# Simulating ERP Cyber Incidents: A Serious Game for Awareness and Incident Management

Judith Strussenberg[0009−0003−8585−7862], Alexander Henkel, Steffi Rudel[0009−0006−5728−7577], and Ulrike Lechner[0000−0002−4286−3184]

University of the Bundeswehr Munich, Neubiberg, Germany
{judith.strussenberg,alexander.henkel,steffi.rudel,ulrike.lechner}@unibw.de

**Abstract.** ERP systems are fundamental to enterprise operations. As a result, they are increasingly targeted by sophisticated cyberattacks. This paper presents the design, implementation and evaluation of a serious game scenario titled *ERP-Systems in Need*, developed to raise awareness of cybersecurity specifically within ERP contexts. Building on the existing game *A Question of Security*, this work applies a Design Science Research approach to simulate realistic ERP security incidents. The serious game emphasizes experiential learning through multirole scenarios and was evaluated in academic settings. The findings suggest that the game is effective in increasing knowledge, participation, and preparedness for ERP-related cyber threats.

**Keywords:** Serious games · ERP · IT security · Cybersecurity · Awareness

## 1 Introduction

Enterprise Resource Planning (ERP) systems are critical to the operational backbone of many organizations, supporting essential processes such as procurement, logistics, finance, and human resource management. As these systems become increasingly interconnected and exposed to external networks, their vulnerability to cyberattacks has increased substantially. A successful cyberattack on an ERP system can paralyze entire supply chains, disrupt production, and cause significant financial and reputational damage. An actual survey shows that ERP systems are in the focus of ransomware attackers. 62 % of the attacked companies faced a downtime of at least 24 hours. Experts see one reason for the lack of knowledge about ERP-specific security [22].

Although cybersecurity training and awareness programs are a common mitigation strategy, traditional approaches such as classroom lectures, slide-based tutorials, or compliance checklists often fail to engage users or produce lasting behavioral change. Recent research suggests that serious games, interactive simulations with educational objectives, offer a promising alternative. By immersing users in realistic scenarios and enabling experiential learning, serious games can foster understanding and long-term awareness of cybersecurity risks.

This paper addresses the lack of gamified training tools specifically aimed at ERP security. Building on the existing serious game *A Question of Security* [26], which focuses on ransomware attacks on mobile devices, we present the design, implementation, and evaluation of a new scenario titled *ERP-Systems in Need*. The game simulates a multi-phase cyberattack on an ERP system and places participants in dual roles: as individual employees and as decision-makers in management. The objective is to improve participants' awareness of ERP system vulnerabilities, incident response strategies, and business continuity.

The development followed the Design Science Research (DSR) methodology according to Hevner and incorporated iterative design evaluation through two playtest sessions. Feedback from these sessions informed improvements to the game structure, content and user interaction elements [12].

This paper is structured as follows. Section 2 reviews the relevant background on ERP systems, cybersecurity training, and serious games. Section 3 outlines the applied research methodology. Section 4 details the game scenario and game development. Section 5 presents the implementation and playtesting process. Section 6 discusses the evaluation results, followed by a critical reflection and future work in Section 7.

## 2 Theoretical Background and Related Work

The following section deals with theories and topics for this serious game. After a look at the challenges related to the security of ERP systems, we consider the background of serious games and discuss the question of which serious games related to ERP are known for research.

### 2.1 ERP Systems and Cybersecurity

Enterprise Resource Planning (ERP) systems are integrated software platforms that support and automate core business functions such as finance, supply chain management, procurement, and human resources. Their centrality in business operations and their role as comprehensive data and process hubs make them high-value targets for cyberattacks. In recent years, attackers have increasingly exploited ERP-specific vulnerabilities, particularly in widely used platforms such as SAP and Oracle ERP [8]. In the basic protection module APP.4.2, the German Federal Office for Information Security (BSI) lists four key reasons for the current vulnerability of ERP systems: failure to take into account SAP security recommendations, failure to apply patches and SAP security notices promptly or at all, lack of planning, implementation and documentation of an SAP authorization concept, and lack of documentation and emergency concept. The measures to be implemented are derived from this, such as secure configuration and rights management, network security, and securing the ERP database and the associated interfaces and servers [3]. SAP itself also provides documents on this topic, such as the SAP Security Baseline Template, which has also been included in the implementation notes for the module APP.4.2 SAP ERP system.

