HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Vol. 7, No.1, (2023)

Importance of Human Error Taxonomy for Unintentional Insider Threat

Setyawan Widyarto[1], Syahirah Mohd Nor[2] and, Wan Basri Wan Ismail[3]

[1,2,3] Faculty of Communication, Visual Art and Computing, Universiti Selangor 45600 Bestari Jaya, Selangor
[1]swidyarto@unisel.edu.my, [2]snsyahirahmohdnor@gmail.com, [3]wanbasri@unisel.edu.my

Abstract: The organization has developed an information security program to guide users in handling their data and systems. However, human errors remain a major challenge to information security. This research aims to explore the human error taxonomy, which is closely linked to human error activities and factors that pose a high risk of information leakage in organizations. To study the activities and factors that contribute to human errors, a systematic literature review was conducted to outline the human errors that impact an organization's information security culture. The paper has utilized the human error taxonomy guidance to identify and classify human error activities with their contributing factors. This approach will assist employees and organizations in understanding the importance of human error taxonomy to prevent unintentional insider threats and enhance their information security measures. The identification and classification of human error activities and factors will provide valuable insights to improve the effectiveness of an organization's information security program.

Keywords: Unintentional insider threat; human error; information security; human error factors

1. Introduction

An unintentional insider threat occurs when an authorized insider, without any malicious intent, accidentally disrupts an organization's information technology infrastructure [1]. This can result in sensitive data being unintentionally exposed to the outside world. Insider threats can arise from human error, negligence, or malicious actions by outsiders.

Information leakage refers to the unauthorized transfer of data to external entities. It occurs when sensitive data is intentionally or unintentionally distributed to unauthorized parties [2]. Information technology security is a crucial safeguard against errors made by individuals. It is widely acknowledged that humans are the weakest link in an organization's security chain [3] when it comes to threats to information security. Statistics indicate that human error is one of the primary causes of information leakage [4]. While unintentional insider threats have been formally studied [5], there has not been much research on human error as a component of insider threat issues. Human error can arise from differences in skills, motivations, and knowledge among employees [6], as well as from factors in the work environment, organization, and job processes that influence employee behavior at work [7]. Human error is a significant contributor to quality and production losses in many industries. This study focuses on human error that disrupts an organization's information security. Understanding human error taxonomy and identifying the activities and factors that contribute to human error can assist in applying appropriate information security measures to prevent unintentional insider threats.

2. Methodology

2.1 The Review Protocol – PICOC

In order to examine the relationship between human error activities, human error factors, and human error taxonomy, a systematic process was used to identify and classify

relevant research, utilizing the PICOC protocol. This protocol includes five elements, which are as follows [8]:

