# Cyber Security Training 2.0 - from theoretical learning to practical experience

Clemens Huber[1], Michael Kohlegger[1], Reinhard Bernsteiner[1] and Christian Ploder[1]

[1]MCI Internationale Hochschule GmbH, Universitätsstraße 15, 6020 Innsbruck / Austria

**Abstract**

In the face of rising cyber threats, particularly SQL injection (SQLi) attacks, improving employee awareness through effective training is critical. This paper presents a comparative study evaluating the impact of a practice-oriented training approach versus a purely theoretical one on learners' understanding and self-efficacy regarding SQLi. Using a pre- and post-test design with 28 participants, the study examined learning outcomes across three knowledge dimensions—basic, application, and transfer—alongside perceived ability and satisfaction. Results show that the combination of theory and hands-on exercises significantly enhances knowledge acquisition and confidence, particularly in basic and application knowledge. While transfer knowledge gains were limited, the findings emphasize the importance of integrating applied content in cybersecurity education. Limitations and future research directions are discussed to improve assessment depth and generalizability.

**Keywords**

IT Security, Security Training, SQL Injections, Security Awareness

## 1. Introduction

This paper aims to investigate whether practice-oriented training formats can significantly improve learners' understanding and practical competence in identifying and mitigating SQL injection vulnerabilities compared to traditional theoretical training approaches.

With the increasing digitization of business processes and the proliferation of interconnected systems, the attack surface for malicious actors has expanded dramatically. Among the most persistent and impactful vulnerabilities in modern web applications is SQL injection (SQLi), which exploits improper handling of user input in database queries. Despite longstanding awareness, SQLi remains prevalent and continues to cause high-impact breaches across sectors [1].

Beyond technical defenses, the human factor remains a critical vulnerability. Studies highlight that a large proportion of security breaches are facilitated by insufficient awareness and training of system users and developers [2]. As such, improving cybersecurity awareness through training is now a central strategy in organizational risk management [3].

While numerous awareness programs exist, their effectiveness varies widely. In many cases, training is delivered through static, theoretical formats that fail to equip learners with practical skills or the confidence to apply them. Particularly for small and medium-sized enterprises (SMEs), the challenge is acute: limited resources often prevent investment in interactive or customized security education [4]. According to the Austrian Federal Criminal Police Office, cybercrime is increasing sharply, with a notable drop in resolution rates [5]. These trends underline the need for more impactful, scalable training models.

This study explores whether incorporating practical exercises into a theoretical training module improves learning outcomes and perceived capability in identifying SQLi threats. This is subsumed in the following overall research question:

*What is the impact of a practice-oriented training approach on learners' knowledge acquisition*

*NWISEd 2025: Workshop on Co-Creating New Ways, of Information Systems Education, September 10–11, 2025, Maribor, Slovenia*
clemens.huber@mci.edu (C. Huber); michael.kohlegger@mci.edu (M. Kohlegger); reinhard.bernsteiner@mci.edu (R. Bernsteiner); christian.ploder@mci.edu (C. Ploder)
0000-0002-4538-973X (M. Kohlegger); 0000-0002-8142-3544 (R. Bernsteiner); 0000-0002-7064-8465 (C. Ploder)

*and perceived self-efficacy regarding SQL injection, compared to a purely theoretical training approach?*

The presented results of this paper exclusively focus on SQL injection. Other attack vectors such as cross-site scripting (XSS) were part of the original study but are excluded here to maintain a focused and coherent contribution. Likewise, technical implementation aspects of the training platform are not the subject of this paper. Defense mechanisms are addressed only at a conceptual level, supporting the didactic framing of the training.

## 2. Theoretical Background

To contextualize the training approach and its relevance, this chapter provides an expanded discussion of the cybersecurity landscape, the attack life cycle, SQL injection as a persistent vulnerability, and key defensive measures. These foundations establish the rationale for integrating practical exercises into cybersecurity education.