The five main topics of the baseline template are infrastructure security, secure code, installation and operational security, and security guidelines [4].

A notable example of a ERP-related security risk occurred in early 2025 with the discovery and active exploitation of the vulnerability CVE-2025-31324. This vulnerability, rated with a maximum CVSS score of 10.0, allowed attackers to gain full administrative control over affected SAP systems. As reported by SAP and Onapsis, exploitation allowed access to sensitive business processes and data, and opened pathways for the deployment of ransomware and lateral movement across enterprise networks [19,14]. Particularly impacted were organizations classified as critical infrastructure providers.

According to Onapsis' mid-year threat report, the first half of 2025 alone revealed an unusually high number of critical vulnerabilities in SAP systems. These weaknesses were found to expose companies to risks such as espionage, sabotage, fraud, and service disruption through malware or ransomware [14]. Numbers like this are also an issue for SAP itself and its relationship with its customers because it leaves some of their most critical processes vulnerable. This causes trust issues and a SAP 2012 awareness campaign shows that they are well aware of the fact that trust is the ultimate currency in their business [17]. The figures mentioned above on vulnerabilities seem somewhat abstract until you look at specific cases, such as the Conapi case study, which shows how human decisions combined with a lack of technical security measures led to a data leak from a medium-sized company's ERP system that ended up costing it around 1.8 million euros and led to the publication of company secrets, a GPDR fine, the loss of customers, and orders [6]. In the case of Stoli Group USA, an SAP security breach was at least partly responsible for the company's insolvency in 2024 [23].

In addition, there are other digital attacks that do not directly target ERP systems but use them as a vehicle, such as deep fake scams. The case of a Hong Kong financial employee has become widely known. He transferred around 25.6 million dollars to cyber criminals after a video call with his 'chief financial officer' and other board members that were all deep faked [11]. Increasing employee awareness of cases like these is essential. Although there were still some sensational cases in 2024, Sam Altman, CEO of OpenAI, the company behind ChatGPT, warned of a global 'fraud crisis' in the summer of 2025. He claimed that AI has now fully defeated most of the ways people currently authenticate, other than passwords [5].

Despite the increasing risk profile of ERP platforms, cybersecurity awareness initiatives in many organizations continue to focus on endpoints, office software, or generic IT systems. ERP platforms are often excluded from such training programs or treated as black-box systems managed solely by IT departments. This creates a dangerous gap, especially as attacks increasingly target ERP users via phishing, misconfigurations, and compromised credentials. To train ERP security tailored to the needs of an organization is crucial because even the smallest affected parts of a critical supply chain can cause massive alterations. We showed this in the example of an infected label printer that was used to print

labels to store and ship goods or labels for traceability. Without this small piece of hardware attached to an ERP system, a company's activity can come to a complete stop [9].

### 2.2 Serious Games

Serious games integrate educational objectives with game-based elements, creating interactive learning experiences that go beyond mere entertainment [7,10,16]. They have proven to be effective in various domains, such as education, healthcare care and corporate training, by enhancing the motivation, engagement, and retention of the learner's knowledge [15,25,13]. Research suggests that features such as progressive difficulty, real-time feedback, and structured reflection phases significantly improve learning outcomes [24]. Immersive and scenario-based game environments contribute to deeper emotional engagement and knowledge retention. In addition, serious games have shown the potential to foster awareness, empathy, and even behavior change in areas such as response to crisis, ethics, and social responsibility [20].

Collaborative gameplay mechanics have also been shown to strengthen communication, negotiation, and coordination skills, especially in multi-role training contexts [1]. These elements are particularly relevant for fields like cybersecurity and incident response, where teamwork is essential.

To be effective, serious games must integrate learning content and game mechanics in a way that is not only educationally sound, but also intuitive and motivating [16]. Designs that support usability, clarity, and low cognitive overhead ensure that learners can focus on content rather than interface. Layered complexity and increasing challenges help maintain motivation, while timely feedback and space for reflection reinforce skill acquisition [15,25].

