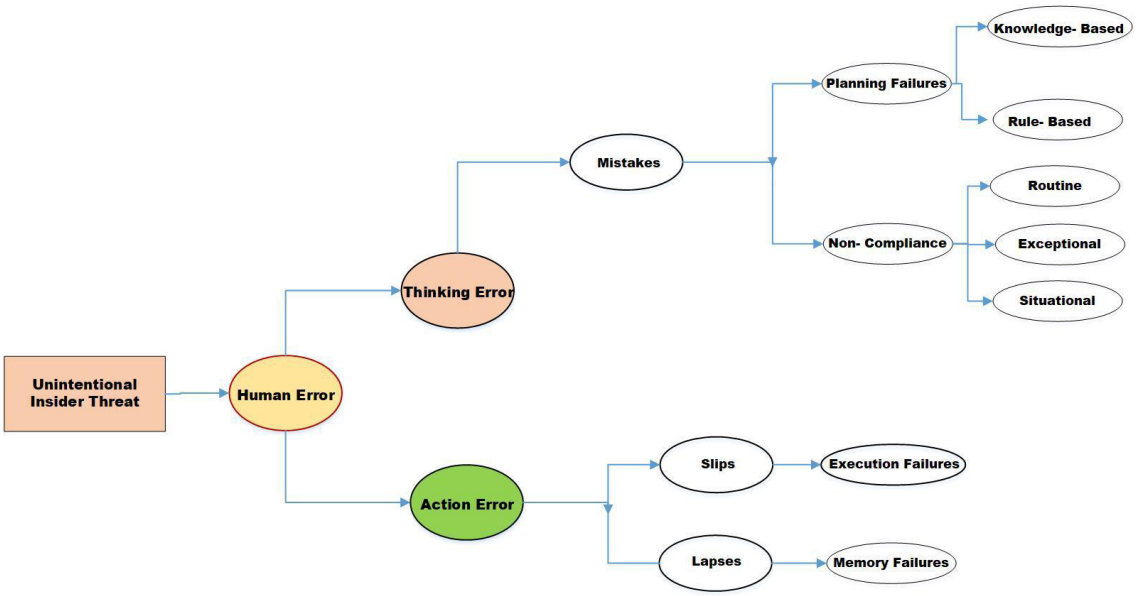

Figure 4. Taxonomy of Human Error

The second category is thinking error, which involves a mental process linked to planning and decision-making failure, such as errors of judgement. When action is planned using conscious thought processes, wrong cause action is taken—something like doing 'the wrong thing believing it to be right. The action of this thinking error is also called a mistake. A mistake occurs because of planning failure and violation. In this case, planning failure is divided into rule-based and knowledge-based. Rule-based mistakes occur when behaviour is based on remembered rules and procedures, or mistakes occur due to

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

misapplication of a good rule or application of a bad rule. It is the opposite of knowledge-based; it occurs if an individual has no rules or routines available to handle an unusual situation.

The violation or non-compliance category refers to deliberate deviations from rules, procedures, or regulations. Sometimes, the action knowingly takes shortcuts or fails to follow procedures to save time, effort, and budget. This action can divide into three acts: routine, situational and exceptional. Routine occurs when non-compliance becomes the 'norm'; consensus that rules no longer apply is commonly characterised by a lack of meaningful enforcement. Situational is non-compliance dictated by situation-specific factors (time pressure; workload; unsuitable tools and equipment; weather); non-compliance may be the only solution to an impossible task. Third, an exception is a person who attempts to solve problems in highly unusual circumstances (often if something has gone wrong); takes a calculated risk in breaking the rules.

Understanding human error taxonomy is essential to understanding the relationship between individual psychological factors and the nature of the organisation. According to Basri and Yusof (2018), human factors that are carelessness and human error have a relationship with management support, training, awareness, job process, data and workflow, nature of business, and work environment.

6.2. Organisation Factor

A vital issue of unintentional internal threats is that organisations rely on trusted personnel to access critical systems, make important decisions, and conduct critical operations. However, any "human error" can lead to various threats if this personnel can endanger confidential data, work for decades, causing losses of millions. Therefore, the justification for selecting technical security controls also should be examined based on human and organisation factors that are possible causes of unintentional internal threats. This criterion is essential since the unintentional action from the negligence of various actions and activities is difficult to predict (Scott & Spaniel, 2017). Based on literature analysis, a relationship between organisational factors and human error factors is shown in Figure 5.

Human error factors are linked to individual psychosocial such as mental health, emotions, behaviour, stress, and demographics will impact when doing tasks or work. Other factors such as stress and emotions can lead to accidents and negligence while performing. Meanwhile, demographic factors that involve culture and gender can also affect personnel's understanding of an information security issue. Sometimes these factors will affect the neglect and violation of policies, procedures, or good practices in an organisation that can inadvertently bring internal threats. Thus, all these human actions are related to the types of human error taxonomy, as explained in Figure 4.

