Information Security Education Journal (ISEJ)

DLINE JOURNALS

Print ISSN: 2349-8161
Online ISSN: 2349-817X

ISEJ 2026:13 (1)
https://doi.org/10.6025/isej/2026/13/1/35-44

Information Security Education and Incident Analysis: A Holistic Approach in the Digital Era

Pit Pichappan
Digital Information Research Labs
Chennai, Tamil Nadu. India
pichappan@dirf.org

ABSTRACT

Information security has become a paramount concern in the modern digital era, where technology underpins most human activities. Despite technological advancements, human factors remain the most critical vulnerability, often representing the weakest link in security systems. This study explores the vital role of information security education in mitigating cyber risks, emphasizing that awareness training is a critical investment rather than a cost center. Consequently, strategic investments in training are vital. It examines the evolution of Intelligent Educational Systems (IES) and the responsibility of higher education institutions for developing cybersecurity talent amid the challenges of digital transformation. This research contributes to evolving domain practices.

Furthermore, the study presents a detailed analysis of security incidents, categorizing them into data breaches, unauthorized access, and information leakage. Empirical findings indicate that human error and organizational issues are the predominant causes of incidents, surpassing technical vulnerabilities. The study also highlights significant reporting biases that obscure the true scale of cybersecurity threats, as many incidents remain undisclosed. An incident lifecycle framework is proposed to manage security events as dynamic processes rather than isolated occurrences.

Ultimately, the analysis advocates for a holistic approach integrating technological controls with human-centric strategies and organizational governance. Enhancing security education, improving incident reporting mechanisms, and fostering a culture of awareness are essential for building resilience. As cyber threats evolve, a comprehensive, adaptive, and education driven approach is necessary to effectively address the complex nature of modern information security challenges.

Keywords: Information Security, Cybersecurity Education, Human Factors, Incident Analysis, Higher Education, Intelligent Educational Systems, Digital Transformation, Security Awareness

Received: 10 September 2025, Revised 16 November 2025, Accepted 30 November 2025

1. Introduction

Information security has emerged as a critical concern in the modern digital era, where information is considered an invaluable asset and technology underpins most human activities [1]. The rapid advancement of information technologies has significantly increased exposure to cyber risks, leading organisations to prioritise cybersecurity as a fundamental aspect of their operations [2]. The growing sophistication of cyber threats, including ransomware attacks, intellectual property theft, and financial fraud, further intensifies the need for robust security frameworks [3].

Information security measures are typically structured around three core elements: technology, organization, and people. Among these, human factors are considered the most critical and challenging to address, as they often represent the weakest link in security systems [4]. Studies indicate that a substantial proportion of security incidents arise from human errors, such as misoperation, improper data handling, and lack of awareness, alongside organizational weaknesses and technical vulnerabilities [5]. Furthermore, attackers frequently exploit psychological weaknesses through social engineering, underscoring the importance of employee awareness in mitigating risk.

Given these challenges, organizations are increasingly implementing security policies, promoting security-conscious behavior, and encouraging knowledge sharing to strengthen their defense mechanisms [6]. However, despite technological advancements, effective cybersecurity requires a holistic approach that integrates human, organizational, and technical dimensions.

2. Importance of Information Security Education

Information security education plays a vital role in protecting both organizations and individuals from cyber threats. Beyond preventing data breaches and cyberattacks, education helps employees avoid unintentionally contributing to security incidents, which can impose significant psychological and professional burdens. By fostering accurate knowledge and awareness, organizations can create a secure working environment that enhances resilience and operational stability.

Despite its importance, security education is often perceived as a cost center because it does not directly generate visible financial returns. However, in reality, it represents a critical investment, as even a single major security incident can threaten organizational survival. Therefore, improving employee awareness remains one of the most effective strategies for ensuring business continuity.

3. Evolution of Intelligent Security Education

Recent developments in intelligent technologies have enabled the emergence of advanced paradigms in security education. Intelligent Educational Systems (IES) provide technology rich environments that support adaptive, personalized, and engaging learning experiences. These systems enhance the teaching learning process by leveraging artificial intelligence and data-driven approaches to deliver customized educational content.

This study contributes to this evolving domain by exploring cybersecurity technologies and applications in education, evaluating their benefits, and bridging the gap between AI innovations and security education practices. It also aims to provide practical insights for both technology developers and educators working in this field.