In sum, serious games offer a powerful approach for conveying complex real-world competencies in a structured yet engaging manner. When applied to domains such as ERP cybersecurity and incident management, they can simulate realistic stress scenarios, encourage active problem solving, and build practical skills that can be transferred to workplace settings.

### 2.3 ERP-Systems in Serious Games

Several gamified approaches have been developed to support ERP learning, primarily in educational settings. One of the most widely used is the ERP Simulation Game (ERPSim), which allows students to experience the integration of business processes and the transaction flow using SAP software in a competitive environment [2]. Similarly, Legner et al. propose a role-based simulation game to teach ERP architecture and process logic in academic curricula [18].

These games have shown benefits in fostering understanding of business concepts and improving soft skills such as problemsolving, teamwork, communication, and time management [21]. However, they primarily focus on process efficiency, system usage, and business decision making under normal operating conditions.

Unlike ERPSim, which emphasizes transactional accuracy and integrated process learning, the game presented in this document prioritizes incident response, role-specific decision making under uncertainty, and cross-functional communication during cybersecurity crises. Changes the learning focus from operational optimization to organizational resilience and situational awareness.

Although there are limited examples of security-focused ERP games, one notable exception is the multiplayer game by Tritscher et al., which explores the misuse of ERP systems for financial fraud scenarios [27]. Although thematically relevant, this game does not emphasize defense mechanisms or awareness training for ERP users.

This indicates a gap in the existing landscape: while simulation-based ERP games are well-established in business education, few address ERP-specific cybersecurity threats. This paper contributes to closing this gap by presenting a serious game adapted to the compromise of the ERP system, enabling players to experience and manage the organizational consequences of a security breach.

## 3 Research Design

This study follows the principles of Design Science Research (DSR) to develop, evaluate and iteratively refine a serious game aimed at increasing cybersecurity awareness in ERP system contexts. DSR provides a structured approach to creating artifacts that are both practically relevant and theoretically grounded [12].

The research process incorporated the following elements:

**Relevance Cycle:** The problem was identified through a gap in existing cybersecurity training, which rarely addresses ERP-specific risks. ERP systems were recognized as critical and highly vulnerable, and users lack contextual awareness and structured response training.

**Design Cycle:** The scenario for the game was developed iteratively, with five structured rounds that simulate a cyber attack on an ERP system. Roles, materials, and mechanics were refined based on user feedback, game testing, and alignment with real-world threat patterns (e.g. ransomware, lateral movement). The core design decisions were informed by the gamification principles and the educational design literature.

**Rigor Cycle:** The artifact is grounded in established knowledge bases, including cybersecurity standards (e.g. BSI, NIST), serious game design research, and ERP threat models. Reviews of the literature and empirical studies on gamified learning shaped the mechanics, role structure, and evaluation metrics of the game.

The game was test played in two academic sessions with groups of technical and non-technical students. Mixed method evaluation was used, combining Likert scale questionnaires, facilitator observations, and open feedback to assess usability, engagement, and perceived learning impact. Revisions were made between sessions to address the complexity of the quiz, the fairness of scoring, and the clarity of the role.

In general, the DSR methodology allowed the development of a validated, context-sensitive learning tool that addresses a concrete organizational need.

## 4 Scenario Design and Game Development

The serious game *ERP-Systems in Need* was developed as a scenario-driven role-based training tool designed to simulate cybersecurity incidents in enterprise environments. It builds on the foundational mechanics of the previously established game *A Question of Security* [26], which focused on the compromise of mobile devices. In contrast, the new scenario shifts focus to the compromise of the entire organization's ERP system, requiring a more complex design to reflect enterprise-level decision-making and coordination.

### 4.1 Scenario Concept and Objectives

The primary objective of the game is to increase awareness of ERP-specific cybersecurity threats and improve players' ability to assess and respond to incidents from both technical and organizational perspectives. The scenario models a progressive cyberattack targeting an ERP environment, involving indicators such as data corruption, access anomalies, and system unavailability. Learning goals include recognizing indicators of compromise within ERP processes, practicing decision making under uncertainty in different organizational roles, understanding interdependencies within supply chain and HR modules, and applying knowledge of best practices for security from standards such as BSI and NIST.