### 2.1. Cybersecurity Landscape and Risk Management

Cybersecurity has evolved from being a purely technical discipline to an integral component of organizational risk management strategies. Increasing digitization and interconnected IT environments amplify both the complexity and potential impact of cyberattacks. Reports consistently highlight that cyber incidents now represent one of the most critical operational risks for enterprises, on par with financial and compliance risks [6]. Beyond the immediate financial implications, breaches frequently trigger reputational damage, legal penalties, and regulatory obligations, particularly under frameworks such as the General Data Protection Regulation (GDPR) [7, 8].

A proactive approach to cybersecurity therefore extends beyond deploying technical controls; it requires the integration of human-centered measures such as training and awareness programs [3]. Numerous studies indicate that technical safeguards alone cannot eliminate vulnerabilities caused by user error or insecure coding practices [2]. Consequently, effective risk management frameworks increasingly incorporate continuous training to reduce human-related weaknesses, strengthen security culture, and ensure compliance with industry standards [4].

### 2.2. Attack Lifecycle: The Cyber Kill Chain

Understanding attacker methodologies is vital for designing effective training programs. The Cyber Kill Chain model, developed by Lockheed Martin, conceptualizes a typical cyberattack as a sequence of seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives [9]. By breaking down complex attacks into discrete steps, this model illustrates how adversaries progress from initial reconnaissance to achieving malicious goals, such as data exfiltration or system compromise [10].

From a pedagogical perspective, the Cyber Kill Chain is valuable for structuring defensive thinking. It helps learners understand not only *where* vulnerabilities exist but also *when* and *how* interventions can be most effective. In the context of this study, the model supports the argument for practical exercises: while theoretical knowledge may help learners recognize high-level concepts, hands-on practice enables them to identify and disrupt specific stages of an attack, thereby translating abstract concepts into actionable defense strategies.

### 2.3. Understanding SQL Injection

SQL injection (SQLi) remains one of the most prevalent and damaging web application vulnerabilities, ranking consistently among the top security risks identified by OWASP and CVE databases [1, 11]. At its core, SQLi exploits insufficient input validation and insecure query construction, enabling attackers

to manipulate application logic to gain unauthorized access to databases [12]. A common example is embedding malicious SQL code in user input fields, which—when concatenated into a query without proper sanitization—executes unintended commands such as retrieving confidential data or altering database structures.

Despite being a well-documented vulnerability for over two decades, SQLi persists in modern systems. This persistence can be attributed to several factors: (1) widespread use of legacy systems that lack robust safeguards, (2) inconsistent adoption of secure coding practices, and (3) inadequate developer training on preventive measures [13]. The impact of SQLi can be severe, ranging from unauthorized disclosure of sensitive data to full system compromise, with cascading effects on operational integrity and regulatory compliance [13].

Addressing SQLi effectively therefore requires not only technical solutions, such as parameterized queries and input validation, but also comprehensive awareness among developers and IT personnel. This connection underscores the rationale for this study: bridging the gap between theoretical understanding and practical competence in mitigating SQLi vulnerabilities.

### 2.4. Defensive Approaches

Mitigating SQLi vulnerabilities requires a layered defense strategy that combines secure coding practices, architectural safeguards, and proactive validation mechanisms. According to OWASP guidelines, one of the most effective measures is the use of *prepared statements* (also known as parameterized queries). These enforce a strict separation between SQL logic and user-provided input by defining the query structure in advance and binding external data as parameters. This approach ensures that user input cannot alter the intended execution flow, effectively eliminating the primary attack vector for SQLi [13].

Complementing this measure, *stored procedures* offer an additional layer of security by encapsulating SQL logic in predefined database routines. These routines operate under restricted execution rights and minimize the need for dynamic query construction, thereby reducing exposure to injection vulnerabilities [11]. When combined with robust access control policies, stored procedures can significantly limit the impact of potential exploitation.