4. Cybersecurity in Higher Education

The growing importance of information security has led to increased emphasis on developing cybersecurity talent, particularly within higher education institutions. Universities play a crucial role in research, development, and education, and are actively establishing IT infrastructures to support secure academic environments [7].

Academic programs are increasingly incorporating cybersecurity into their curricula, focusing on essential skills such as secure programming, network security, and offensive security [8]. Literature reviews have further examined the competencies required for cybersecurity professionals [9] and the effectiveness of existing curricula [10]. These efforts highlight the necessity of equipping students with practical and theoretical knowledge to address real world security challenges.

Moreover, cybersecurity education is essential not only for IT professionals but also for organizations of all sizes. Tailored training programs, particularly for small- and medium-sized enterprises (SMEs), are necessary to address their unique security challenges and resource constraints [11] . Universities are also adopting innovative teaching methodologies to ensure that students remain up to date with evolving cyber threats [12, 13].

5. Challenges in Information Security and Digital Transformation

The integration of digital technologies in higher education has transformed the information security landscape, introducing new vulnerabilities and challenges. As institutions adopt advanced digital tools, aligning security measures with technological advancements becomes increasingly critical [14, 15].

Rapid technological adoption often outpaces the development of appropriate security protocols, increasing exposure to cyber risks [Fernández, A]. Additionally, the complexity of modern cybersecurity challenges is amplified by emerging technologies such as cloud computing, Internet of Things (IoT), and artificial intelligence. These technologies introduce new vulnerabilities while also offering potential solutions through machine learning and defensive AI techniques.

To address these challenges, several strategies have been proposed, including strengthening IT infrastructure, implementing secure networks, updating systems, and ensuring data encryption [16] Furthermore, enhancing cybersecurity awareness among staff and students is essential for reducing the likelihood of security breaches

[17]. Building a culture of security awareness within institutions is therefore a key priority, as emphasized in recent research [18].

6. Dependability and Security in Intelligent Educational Environments

Intelligent educational environments, while offering numerous benefits, must also address issues of dependability and security. Dependability is typically associated with high-reliability and safety-critical systems and encompasses attributes such as availability, reliability, and security [19, 20, 21].

As these environments become increasingly complex and technology-driven, ensuring their security and reliability is essential for maintaining trust and effectiveness in educational systems.

7. Security Education Efforts and Incident Analysis

Security education efforts are closely linked to the analysis of real-world security incidents. Studies in this domain often rely on publicly disclosed data from sources such as media reports, corporate announcements, and official disclosures. While this approach provides valuable insights, it is inherently limited by reporting bias, as many incidents remain undisclosed due to reputational and regulatory concerns. [22, 23, 24].

Security incidents can be broadly categorized into data breaches, unauthorized access, and personal information leakage. Analysis indicates that human and organizational factors are the predominant causes of these incidents, including operational errors, weak governance, and insider-related risks. Technical vulnerabilities, such as misconfigurations and unpatched systems, further contribute to these issues. [25, 26.]

A significant limitation in current research is the lack of comprehensive datasets that accurately represent the true scale of cybersecurity incidents. Variations in detection capabilities and disclosure policies lead to inconsistencies in reported data, affecting the reliability of statistical analyses.

Despite these limitations, the findings emphasize the importance of adopting a holistic approach to cybersecurity that integrates human, organizational, and technical perspectives. Enhancing incident reporting mechanisms, improving security awareness, and strengthening governance structures are critical steps toward addressing these challenges.

8. Empirical outlook

In the following section, we present a few empirical discussions of the incidents and the security distribution pattern.

The analysis of security incidents is presented through a structured examination of incident classification, causative factors, distribution patterns, reporting biases, and lifecycle processes. The results derived from Tables 1–2 and Figures 1–3 provide significant insights into the nature and management of security incidents.

As shown in Table 1, security incidents are broadly categorized into data breaches, unauthorized access, and information leakage. Data breaches represent the unauthorized exposure of sensitive information, often

resulting from both external attacks and internal failures. Unauthorized access refers to illicit entry into systems or networks, typically associated with compromised credentials or system vulnerabilities. Information leakage encompasses both accidental and intentional disclosure of data.