In contrast, organisational factors can be categorised into three main domains: job process, resources, and nature of the organisation. Job process refers to data flow, data classification, the complexity of tasks and the workplace. The complexity in these work processes is a factor to the unintentional insider if the individual is experiencing emotional and physical stress problems. At the same time, management support is crucial because they are the backbone of all organisation implementation and decision-making. Approval elements related to finance, staffing, policy enforcement, and organisational culture are controlled by this group.

https://doi.org/10.15405/epms.2022.10.63
Corresponding Author: Wan Basri Wan Ismail
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

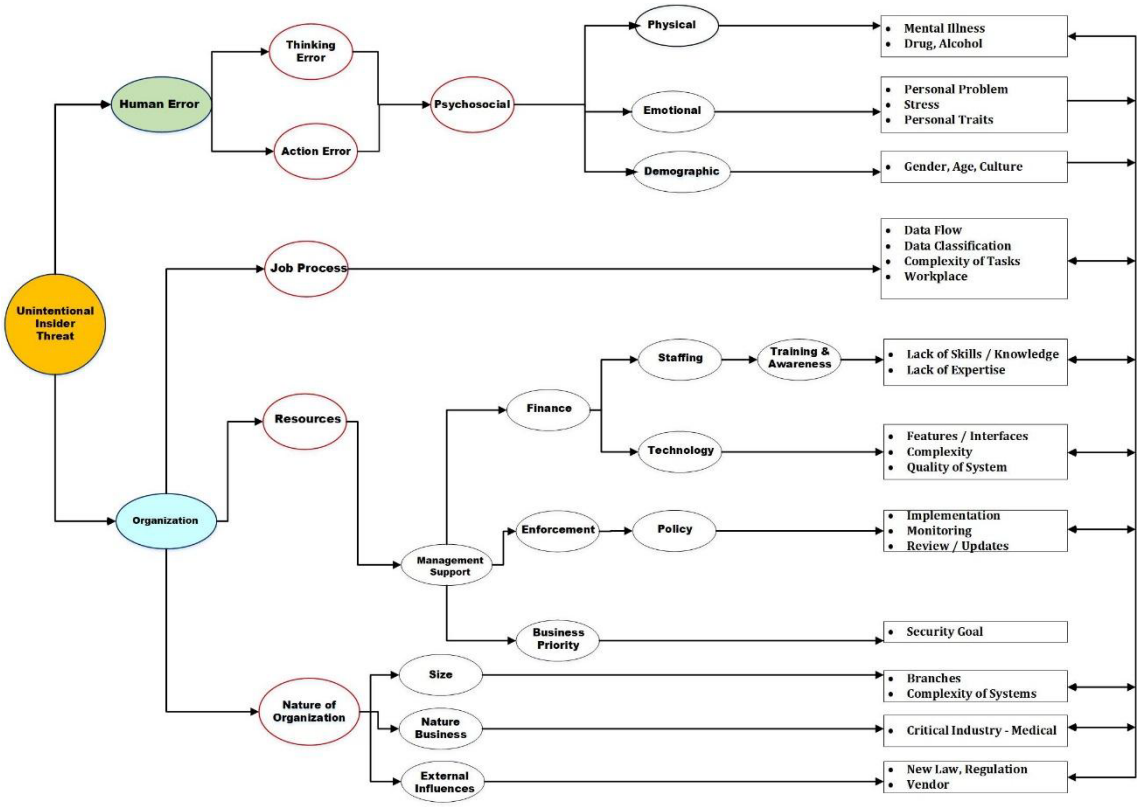

Figure 5. Relationship between Human Error and Organisation Factor

The next crucial organisational factor is related to the type of industry, business and size of the organisation that will affect the unintentional insider threats. The larger the organisation's size, the more complex the system and work processes, causing more challenges to the ICT department to control information security issues. The current high-end technology also does not reach the optimum level if the users and individuals who maintain and monitor it do not follow the correct procedures in setting the system configuration of this technology (Akhunzada et al., 2015; Herath & Rao, 2009; Öğütçü et al., 2016; Safa et al., 2015). Therefore, the factors that influence human behaviour and human factors should be studied more carefully to help improve information security in an organisation.

7. Conclusion

Unintentional internal threats caused by human errors are difficult to predict. Therefore, the organisation must make an appropriate justification for selecting the type of security control that suits the organisation's needs. Although various security control technologies such as the latest firewall or security protection are designed, these technologies cannot work well due to complex tasks. Moreover, hackers are always looking for opportunities and figuring out weaknesses in security technology; the more technologies are created, the more malware is released. Although the technical equipment is sophisticated and meets the required criteria, the technology's operation is human-dependent. If humans fail to handle it properly, information security threats remain.