Another critical element is *allow-list input validation*, which proactively defines acceptable input patterns based on data type, character set, and length constraints. Unlike blacklisting—where known malicious patterns are excluded—allow-listing only permits predefined valid inputs, thereby reducing the likelihood of unanticipated attacks [13]. For maximum effectiveness, this approach should be supported by regular expressions, schema validation, and centralized input handling routines.

These defensive practices, while highly effective when implemented correctly, rely on consistent developer awareness and adherence to secure coding standards. Consequently, the inclusion of such concepts in cybersecurity training is essential. The goal is not only to convey abstract principles but also to demonstrate practical application through realistic scenarios, reinforcing the connection between defensive theory and implementation in real-world systems.

## 3. Methodology

This chapter outlines the research methodology used to assess the effectiveness of the proposed practice-oriented cybersecurity training. It details the underlying evaluation framework, research design, hypothesis development, survey instrumentation, and validation procedure, with a focus on understanding learning gains related to SQL injection and stored cross-site scripting (see 1.

### 3.1. Research Design and Evaluation Model

To investigate the impact of integrating interactive, practice-based elements into cybersecurity training, a comparative quantitative study was conducted. The objective was to determine whether learners exposed to a combined theoretical and practical learning environment demonstrate significantly greater knowledge acquisition than those receiving only theoretical content.

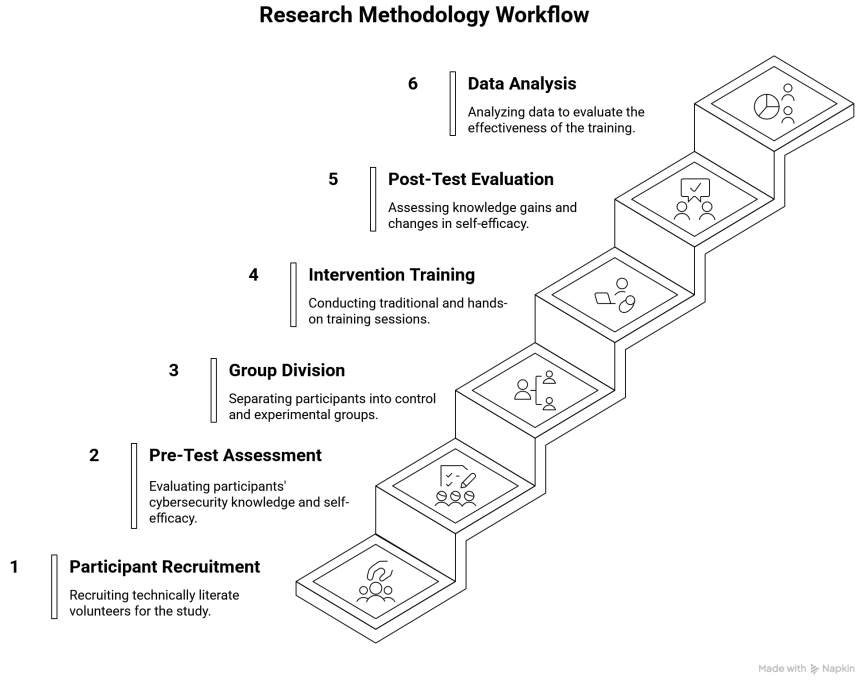


**Figure 1:** Overall Methodology Workflow

The study design followed a pre-test/post-test format with a between-subjects comparison, where participants were randomly assigned to one of two conditions: Group A received purely theoretical instruction, while Group B received identical theoretical content supplemented by hands-on exercises on a controlled training platform. Knowledge gain was measured by comparing pre- and post-test results, while learner self-efficacy and satisfaction were evaluated using Likert-scaled survey items.