This classification highlights the multifaceted nature of security incidents, emphasizing that threats originate from both external adversaries and internal actors. The inclusion of information leakage underscores the importance of addressing non-malicious yet impactful incidents, thereby broadening the scope of security management strategies.

8.1 Classification of Security Incidents

Incident Type	Description
Data Breach	Unauthorized exposure of sensitive data
Unauthorized Access	Illicit system or network access
Information Leakage	Accidental or intentional data disclosure

Table 1. Classification of Security Incidents

8.2 Major Causes of Security Incidents

Category	Examples
Human Error	Misoperation, incorrect data handling
Organizational Issues	Weak policies, poor governance
Technical Vulnerabilities	Misconfigurations, unpatched systems
Insider Threats	Malicious or negligent internal actors

Table 2. Major Causes of Incidents

Table 2 identifies four primary categories of incident causes: human error, organizational issues, technical vulnerabilities, and insider threats. Human error includes misoperations and improper data handling, while organizational issues stem from weak governance structures and inadequate policies. Technical vulnerabilities involve system misconfigurations and unpatched software, whereas insider threats refer to malicious or negligent actions by internal personnel.

The results indicate that security incidents are not solely driven by technical shortcomings but are significantly influenced by human and organizational factors. This finding suggests that effective mitigation strategies must integrate technical solutions with organizational reforms and user awareness initiatives.

8.3 Distribution of Incident Causes

Figure 1 illustrates the distribution of incident causes using a conceptual bar chart. The visual representation indicates that human error and organizational issues constitute the most significant contributors to security incidents, surpassing technical vulnerabilities and insider threats in frequency.

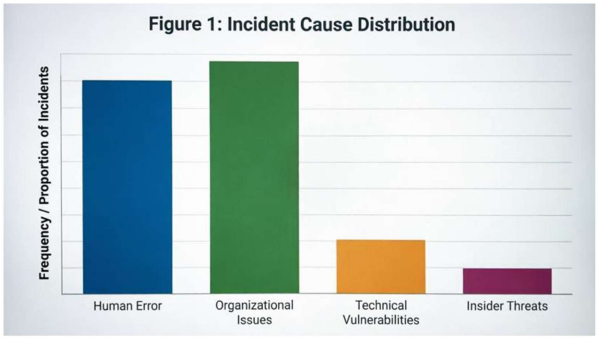

Figure 1. Incident Cause Distribution
(Conceptual Bar Chart)

This distribution reinforces the argument that security challenges are predominantly rooted in human behaviour and organisational practices. Consequently, investments in employee training, policy enforcement, and governance frameworks are likely to yield substantial improvements in security posture. While technical controls remain essential, they should be complemented by robust human-centric and process-oriented measures.

8.4 Incident Reporting Bias

Figure 2 presents the Incident Reporting Bias Model, which demonstrates the progressive reduction of incident data from actual occurrences to publicly disclosed cases. The model shows four stages: actual incidents, detected incidents, reported incidents, and publicly disclosed incidents.

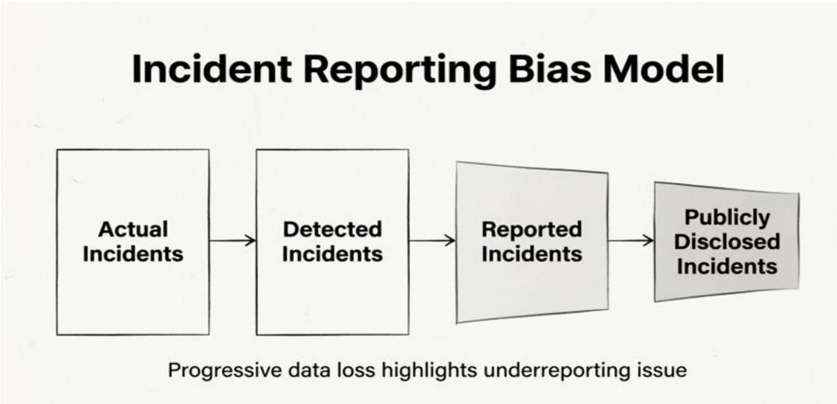

Figure 2. Incident Reporting
Bias Model

The analysis reveals a significant underreporting bias, as a considerable proportion of incidents remain undetected or unreported. Furthermore, only a subset of reported incidents is made publicly available, resulting in incomplete datasets. This discrepancy has important implications for research and policy-making, as reliance on publicly disclosed data may lead to underestimation of the true scale and severity of security threats.