### 4.2 Structure and Gameplay Flow

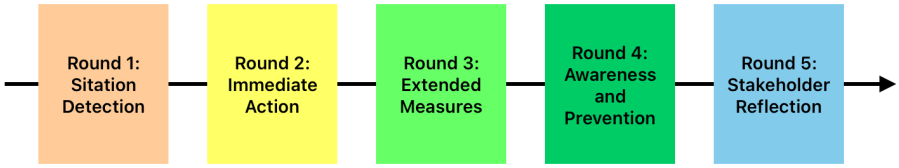


**Fig. 1.** Round scheme of *ERP-Systems in Need*.

The game consists of five rounds, each representing a phase in the incident lifecycle:

1. **Situation Detection:** Players analyze symptoms and system behavior to identify a possible breach.

2. **Immediate Action:** Groups develop short-term containment and communication strategies.
3. **Extended Measures:** Participants propose strategic and technical follow-up actions to limit impact and resume operations.
4. **Awareness and Prevention:** A technical quiz challenges players to reflect on real-world attack vectors and mitigation measures.
5. **Stakeholder Reflection:** Teams assume the roles of affected departments (e.g., HR, Finance, Management) and evaluate the scenario from their perspective.

Each round builds on the results of the previous phase, encouraging cumulative learning. The design incorporates both cooperative and competitive elements through point-based scoring and structured group roles.

### 4.3 Role Design and Group Dynamics

The game is designed for groups of 6–10 participants, divided into mixed teams consisting of two primary roles: operational employees and management representatives. This dual-role system enables perspective taking across functional hierarchies and reflects real-world ERP use cases.

Operational players focus on technical implications, such as failed transactions or missing purchase orders, while management roles address business continuity, stakeholder communication, and regulatory concerns. Throughout the game, players are encouraged to coordinate actions and justify decisions based on role responsibilities.

### 4.4 Game Materials and Facilitation

Physical implementation includes the following.

- A printed game board visualizing the round progression (see Fig. 2).
- Scenario and role description cards.
- Event and response cards, some introducing disruptive “surprise” scenarios.
- Quiz sheets based on the BSI guidelines and attack typologies.
- A point tracking mechanism for feedback and gamification.

A trained facilitator moderates the session, introduces round content, provides optional hints, and awards points based on correctness, creativity, and collaboration. Additional tools such as mind maps and help cards assist less experienced players in identifying threats and appropriate responses.

### 4.5 Iterative Refinement and Adaptability

Between version 1 and version 2 of the game, there was one key improvement made based on participant feedback: the point distribution system was adjusted to reward early rounds more evenly and to encourage consistent engagement.

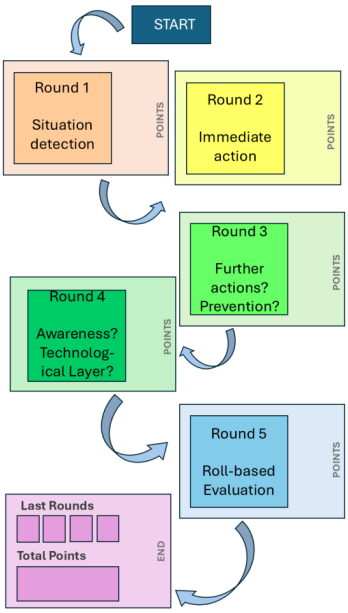


**Fig. 2.** The board of *ERP-Systems in need*

During the second iteration, there was some feedback, that will lead to some major changes in the next iteration to follow: the quiz questions in round four will be simplified and supplemented with support cards to accommodate nontechnical participants. Lastly, the visual design of the materials will be enhanced by color-coded laminated cards for improved usability.

The modular structure of the game allows future expansions and the training of other ERP related topics like cloud compromise or third-party access breaches. The game is easily adaptable for both in-person and potential digital formats as described for the digital version of *A Question of Security* [26].