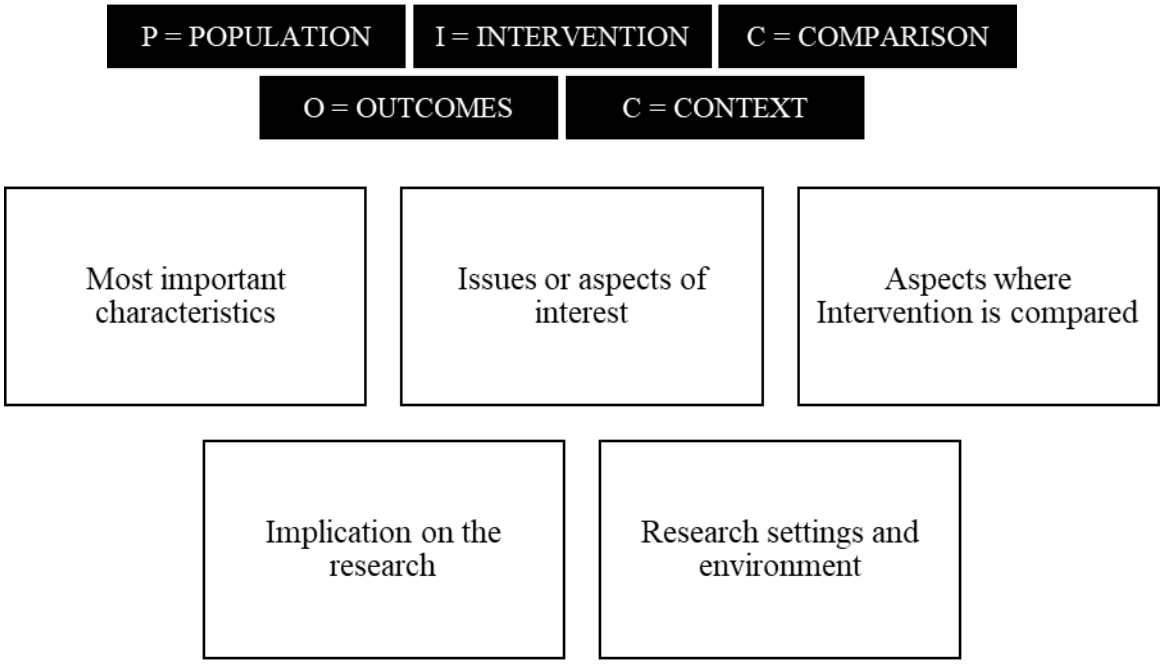

Figure 1: Definition of PICOC

2.1.1 PICOC Structure

PICOC structure for this study will be as follows:

CRITERIA	SCOPE
Population	Organisation
Intervention	Human Error Activities and Human Error Factor
Comparison	Human Error Taxonomy (HET)
Outcomes	Relationship human error elements
Context	Review any studies related to human error elements

2.2 Systematic Research Strategies

A human error taxonomy plays a crucial role in addressing unintentional insider threats, which are caused by individuals within an organization who inadvertently harm its systems, data, or operations. The taxonomy is a systematic classification system that identifies various types of human errors, enabling organizations to determine their root causes and prevent them from recurring in the future. By categorizing human errors into specific types, organizations can prioritize their efforts to mitigate the most significant

risks and minimize the occurrence of unintentional insider threats. Employing a human error taxonomy also enables organizations to identify patterns and trends in human errors, develop targeted solutions to prevent them, improve communication between stakeholders, and enhance their overall risk management strategy.

This study conducted a systematic literature review to identify the human errors that could result in unintentional insider threats in an organization. The review process consisted of four phases: identification, screening, eligibility, and results (see Figure 2). The first phase involved using keywords related to human error, unintentional insider threats, and information leakage (see Table 1). In the screening phase, the 3335 articles were first screened for duplicates, and then the remaining articles were screened based on several inclusion and exclusion criteria (see Table 2). Out of the 155 articles that passed the screening phase, the third stage, known as eligibility, involved reading the full texts of the articles to remove those that did not focus on human error activities and factors that could contribute to unintentional insider threats and information leakage. In the end, only 52 articles were selected for inclusion in the review.

Table 1
Keywords used for the systematic review process

Database	Keyword used
Science Direct / IEEE / Scopus / Web of Science / ProQuest / ACM / Emerald / Taylor&Francis / Springer	Unintentional insider threat, accidental insider threat, human error, human error taxonomy, human error factor, information security, information leakage, data breach, data loss, data exfiltration

Table 2
Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Human Error	• Papers that focus on human error taxonomy and describe human error classifications • Papers that provide human error, human mistakes on information security • Empirical studies on human error factors	• Papers not related to human error in information security • Paper that focus on intentional insider threat