8.5 Incident Lifecycle Framework

Figure 3 depicts the Incident Lifecycle Framework, outlining five sequential stages: occurrence, detection, response, disclosure, and analysis. The framework incorporates feedback loops that facilitate continuous improvement across all stages.

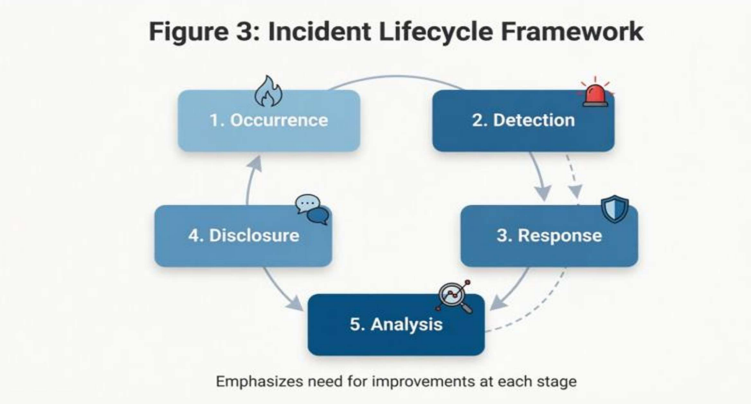

Figure 3. Incident Lifecycle Framework

The lifecycle perspective emphasizes that security incidents should be managed as dynamic processes rather than isolated events. Each stage plays a critical role in determining the overall effectiveness of incident management. In particular, the analysis stage enables organizations to learn from past incidents and implement preventive measures, thereby enhancing future resilience. The presence of feedback mechanisms further highlights the importance of iterative refinement in security practices.

8.6 Integrated Discussion

The combined analysis of the tables and figures reveals several key insights. First, security incidents are inherently multidimensional, involving diverse types, causes, and lifecycle stages. Second, human and organizational factors emerge as dominant contributors, indicating that technical solutions alone are insufficient. Third, the presence of reporting bias suggests that existing datasets may not fully capture the extent of security challenges. Finally, the lifecycle framework underscores the need for continuous monitoring and improvement.

Overall, the findings advocate for a holistic approach to security management that integrates technological controls with human centric strategies, organizational governance, and data transparency. Such an approach is essential for effectively mitigating risks and enhancing the resilience of modern information systems.

9. Discussion

The overall analysis underscores that cybersecurity is a multidimensional challenge requiring coordinated efforts across multiple domains. While technological solutions remain essential, human and organizational factors play a more significant role in determining security outcomes. The increasing complexity of cyber threats further necessitates continuous innovation in both security technologies and educational practices.

Moreover, the presence of reporting bias highlights the need for greater transparency and standardized reporting frameworks to improve the accuracy of cybersecurity research. Educational institutions, in particular, must play a proactive role in developing skilled professionals and fostering a culture of security awareness.

10. Conclusion

In conclusion, information security has become a critical priority in the digital age, driven by the rapid evolution of technology and the increasing sophistication of cyber threats. The findings highlight the importance of integrating human, organizational, and technical approaches to effectively mitigate risks.

Information security education emerges as a key enabler in this context, supporting both individual awareness and organizational resilience. As higher education institutions continue to evolve, their role in shaping future cybersecurity professionals and advancing research becomes increasingly significant. A comprehensive, adaptive, and education-driven approach is therefore essential for addressing the complex and dynamic nature of modern cybersecurity challenges.

References

[1] Burov, O., Lytvynova, S., Lavrov, E., et al. (2020). Cybersecurity in Educational Networks. Ahram ET, Karwowski W, Vergnano A, et al., editors. Intelligent Human Systems Integration 2020. IHSI 2020. *Advances in Intelligent Systems and Computing*. *Springer*; 2020; Vol.1131: p.359–364.

[2] Safa, N. S., Sookhak, M., Solms, R., et al. (2015). Information security conscious care behaviour formation in organisations. *Comput. Secur.* 53:65–78. 10.1016/j.cose.2015.05.012.