### 4.6 Pedagogical Considerations

The design decisions were guided by the principles of experiential learning and gamification. By simulating a time-sensitive multirole incident, the game promotes participation, decision-making, and knowledge transfer. Reflection phases at the end of each round encourage metacognitive processing and reinforce key concepts.

Through tentative action and structured facilitation, *ERP-Systems in Need* provides a low-risk, yet realistic environment to explore complex challenges in cybersecurity and organizational resilience.

## 5 Implementation and Playtesting

The serious game *ERP-Systems in Need* was implemented and evaluated through two playtesting sessions with students from the University of the Bundeswehr München. The goal was to assess the usability, relevance and impact of the game on cybersecurity awareness among participants of varying backgrounds.

### 5.1 Participants and Setup

The first group consisted of nine students from the Information Systems. Most had prior experience with ERP systems and basic cybersecurity knowledge. The second group included eight participants from social and political sciences with limited technical experience but a strong interest in digital security issues. This cross-disciplinary mix allowed for a comparative assessment of how diverse users interact with and benefit from the game.

The sessions were held in a classroom setting with printed game boards, cards, pens, and a time keeping tool. The participants were split into teams, each assuming one of two primary roles: operational employee or strategic manager. The facilitator (game master) explained the rules, introduced the scenarios, moderated the game play, and encouraged reflection throughout the session.

Each session followed the full five-round structure:

1. Identification of a security incident
2. Immediate containment strategies
3. Strategic and technical response measures
4. Awareness through quiz-based learning
5. Role-based stakeholder evaluation

The first group demonstrated fast adoption of technical concepts, but initially underappreciated the strategic decisions required at the management level. The facilitator's guidance helped bridge this gap. The second group needed more time to engage with the technical vocabulary and threat models but showed a high degree of collaboration and creativity once the core mechanics were understood.

### 5.2 Observations

Playtesting led to multiple refinements. Participants in both groups provided feedback via structured Likert scale questionnaires and open-ended comments. Based on this, improvements were implemented like a weighted point system to balance early and late game influence. Color-coded and laminated cards were introduced to improve clarity and usability, as well as optional support cards for players unfamiliar with cybersecurity terminology. Regarding the quiz, difficulty adjustments were made to adapt to the group experience.

The duration of the game was averaged 90 to 100 minutes, including feedback sessions. The sessions confirmed that the game successfully promoted cross-role

understanding, encouraged realistic incident thinking, and highlighted the complexity of ERP security incidents. Participants reported a greater confidence in identifying and responding to cyberattacks within critical business systems.

These findings validate the potential of the game as a flexible and engaging tool for cybersecurity training in both academic and professional contexts.

## 6 Evaluation Results

| Question | It. 1 (N=9) | It. 2 (N=8) |
|---|---|---|
| How did you like the game? | 4.78 | 4.75 |
| Did the game meet your expectations? | 4.44 | 4.63 |
| Were you satisfied with the transported information? | 4.78 | 4.88 |
| Did you enjoy the game design? | 4.11 | 4.75 |
| Were you satisfied with the Game Master? | 4.89 | 4.88 |
| Did you enjoy the technological focus? | 4.44 | 4.00 |
| Would you like to see further serious games like the given one? | 3.89 | 4.88 |

**Table 1.** Survey results of *ERP-Systems in need* on a 5-point Likert scale (means).

Two play testing sessions were conducted with students from the University of the Bundeswehr Munich to evaluate the game. Quantitative feedback was collected using a 5-point Likert scale from -2 (very negative) to +2 (very positive). The results were transformed using a 5-point Likert scale from 1 to 5 to make them comparable to the results of the serious game *A Question of Security* that will be discussed in this section. The results showed high satisfaction: 7 of 9 participants rated the overall experience of the game as'very good' and all agreed that the scenario improved their awareness of cybersecurity. Some confusion arose in the first round with respect to player roles, but this was resolved through facilitator guidance. Although game design received slightly mixed feedback – attributed to early-stage prototyping – facilitation and content clarity were highly rated.