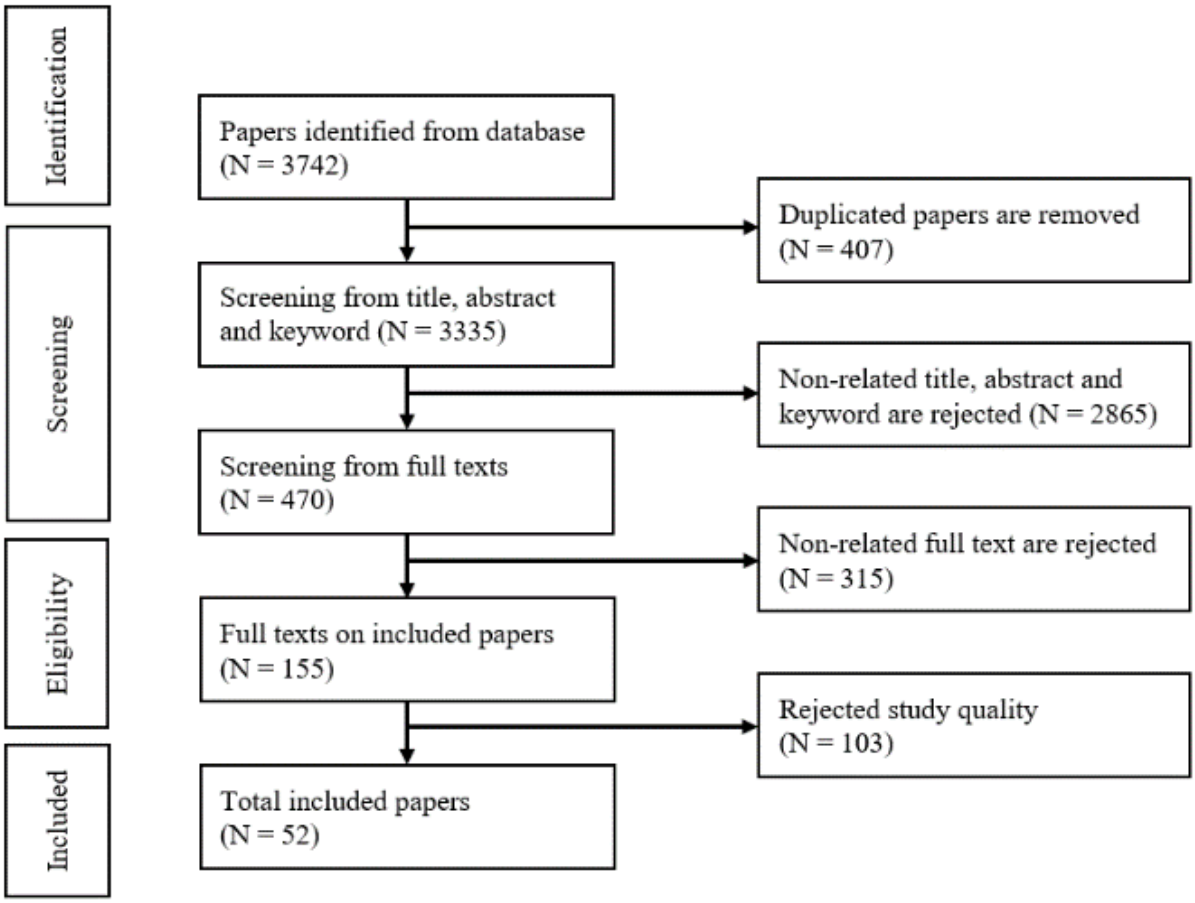

Figure 2: Flow diagram of the study selection

3. Results And Discussion

A systematic review process has resulted in 52 articles related to human error on information security. The result indicates that human error is important to understand to prevent human error in unintentional insider threats. Human error taxonomy and human error factors have been identified and classified as main elements in this study.

3.1 Human Error Taxonomy

There are three types of human errors: mistakes, slips, and lapses [9], leading to information leakage [4]. **Firstly**, slip is a failure of execution, whereas a result of carelessness, the informant fails to perform a properly planned step. **Secondly**, the lapse is an execution failure, whereas a result of a memory failure. **Finally**, the mistake is a knowledge-based error when the plan itself is inadequate to accomplish the objective [10].