### 3.1.1. Evaluation Framework: The Kirkpatrick Model

The evaluation framework was guided by the well-established Kirkpatrick Model [14], which provides a comprehensive four-level structure for assessing training effectiveness. **Level 1, Reaction** evaluates participants' satisfaction with the training and their perceived self-efficacy—in this study, specifically their confidence in identifying SQL injection vulnerabilities. **Level 2, Learning** assesses the degree to which participants acquire intended knowledge, skills, and attitudes, which was measured here using structured pre- and post-tests on cybersecurity concepts. Each test comprised five multiple-choice items aligned with Bloom's taxonomy, including two questions on basic knowledge (e.g., "Which of the following best describes an SQL injection?"), two on application knowledge (e.g., "Which query construction introduces the highest SQLi risk?"), and one on transfer knowledge involving an unfamiliar scenario.

The remaining levels of the model, while not implemented in the present study, are important for understanding the broader framework. **Level 3, Behavior** focuses on the transfer of learning to actual practice, i.e., whether participants apply the acquired knowledge in their work or daily behavior. **Level 4, Results** evaluates the training's ultimate impact on organizational or systemic performance outcomes, such as reduced security incidents or improved compliance rates.

This two-level evaluation design—centered on Reaction and Learning—enabled triangulation of objective learning outcomes and subjective participant perceptions. These are both critical dimensions in assessing the short-term effectiveness of cybersecurity training interventions, particularly in settings where long-term behavioral tracking (Level 3) or organizational metrics (Level 4) are impractical due to temporal or contextual constraints.

#### 3.1.2. Hypothesis Development

Based on the study's objectives and grounded in learning science and cybersecurity training literature, the following four hypotheses were formulated:

- **H1:** Group B achieves significantly higher overall learning gains than Group A.
- **H2:** Group B demonstrates significantly greater improvement in application-level knowledge than Group A.
- **H3:** Group B achieves higher gains in transfer knowledge compared to Group A.
- **H4:** Participants with less than six years of IT experience in Group B achieve above-average learning gains compared to the overall average.

These hypotheses aimed to test both content-specific knowledge acquisition and differential effects across subgroups, particularly based on prior IT experience. Participants provided background information including self-reported years of IT experience, prior exposure to security training, and professional role. IT experience was captured as a continuous variable in years.

### 3.2. Survey Instruments and Test Design

The central research instrument consisted of pre- and post-tests aligned with Bloom's revised taxonomy [15], focusing on three cognitive levels: factual knowledge (basic understanding), application (use of concepts in familiar contexts), and transfer (application in novel situations).

#### 3.2.1. Pre- and Post-Test Structure

Each test included five questions, divided across the three knowledge dimensions:

- **Basic Knowledge (2 items):** Definitions and recognition of SQLi/XSS mechanisms.
- **Application Knowledge (2 items):** Problem-solving based on realistic attack scenarios.
- **Transfer Knowledge (1 item):** Application of learned principles to unfamiliar but analogous contexts.

Identical questions were used in the pre- and post-tests to measure learning gains. All questions were multiple choice with equal weight to ensure fair aggregation of results across groups and categories.

#### 3.2.2. Scoring and Measurement Consistency

Each correct answer was awarded one point, resulting in a maximum test score of five points. By assigning uniform weights across all items, we ensured internal consistency and comparability across test conditions. Although the transfer category included only a single item, it was weighted equally to reflect its importance in gauging deep conceptual understanding.

### 3.3. Validation Procedure and Sample Characteristics

A total of 28 participants took part in the study. They were recruited from a technically literate population with varying degrees of cybersecurity experience. Participants provided informed consent and were randomly assigned to Group A or B based on anonymized IP registration, which was deleted post-analysis in accordance with data privacy protocols.

To protect participant identity while preserving test traceability, all responses were linked using pseudonymous IDs. The collected data were cleaned and standardized before analysis. No participants were excluded.