The second group included eight students with limited technical knowledge. Their interest in ERP systems was strong and they welcomed the serious game format as a new learning experience. Most of the participants rated the game positively, although the technical quiz in round four proved challenging. Feedback suggested that the technological focus should be simplified or more gradually introduced for non-technical audiences. Despite this, the group found the game engaging and valuable. Both groups expressed interest in seeing the further development of serious games for cybersecurity training. The session durations were 82 and 101 minutes, respectively, exceeding the planned time of 60 minutes due to active discussions and clarifications.

| Question | N | Min. | Max. | Mean |
|---|---|---|---|---|
| How would you rate your knowledge of IT security? | 85 | 1 | 5 | 3,78 |
| How much fun did you have with this serious game? | 85 | 3 | 5 | 4,50 |
| The serious game has increased my awareness of IT security. | 84 | 1 | 5 | 3,58 |
| The serious game taught me something new about the correct behavior during a ransomware incident. | 85 | 1 | 5 | 3,67 |
| I believe that by participating in the serious game, I will be able to behave appropriately in the event of a ransomware attack in the future. | 83 | 3 | 5 | 4,30 |
| How suitable do you think the serious game is for learning more about how to deal with ransomware incidents? (personally) | 84 | 2 | 5 | 4,40 |
| How suitable do you think the serious game is for learning more about how to deal with ransomware incidents? (your organization) | 83 | 2 | 5 | 4,24 |

**Table 2.** Selected results of the questionnaires from *A Question of Security*

As explained, *ERP-Systems in Need* is based on the serious game *A Question of Security*. It has largely adopted the mechanics of the game and developed a new scenario for it. Although there are differences in terms of sample size (ERP n=17, Security n=85), it is worth taking a brief comparative look at the two serious games, because although different, the scenarios have the fact in common that the user cannot do a lot on their own in case of an incident but needs help from experts. Although an attack on an ERP system has a more probable bigger impact on a business than a single compromised mobile device, the things users can do in both cases are basically the same: they can coordinate, organize, and communicate. As the surveys were based on different questionnaires, the results were clustered thematically. Both games scored highly on player experience (ERP: 4.76; Security: 4.50), which makes it a good tool for awareness campaigns and a promising base for more scenarios to be developed. The most noticeable difference appeared in the perceived learning content, where the ERP game reached 4.83 compared to 3.67 for the security game. There may be several reasons for this result. Firstly, ERP security has already been shown to be an issue that is still underestimated in terms of importance. There may be several reasons for this result. Firstly, ERP security has already been shown to be an issue that is still underestimated in terms of importance. In other words, even regular users can still learn a lot of new things here, while IT security awareness is already widely discussed, whether at work or in emails from your own bank or other service providers, for example. Secondly, it is important to consider the target group of players when interpreting the results. The results of the security game have shown a relatively high overall knowledge of IT security.

Observations during the games showed that the experts gain less new factual knowledge but are able to rethink their own processes or engage more with the user's perspective when the serious game is played in mixed groups. The question "Would you like to see more serious games like the given one?" from the ERP game is comparable to the question from the security game questionnaire as to whether players would recommend the game to others in terms of a positive overall assessment and acceptance. In the second iteration of the ERP game, all 8 players agreed very strongly or strongly, in iteration 1, only one player disagreed. 82 of 85 respondents to the security game would also recommend the serious game to others.

## 7 Discussion

The evaluation results of the serious game *ERP-Systems in Need* show its potential as an effective training tool for ERP-specific cybersecurity awareness. The dual-role setup (employee and management) appears valuable for promoting perspective taking and fostering discussion across organizational levels. Both technical and non-technical participants showed increased confidence in identifying threats and responding to incidents, indicating the accessibility and relevance of the game.

However, some limitations must be acknowledged. The game was tested exclusively in an academic environment, which may not fully reflect the pressure, complexity, or accountability present in corporate settings. The sessions were also facilitated by a knowledgeable moderator, which may not always be feasible in practical deployments. Furthermore, the game requires group and time coordination, which may be a barrier in fast-paced enterprise contexts.

The participants noted that the structure of the game encouraged collaboration, strategic thinking, and communication. In particular, the scenario-based progression and the stakeholder reflection of round five were praised for deepening the understanding. However, some players, especially those with less technical background, found the quiz in round four challenging, suggesting the need for more flexible and adaptive content delivery.