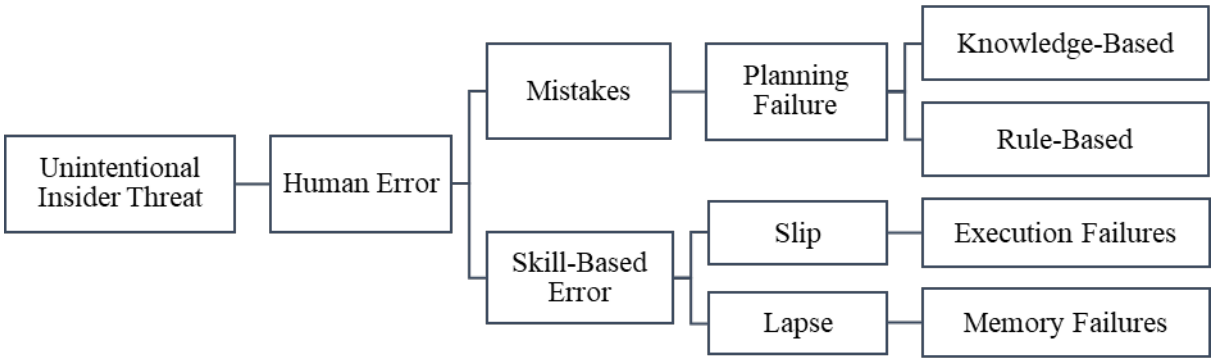

Figure 3: Human Error Taxonomy according to Generic Error Modelling System (GEMS)[11]

3.2 Human Error Factors

Environmental, organisational, and job process will influence the behaviour at work to affect the employee's health and safety. A simple way to view human error factors is to think about four aspects: the individual, job process, work environment, and management support.