The cohort included both entry-level learners and professionals with IT backgrounds, ensuring a diverse sample to test hypothesis H4 related to prior experience. The threshold of six years was selected based on prior literature identifying this as an approximate boundary between early-career and experienced IT professionals [16]. While the sample size limits generalizability, it allowed for meaningful statistical comparisons under controlled conditions.

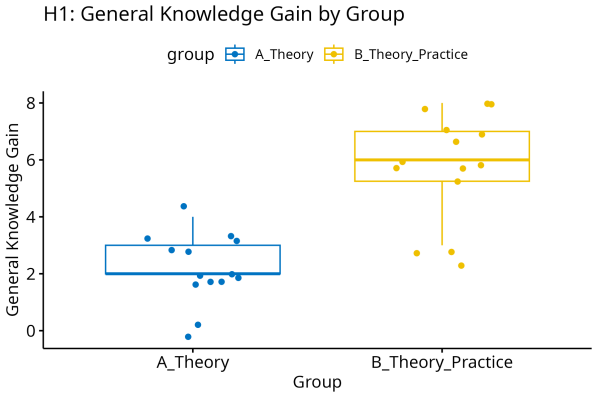


**Figure 2:** Learning gains: Group A vs. Group B (H1)

# 4. Results and Interpretation

This chapter presents the results of the quantitative evaluation of the cybersecurity training formats and interprets them with regard to the defined hypotheses. The data were analyzed using non-parametric statistical tests due to the small sample size and non-normal distribution. The central research question guiding this analysis is whether integrating practical exercises significantly improves learners' understanding of SQL injection and their ability to apply this knowledge in realistic contexts.

## 4.1. Overview of Key Findings

The data analysis reveals several notable patterns. First, participants in the combined training group (Group B) consistently outperformed those in the theory-only group (Group A) across all tested knowledge dimensions. This performance gap was particularly pronounced for basic understanding and applied knowledge of SQL injection and cross-site scripting, supporting the notion that practice-based reinforcement enhances knowledge retention and applicability.

However, the analysis also revealed limitations in knowledge transfer. Despite modest improvements in the transfer category, the results were not statistically significant. This finding suggests that deep conceptual understanding, required for transfer to unfamiliar situations, may require longer or more complex instructional interventions.

## 4.2. Hypothesis-Specific Results and Interpretation

Each of the four evaluated hypotheses is discussed below, based on descriptive statistics and inferential analysis using the Mann–Whitney U test.

**H1: Group B achieves significantly higher overall learning gains than Group A.** Group B (theory + practice) achieved a mean learning gain of 5.86 points, while Group A (theory only) averaged 2.21 points. The Mann–Whitney U test yielded a statistically significant result with a large effect size ($r = 0.726$), indicating that the practical components contributed meaningfully to learning success. The result supports H1 and confirms that practical exercises improve overall knowledge acquisition in SQL injections.

**H2: Group B demonstrates significantly greater improvement in application-level knowledge than Group A.** Application knowledge scores, which reflect learners' ability to solve concrete problems based on SQLi scenarios, showed a significant advantage for Group B. The mean learning gain in this category was 2.79 points for Group B compared to significantly lower scores in Group A. The statistical analysis revealed a large effect size ($r = 0.752$), confirming H2. These results align with prior

research suggesting that active engagement with realistic scenarios enhances applied cybersecurity competence [17].