In many cases, humans always ignore the technical policies and the warnings issued by such control technologies. Therefore, identifying and classifying human error taxonomy and human error

factors will help employees and organisations prevent unintentional insider threats and improve their information security. Organisations should examine the holistic solution to protect their valuable information, especially from unintentional insider threats.

Acknowledgements

This study is funded by the Ministry of Higher Education (MOHE) Malaysia with grant FRGS/1/2019/ICT04/UNISEL/03/1 for the project " A Socio-technical Approach to Unintentional Insider Threats Protection".

References

Akhunzada, A., Sookhak, K., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., Furnell, S., Hayat, A., & Khurram, K. M. (2015). Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, *48*, 44–57. https://doi.org/10.1016/j.jnca.2014.10.009

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework, International *Journal of Social Research Methodology*, *8*(1), 19-32. https://doi.org/10.1080/1364557032000119616

Aytes, K., & Connolly, T. (2005). 'Computer security and risky computing practices: A rational choice perspective', *Advanced Topics in End User Computing*, *4*, 257–279. https://doi.org/10.4018/978-1-59140-474-3.ch013

Basri, W., & Yusof, M. (2018). 'Mitigation Strategies for Unintentional Insider Threats on Information Leaks', *International Journal of Security and Its Applications*, *12*(1), 37–46. https://doi.org/10.14257/ijsia.2018.12.1.03

Boulton, C. (2017, April 19). Humans are (still) the weakest cybersecurity link. *CIO website*. Retrieved on January, 28, 2022 from https://www.cio.com/article/3191088/humans-are-still-the-weakest-cybersecuritylink.html

CyberEdge Group (2020). *2020 Cyberthreat Defense Report*. Retrieved on January, 28, 2022 from https://cyber-edge.com/cdr/#infographic

Ganguly, P. S. (2011). 'Human error Vs . Work place Management in modern organisations', *International Journal of Research in Management and Technology*, *1*(1), 13–17. https://moam.info/queue/human-error-vs-work-place-management-in-modern-iracst_59f283f61723ddbf6358bfc6.html

Gerić, S., & Hutinski, Ž. (2007). Information System Security Threats Classifications. *Journal of Information and Organizational Sciences, 31*(1), 51-61. https://hrcak.srce.hr/21445

Herath, T., & Rao, H. R. R. (2009). 'Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: advancing the methodology. *Implement Sci*, *5*(69). https://doi.org/10.1186/1748-5908-5-69

Liginlal, D., Sim, I., & Khansa, L. (2009). 'How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, *Computers and Security, 28*(3–4), 215–228. https://doi.org/10.1016/j.cose.2008.11.003

Lush, M. (2017). Human Error Prevention : Solutions and Answers. *WHITE PAPER | PHARMA BIOTECH.* Retrieved on January 28, 2022, from https://www.nsf.org/newsroom_pdf/pb_human_error_prevention_solutions_and_answers.pdf

Miyamoto, D., & Takahashi, T. (2013). 'Toward automated reduction of human errors based on cognitive analysis, in *Proceedings - 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2013*, 820–825. https://doi.org/10.1109/IMIS.2013.147

Munshi, A., Dell, P., & Armstrong, H. (2011). 'Insider threat behavior factors: A comparison of theory with reported incidents', *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2402–2411. https://doi.org/10.1109/HICSS.2012.326

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). 'Analysis of personal information security behavior and awareness', *Computers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Reason, J. (1990). *Human Error*. Cambridge University Press. https://doi.org/10.1017/CBO9781139062367

Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. A., & Herawan, T. (2015). 'Information security-conscious care behaviour formation in organisations', *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Schulze, H. (2020). *Insider Threat: 2020 Report*, *Cybersecurity Insiders*. Retrieved Jan 28, 2022, from website: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf

Scott, J., & Spaniel, D. (2017). *In 2017, The Insider Threat Epidemic Begins ICIT Briefing: In 2017, The Insider Threat Epidemic Begins ICIT Critical Infrastructure Forum*. Retrieved on May 28, 2022, from https://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf

Selvik, J. T., & Bellamy, L. J. (2020). "Addressing human error when collecting failure cause information in the oil and gas industry: A review of ISO 14224:2016," *Reliability Engineering and System Safety*, *Elsevier, 194*(C). https://doi.org/10.1016/j.ress.2019.03.025

Shareth Ben (2020). *Insider Threat Report by Securonix*. Retrieved on January 28, 2022, from https://brage.bibsys.no/xmlui/bitstream/handle/11250/143847/Syvertsen-InsiderThreat.pdf?sequence=1&isAllowed=y

Shu, X., Zhang, J., Yao, D. D., & Feng, W-C. (2016). 'Fast Detection of Transformed Data Leaks', *IEEE Xplore: Transactions on Information Forensics and Security*, *11*(3), 528–542. https://doi.org/10.1109/TIFS.2015.2503271