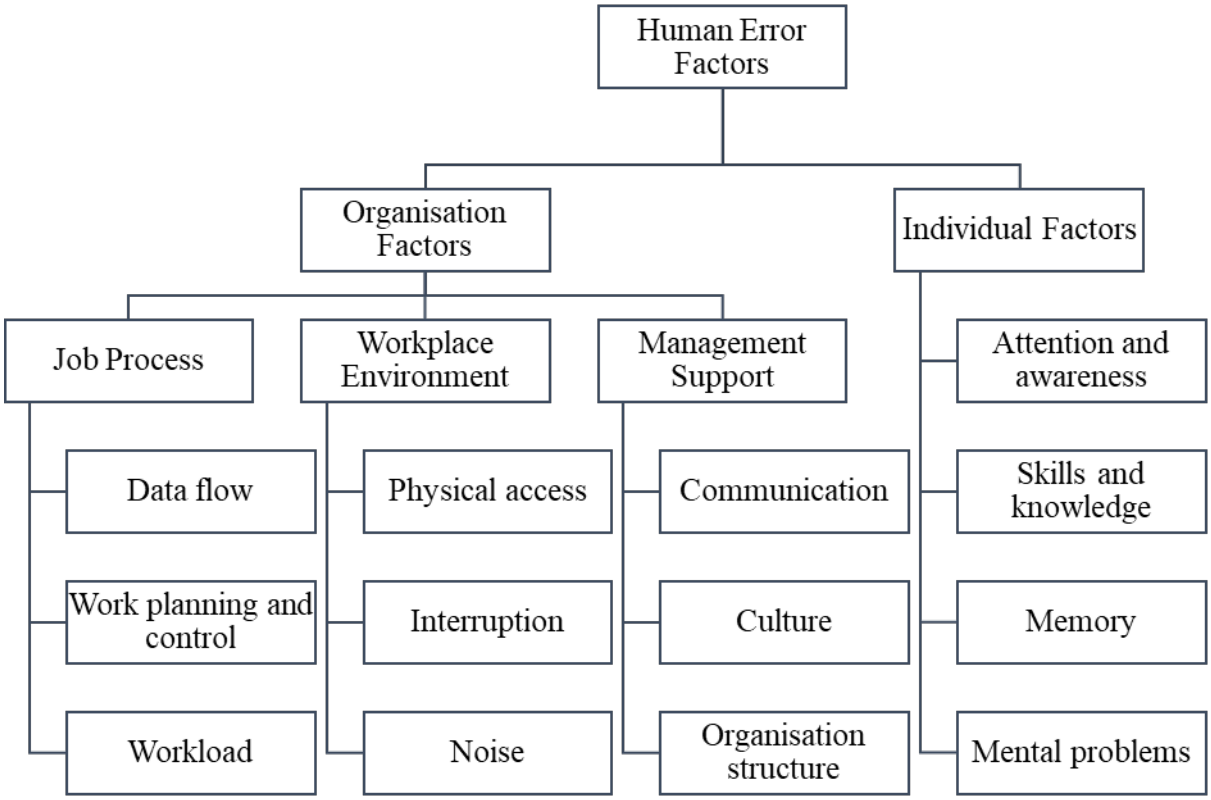

Figure 4: Contributing factors of human error

3.3 Relationship between human error activities, factors, and taxonomy

Possible human error activities have been identified based on the review process and human error taxonomy classification with contributing factors in unintentional insider threat. As a result, we have mapped out the relationship between possible human error activities, human error factors, and human error taxonomy, which will adversely affect an organisation's information security.

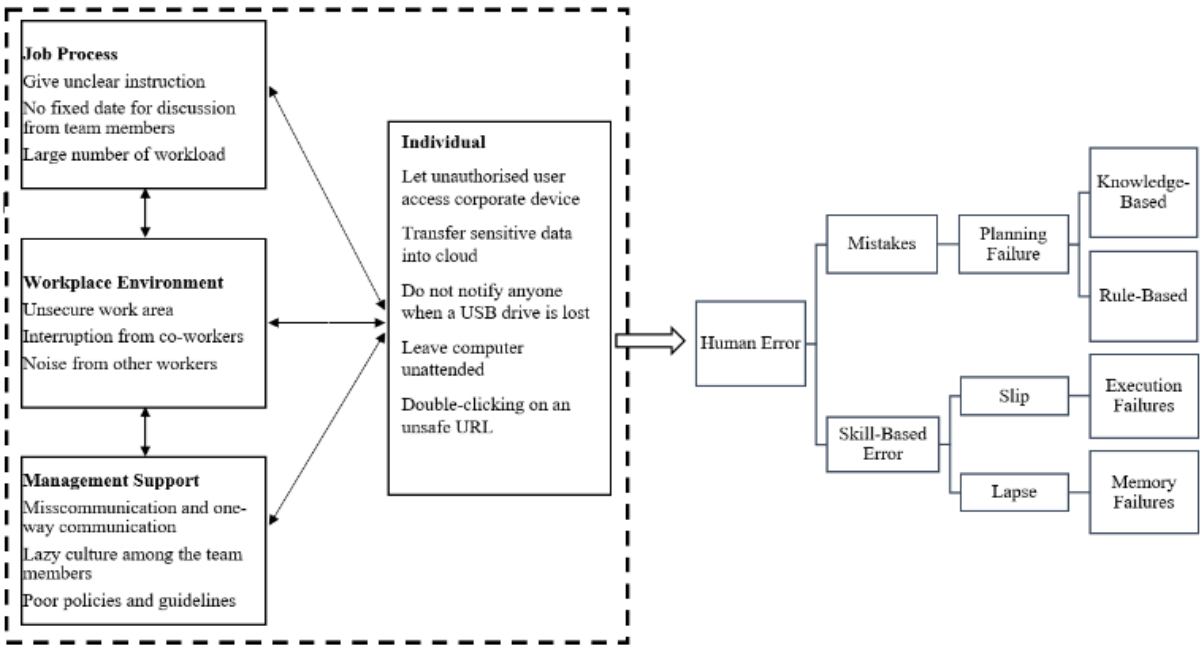

Figure 5: Relationship between possible human error activities, human error factors, and human error taxonomy