These findings highlight two key design considerations for future iterations: first, balancing technical depth with clarity, and second, enabling scalable facilitation through modular, digital, or self-guided formats. Furthermore, integration of resource constraints, time pressure, or branching narratives could more realistically simulate crisis dynamics and decision fatigue, enhancing transferability to workplace scenarios.

In general, the game successfully translates abstract risks into actionable learning, supports role-based participation, and stimulates critical reflection - the key ingredients for meaningful awareness training in ERP cybersecurity.

## 8 Conclusion and Future Work

This paper presented the design, implementation and evaluation of the serious game *ERP-Systems in Need*, which aims to raise awareness of cybersecurity in ERP environments through a role-based scenario-driven serious game. Building on the established game framework of *A Question of Security*, the extended version introduced a scenario that allowed participants to explore the security challenges of the ERP from both the operational and managerial perspectives.

The game was evaluated in two academic playtesting sessions that included participants with technical and non-technical backgrounds. The results indicate that the format is well suited to engage learners, foster collaboration, and support knowledge retention. The combination of progressive rounds, structured facilitation, and real-world threat scenarios proved effective in illustrating the complexity of ERP-specific incidents.

However, the findings also highlight several opportunities for further development. First, the game requires broader validation beyond academic settings. Future studies should assess its applicability and effectiveness in corporate environments, where ERP systems are mission critical and user responsibilities vary widely.

Second, the integration of an adaptive difficulty model is a promising enhancement. By adjusting the technical complexity, the pressure of decisions, and the information flow according to the level of experience of the players, the game can better support heterogeneous learning groups. This could include time-sensitive decision-making elements, resource constraints (e.g. limited staff or IT capacity), and dynamic scenario branches based on player actions.

Third, the role system can be extended to reflect more nuanced organizational structures. Additional roles, such as IT forensics, data protection officers, C-level executives, or legal advisors, could enrich the game and promote deeper reflection on real-world interdependencies and decision trade-offs.

Together, these future directions aim to increase the realism, scalability, and educational impact of the game. A digital implementation may further support hybrid delivery formats and facilitate automated feedback. Ultimately, *ERP-Systems in Need* seek to serve as a flexible training platform that empowers organizations to strengthen their security culture through collaborative, experiential learning.

**Acknowledgments.** This work originates from CONTAIN and the LIONS research projects. We acknowledge funding for CONTAIN by the Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) (grant number 13N16581-13N16587) as part of the SIFO program. LIONS is funded by dtec.bw — Digitalization and Technology Research Center of the Bundeswehr, which we gratefully acknowledge. dtec.bw is funded by the European Union — NextGenerationEU.