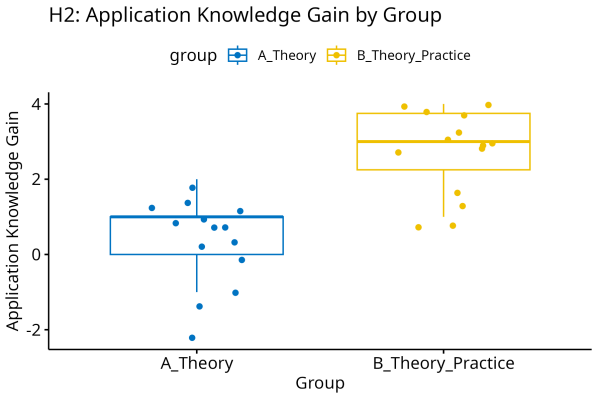


**Figure 3:** Application knowledge gains (H2)

**H3: Group B achieves higher gains in transfer knowledge compared to Group A.** Transfer knowledge refers to learners' ability to apply concepts to novel or unfamiliar scenarios. While Group B showed a slightly higher mean gain (0.786 points) compared to Group A (0.643 points), the difference was not statistically significant ($p = 0.286$). The limited effect could be attributed to several factors: (1) only one transfer item was included in the test, reducing the sensitivity of the measurement, and (2) transfer generally requires abstract reasoning and time for reflection—conditions not fully met in this study's short intervention format. Therefore, H3 must be rejected.

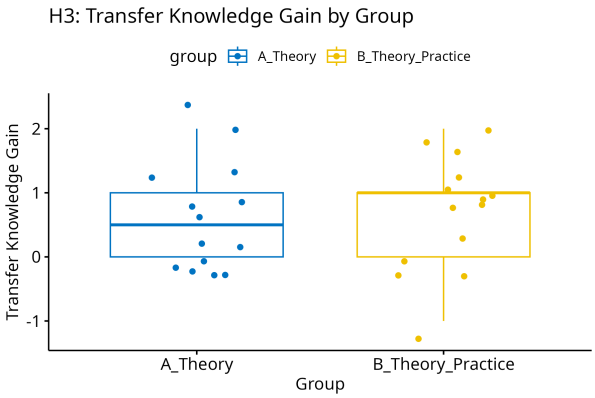


**Figure 4:** Transfer knowledge comparison (H3)

**H4: Participants with less than six years of IT experience in Group B achieve above-average learning gains.** To assess whether less experienced participants (IT experience < 6 years) benefited more from the combined approach, their mean gain (6.42 points) was compared to the overall Group B average (5.86 points). While this subgroup demonstrated higher learning gains, the difference was not statistically significant. Nevertheless, the trend suggests that interactive, hands-on formats may be particularly helpful for novices, a finding consistent with constructivist learning theories [16]. Thus, H4 is partially supported.

## 4.3. Answering the Research Question

The primary research question posed by this study was:

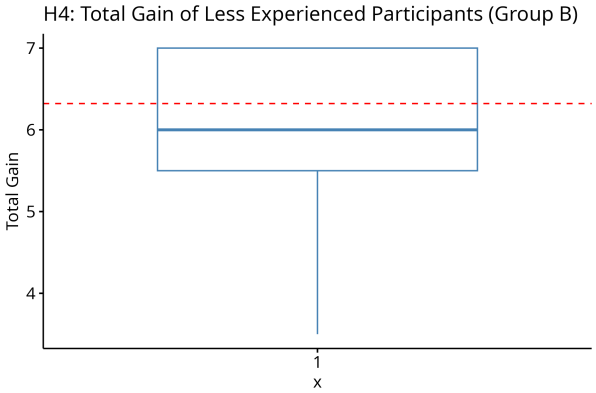


**Figure 5:** Learning gains by IT experience (H4)

> *What is the impact of a practice-oriented learning approach on learners' knowledge acquisition and perceived self-efficacy regarding SQL Injection and Stored Cross-Site Scripting, compared to a purely theoretical training approach?*

The findings demonstrate that integrating practical training elements significantly improves learning outcomes in foundational and application-level cybersecurity knowledge. This is particularly relevant in the context of known vulnerabilities such as SQL injection, which continue to be a major threat to web applications [1, 12].

Moreover, the study underscores the value of active learning formats in boosting self-efficacy—an important determinant of behavior change in security practices [17]. While the short duration of the intervention limited deep transfer learning, the results clearly support the integration of practice-based content in future cybersecurity education formats.