4. Conclusion

By identifying and classifying human errors, organisations can develop a structured approach to understanding and preventing errors that could lead to information leakage. The human error taxonomy presented in this paper provides a useful tool for employees and organisations to gain a deeper understanding of the various types of human errors that can occur and the factors that contribute to them. By identifying the most common activities and factors that lead to human error, organisations can take proactive steps to mitigate the risk of information leakage.

For instance, with the help of this taxonomy, organisations can develop tailored training programs and awareness campaigns for their employees to prevent errors caused by specific factors or activities. In addition, organisations can conduct regular reviews of their processes and systems to identify and remove any faults that may have resulted from human errors.

Overall, the identification and classification of human error activities and factors are critical to prevent unintentional insider threats and improve an organisation's information security culture. It is imperative that organisations pay attention to human error taxonomy

and develop strategies to prevent human errors from occurring in the first place. By doing so, they can safeguard sensitive information and protect their reputation and assets. Identifying and classifying human error provides a structured way to understand and prevent human errors that cause information leakage in the organisation. The classification of human error in this paper will help employees and organisations to understand the importance of human error taxonomy and identify the most common activities and factors of human errors to warn against those errors or focus the review process on identifying and removing the faults caused by those errors.

5. Acknowledgements

This research was supported by the A Socio-technical Approach to Unintentional Insider Threats Protection from the FRGS/1/2019/ICT04/UNISEL/03/1. We would like to express our sincere gratitude to the Ministry of Higher Education (KPT) Malaysia for providing the financial support necessary to conduct this research. We would also like to thank Universiti Selangor, where this research was conducted, for providing us with the necessary resources, equipment, and facilities.

References

[1] F. L. Greitzer *et al.*, "Unintentional insider threat: Contributing factors, observables, and mitigation strategies," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2014, doi: 10.1109/HICSS.2014.256.

[2] A. Shabtai, Y. Elovici, and L. Rokach, "A survey of data leakage detection and prevention solutions," in *SpringerBriefs in Computer Science*, 2012.

[3] C. Boulton, "Humans are (still) the weakest cybersecurity link," *Cio.Com*, 2017. .

[4] X. Shu, J. Zhang, D. Yao, S. Member, and W.-C. Feng, "Fast Detection of Transformed Data Leaks," *Ieee Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 528–542, 2016, doi: 10.1109/TIFS.2015.2503271.

[5] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2014-Janua, pp. 236–250, 2014, doi: 10.1109/SPW.2014.39.

[6] D. Miyamoto and T. Takahashi, "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*, 2013, pp. 820–825, doi: 10.1109/IMIS.2013.147.

[7] P. S. Ganguly, "Human error Vs . Work place Management in modern organizations," *Int. J. Res. Manag. Technol.*, vol. 1, no. 1, pp. 13–17, 2011.

[8] T. Dybå, B. A. Kitchenham, and M. Jorgensen, "Evidence-based software engineering for practitioners," *IEEE Softw.*, 2005, doi: 10.1109/MS.2005.6.

[9] J. T. Selvik and L. J. Bellamy, "Addressing human error when collecting failure cause information in the oil and gas industry: A review of ISO 14224:2016," *Reliab. Eng. Syst. Saf.*, no. January, 2019, doi: 10.1016/j.ress.2019.03.025.

[10] V. Anu *et al.*, "Development of a human error taxonomy for software requirements: A systematic literature review," *Inf. Softw. Technol.*, vol. 103, no. June, pp. 112–124, 2018, doi: 10.1016/j.infsof.2018.06.011.

[11] J. Reason, "Review. Human error.," *Hum. error.*, 1990.