## References


1. Almås, H., Giæver, F.: The emergence of collaboration in serious games. an exploratory study. International Journal of Serious Games **11**(3), 89–108 (2024)
2. Beranič, T., Heričko, M.: The impact of serious games in economic and business education: A case of erp business simulation. Sustainability **14**(2), 683 (2022)
3. Bundesamt für Sicherheit in der Informationstechnik: APP.4.2 SAP-ERP-System (2023), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_4_2_SAP_ERP_System_Edition_2023.pdf
4. Bundesamt für Sicherheit in der Informationstechnik: Umsetzungshinweise zum Baustein APP.4.2 SAP-ERP-System (2023), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2022/Umsetzungshinweis_zum_Baustein_APP_4_2_SAP_ERP_System.pdf
5. Clare Duffy: OpenAI CEO Sam Altman warns of an AI 'fraud crisis' (2025), https://edition.cnn.com/2025/07/22/tech/openai-sam-altman-fraud-crisis
6. Conapi GmbH: Case Study: ERP API Security Breach Costs Distributor €1.8M (2025), https://conapi.at/erp-api-security-breach-case-study/
7. Djaouti, D., Alvarez, J., Jessel, J.P.: Classifying serious games: the g/p/s model. In: Handbook of research on improving learning and motivation through educational games: Multidisciplinary approaches, pp. 118–136. IGI global (2011)
8. Gangapatnam, K.: Securing the digital core: Cybersecurity challenges and strategies in sap erp systems. Journal of Computer Science and Technology Studies **7**(3), 270–276 (2025)
9. Greiner, M., Strussenberg, J., Seiler, A., Hofbauer, S., Schuster, M., Stano, D., Fahrnberger, G., Schauer, S., Lechner, U.: Scared? prepared? toward a ransomware incident response scenario. In: International Conference on Innovations for Community Services. pp. 289–320. Springer (2024)
10. Hamari, J., Shernoff, D.J., Rowe, E., Coller, B., Asbell-Clarke, J., Edwards, T.: Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. Computers in Human Behavior **54**, 170–179 (2016)
11. Heather Chen and Kathleen Magramo: Finance worker pays out $25 million after video call with deepfake 'chief financial officer' (2024), https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
12. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS quarterly pp. 75–105 (2004)
13. Hofstede, G.J., De Caluwé, L., Peters, V.: Why simulation games work-in search of the active substance: A synthesis. Simulation & Gaming **41**(6), 824–843 (2010)
14. JP Perez-Etchegoyen: SAP Security Notes & CVEs 2025: Analysis & Threats (2025), https://onapsis.com/blog/critical-sap-security-notes-cves-2025/
15. Kerres, M., Bormann, M., Vervenne, M.: Didaktische Konzeption von Serious Games: Zur Verknüpfung von Spiel- und Lernangeboten. MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung pp. 1–16 (2009)
16. Lameras, P., Arnab, S., Dunwell, I., Stewart, C., Clarke, S., Petridis, P.: Essential features of serious games design in higher education: Linking learning attributes to game mechanics. British journal of educational technology **48**(4), 972–994 (2017)
17. Lechner, U., Dännart, S., Rieb, A., Rudel, S.: Case Kritis-Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Logos Verlag Berlin (2018)

18. Legner, C., Estier, T., Avdiji, H., Boillat, T.: Designing capstone courses in management education: Knowledge activation and integration using an erp-based simulation game. In: Proceedings of the International Conference on Information Systems 2013 (ICIS 2013) (2013)
19. NIST: CVE-2025-31324 Detail (2025), https://nvd.nist.gov/vuln/detail/CVE-2025-31324
20. Ntoa, S., Ntagianta, A., Flores, F., Kolek, L., Petrova, A., Apostolakis, K.C., Stamou, S., Margetis, G., Stephanidis, C.: Serious games beyond entertainment and learning: An evaluation methodology for assessing awareness raising, empathy, and social change. In: International Conference on Human-Computer Interaction. pp. 141–164. Springer (2024)
21. Octavio, M.F.R., et al.: New learning method with erp business simulation games: What can we learn? user perception. Journal of Contemporary Accounting (2024)
22. Onapsis: 46% of Enterprises Experience Four or More Ransomware Attacks in a Single Year, Affecting ERP Applications and Systems 89% of the Time (2024), https://onapsis.com/press-releases/new-onapsis-ransomware-research/
23. Paul Laudanski: SAP Security Breach Cited as a Major Factor in Company's Bankruptcy (2025), https://onapsis.com/blog/sap-security-breach-cited-in-companys-bankruptcy/
24. Ravyse, W.S., Seugnet Blignaut, A., Leendertz, V.e.a.: Success factors for serious games to enhance learning: a systematic review. Virtual Reality **21**, 31–58 (2017)
25. Serrano-Laguna, Á., Martínez-Ortiz, I., Haag, J., Regan, D., Johnson, A., Fernández-Manjón, B.: Applying standards to systematize learning analytics in serious games. Computer Standards & Interfaces **50**, 116–123 (2017)
26. Strussenberg, J., Seidenfad, K., Greiner, M.: From paper to pixel: The digitalization. In: Innovations for Community Services: 25th International Conference, I4CS 2025, Munich, Germany, June 11–13, 2025, Proceedings. vol. 2513, p. 307. Springer Nature (2025)
27. Tritscher, J., Krause, A., Schlör, D., Gwinner, F., Von Mammen, S., Hotho, A.: A financial game with opportunities for fraud. In: 2021 IEEE Conference on Games (CoG). pp. 1–5. IEEE (2021)