## 5. Limitations

While the findings of this study provide valuable insights, several methodological limitations warrant explicit consideration. These limitations influence both the internal validity of the results and their generalisability to broader contexts.

### 5.1. Sample Size and Participant Profile

The sample consisted of 28 participants, which, although sufficient for exploratory analysis, constrains statistical power and increases susceptibility to Type I and Type II errors [18]. Furthermore, the cohort was relatively homogeneous, consisting primarily of technically literate individuals who voluntarily opted into the study. This may introduce self-selection bias and reduce the representativeness of the findings, particularly for learner groups with less technical background or lower intrinsic motivation. Future research should address these limitations by recruiting larger, more heterogeneous samples, ideally incorporating participants from diverse professional domains and varying levels of technical expertise.

### 5.2. Assessment Instrument Design

The evaluation relied exclusively on multiple-choice questions, which, while suitable for measuring factual knowledge and structured application, may inadequately capture nuanced understanding or complex reasoning processes essential for real-world cybersecurity decision-making. Additionally, the measurement of transfer knowledge—the ability to apply principles to unfamiliar scenarios—was limited to a single item. This narrow design likely reduced sensitivity in detecting deeper cognitive learning

outcomes, which are central to long-term behavioral change. Future studies should employ mixed-method approaches, integrating open-ended questions, multi-step problem-solving tasks, or qualitative methods such as interviews and think-aloud protocols to achieve richer and more comprehensive assessments.

### 5.3. Intervention Duration and Depth of Learning

The practical training component was delivered within a brief intervention window, which, although sufficient for demonstrating short-term gains in basic and application-level knowledge, limits the ability to foster and measure sustained learning retention or higher-order cognitive processes. Transfer of learning typically requires iterative practice, reflection, and exposure to varied contexts [19]. Future research should therefore consider longitudinal designs with extended interventions and post-training follow-ups to evaluate both knowledge durability and behavioral integration in professional environments.

## 6. Conclusion

This study examined the effectiveness of integrating practical exercises into cybersecurity training focused on SQL injection, comparing a theory-only approach with a combined theory-and-practice format. The findings clearly demonstrate that practice-oriented training significantly enhances learners' knowledge acquisition and self-efficacy, particularly in basic and application-level competencies. These results support the argument that experiential learning formats offer greater value than purely theoretical approaches in preparing individuals to recognize and mitigate security vulnerabilities.

Despite these promising outcomes, the research is subject to important methodological constraints that inform directions for future work. The modest sample size and relatively homogeneous participant profile limit statistical power and generalisability. Expanding future studies to include larger and more diverse cohorts will improve robustness and relevance across different learner populations. Furthermore, the reliance on multiple-choice assessments, combined with the inclusion of only a single transfer knowledge item, restricts the ability to capture nuanced reasoning and deeper conceptual understanding. Employing adaptive assessment strategies—such as open-ended problem-solving tasks or qualitative interviews—would allow richer insights into cognitive processes and learning strategies. Finally, the brief duration of the intervention constrains evaluation of long-term retention and behavioral transfer, which are essential for meaningful impact in professional contexts. Longitudinal research designs incorporating extended interventions and complex real-world scenarios are recommended to address this gap.

By systematically addressing these limitations, future research can contribute to the development of scalable, evidence-based training models that foster not only short-term knowledge gains but also sustained behavioral change. This will be critical for equipping organizations with the human capabilities needed to counter evolving cyber threats in increasingly complex digital ecosystems.

## Declaration on Generative AI

During the preparation of this work, the author(s) used ChatGPT 4o in order to: Grammar, spelling check and improving the language quality. After using the tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content. Additionally figure 1 was built with the support of napkin.ai.

## References

[1] CVE Details, Vulnerabilities by type, https://www.cvedetails.com/vulnerabilities-by-types.php, n.d. Accessed: 2025-05-23.

[2] Verizon, 2022 Data Breach Investigations Report, Technical Report, Verizon, 2022. URL: https://www.verizon.com/business/resources/reports/dbir/, accessed: 2025-05-21.