[3] Torten, R., Reaiche, C., Boyle, S. (2018). The impact of security Awareness on information technology professionals' behavior. *Comput. Secur.* 79:68–79.

[4] https://in.kddi.com/en/resources/knowledge/column-security-09/#1.-why-is-information-security-education-important? [What Is Information Security Education? Effective Training Topics and Methods to Raise Employee Awareness].

[5] https://www.jnsa.org/result/incident/2019/2019-005.pdf.

[6] Safa, N. S., Maple, C., Watson, T., et al. (2018). Information security collaboration formation in organisations. *IET Inf. Secur.* 12 (3)238–245.

[7] Ulven, J. B., Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet.13* (2):39.

[8] Švábenský, V., Vykopa,l J., Èeleda, P. (2020). What Are Cybersecurity Education Papers About?: A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In: SIGCSE'20: Proceedings of the 51st *ACM Technical Symposium on Computer Science Education.*

[9] Jones, K. S., Namin, A S., Armstrong, M. E. (2018). The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Trans. Comput. Educ.*18 (3) 1–12.

[10] Parrish, A., Impagliazzo, J., Raj, R. K, et al. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. ITiCSE 2018 Companion: Proceedings Companion of the 23rd Annual ACM Conference

on *Innovation and Technology in Computer Science Education*.

[11] Bada, Maria., Jason, R. C., Nurse. (2019). Developing cybersecurity education and awareness programmes for Small and medium-sized enterprises (SMEs, *Information Computer Security Journal*, 27 (3) 393-410.

[12] Cheung, R. S, Cohen, J.P, Lo, H. Z. (2011). Challenge based learning in cybersecurity education. In: Proceedings of the International Conference on Security and Management (SAM). 2011;1

[13] Beuran, R., Chinen, K i., Tan, Y. et al. (2016). Towards Effective Cybersecurity Education and Training. *Japan Advanced Institute of Science and Technology*.

[14] Jonathan, G. M., Gebremeskel, B. K. (2020). Information security and organisational agility in the digital era: Exploring the role of IT alignment. *In: Proceedings of the 11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference, IEMCON 2020, Vancouver, BC, Canada, 4–7 November 2020; IEEE: Piscataway, NJ, USA*. p. 831–836.

[15] Mohamed Hashim, M. A., Tlemsani, I., Matthews, R. (2022). Higher education strategy in digital transformation. *Educ. Inf. Technol.* 2022, 27, 3171–3195.

[16] Alenezi, A. (2024). Cybersecurity risks and strategies in learning services of higher education institutions (HEIs) in developing and emerging countries A critical scoping review. *Egypt J. Bus. Stud.* 48, 480–506.

[17] Siphambili, N. (2024). Exploring cybersecurity implications in higher education. In Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS 2024), Jyvaskyla, Finland, 27–28 June 2024; p. 526–531.

[18] Gkrimpizi, T., Peristeras, V., Magnisalis, I. (2023). Classification of barriers to digital transformation in higher education institutions: Systematic literature review. *Educ. Sci.* , 13, 746.

[19] Avižienis, A., Laprie, J.C., Randell, B., Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secur. Comput.* 1, 11–33.

[20] Laprie, J.C. (1995). Dependability Its attributes, impairments and means. In: Predictably Dependable Computing Systems; Randell, B., Laprie, J.C., Kopetz, H., Littlewood, B., Eds.; ESPRIT Basic Research Series; Springer: Berlin/ Heidelberg, *Germany* .

[21] Dubrova, E. (2013). Fault-Tolerant Design; Springer Science+Business Media: *New York, NY, USA*.

[22] Flores, WR., Ekstedt, M (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Comput. Secur.* 2016;59:26–44.

[23] Rowe, DC., Lunt, BM., Ekstrom, JJ (2011). The role of cyber-security in information technology education. In: SIGITE'11: *Proceedings of the 2011 Conference on Information Technology Education* .

[24] Khaleefah, A. D., Al-Mashhadi, H. M. (2024). Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review. *Iraqi J. Sci.* 65 (1) 468–486.

[25] AlDaajeh, S., Saleous, H., Alrabaee, S, et al. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Comput. Secur.* 119:102754.

[26] Fernández, A., Gómez, B., Binjaku, K., Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. *In: Education and Information Technologies; Springer: New York, NY, USA,* 2023; Volume 28, p. 12351–12382.