[3] H. Aldawood, G. Skinner, Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues, Future Internet 11 (2019) 1–16. URL: https://www.mdpi.com/1999-5903/11/3/73. doi:10.3390/fi11030073.

[4] A. Chidukwani, S. Zander, P. Koutsakis, A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations, IEEE Access 10 (2022) 88243–88269. doi:10.1109/ACCESS.2022.3197899, received 7 July 2022, accepted 26 July 2022, published 10 August 2022, current version 19 August 2022.

[5] Bundesministerium für Inneres, Bundeskriminalamt, Cybercrime Report 2023: Lagebericht über die Entwicklung von Cybercrime, Technical Report, Bundesministerium für Inneres, Wien, 2024. URL: https://bundeskriminalamt.at, zugriff am 21. Mai 2025.

[6] IBM Security, Cost of a Data Breach Report 2024, Technical Report, IBM Corporation, 2024. URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec, accessed: 01 May 2025.

[7] European Parliament and Council of the European Union, Article 33 GDPR – Notification of a personal data breach to the supervisory authority, 2016.

[8] European Parliament and Council of the European Union, Article 82 GDPR – Right to compensation and liability, 2016.

[9] Lockheed Martin Corporation, Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense, Technical Report, Lockheed Martin Corporation, 2015. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf, whitepaper.

[10] I. Tarnowski, How to use cyber kill chain model to build cybersecurity?, 2017. URL: https://tnc17.geant.org/core/presentation/49.html.

[11] J. Clarke, SQL Injection Attacks and Defense, Syngress Publishing / Elsevier, Burlington, MA, 2009.

[12] M. Alsalamah, H. Alwabli, H. Alqwifli, D. M. Ibrahim, A review study on sql injection attacks, prevention, and detection, The ISC International Journal of Information Security 13 (2021) 1–9. doi:10.22042/ISECURE.2021.0.0.0, selected Paper at ICCMIT'21 in Athens, Greece.

[13] OWASP Foundation, Sql injection prevention cheat sheet, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#defense-option-1-prepared-statements-with-parameterized-queries, 2024. Accessed: 2025-05-21.

[14] H. Khan, H. Patil, Effective teaching assessment model: Utilizing the kirkpatrick evaluation framework, International Journal of Creative Research Thoughts (2024). Assistant Professor, Computer Engineering Department, Thakur College of Engineering & Technology, Mumbai, India.

[15] B. S. Bloom, M. D. Engelhart, E. J. Furst, W. H. Hill, D. R. Krathwohl, Taxonomy of Educational Objectives: The Classification of Educational Goals, Handbook 1: Cognitive Domain, David McKay Company, Inc., Ann Arbor, Michigan, USA, 1956. Originally published by Longmans, Green and Co., London.

[16] N. Ben-Asher, C. Gonzalez, Effects of cyber security knowledge on attack detection, Computers in Human Behavior 48 (2015) 51–61. URL: https://doi.org/10.1016/j.chb.2014.10.076. doi:10.1016/j.chb.2014.10.076, available online 9 February 2015.

[17] J. W. Coffey, Ameliorating sources of human error in cybersecurity: Technological and human-centered approaches, in: Proceedings of the 8th International Multi-Conference on Complexity, Informatics, and Cybernetics (IMCIC 2017), International Institute of Informatics and Systemics (IIIS), Pensacola, FL, USA, 2017, pp. 85–88. URL: https://www.iiis.org/CDs2017/CD2017Spring/papers/ZA253LY.pdf.

[18] D. Knudson, Type i and type ii errors: What do they mean and why are they important?, Kinesiology Review 3 (2014) 3–5. doi:10.1123/kr.2013-0011.

[19] D. N. Perkins, G. Salomon, Transfer of learning, International Encyclopedia of Education 2 (1992) 6452–6457.