Crisis in Syndstad: A Serious Game for Post-Incident Investigation Training

Richard McEvoy and Stewart Kowalski
NTNU, Teknologiveien 22, 2815 Gjøvik, Norway

Abstract

Crisis in Syndstad is a serious game designed to enhance post-incident investigation training in cybersecurity by integrating both technical and interpersonal skills. The game immerses players in a simulated crisis, challenging them to apply empathetic communication with diverse stakeholders in contrast to analytical investigative techniques. By contrasting logical deduction with empathetic engagement, the study explores how soft skills can improve information gathering, collaboration, and understanding in high-pressure environments. This approach advocates for a shift in cybersecurity education, emphasizing the value of trust, negotiation, and emotional intelligence in analyzing and preventing socio-technical failures over purely analytical approaches.

Keywords
CDX, empathy, sociotechnical, investigation, incident, serious games

1.Introduction

Cybersecurity incident response has traditionally been rooted in a logic-driven, systems-thinking approach that prioritizes technical analysis and structured problem-solving over human and social aspects. While effective in identifying vulnerabilities and mitigating threats, this methodology often overlooks the critical interpersonal and psychological dimensions of security investigations. In particular, it neglects the requirement to understand incidents from the point of view of the individuals caught up in them – something that has been seen as key to understanding similar crises in health and safety engineering (which we regard as a superset of cyber security engineering) particularly in the work of Reason and Dekker, who emphasize latent conditions and second-victim dynamics[1, 2].Recent research in cybersecurity education and crisis communication suggests that technical expertise alone is insufficient in high-pressure scenarios where stakeholder coordination, trust, and collaboration are essential[3]. This paper argues that security narratives must evolve—not only from a technical to a sociotechnical perspective but, as a corollary, from one emphasizing forensic analysis, deduction and fault identification to one centred on interpersonal negotiation and empathetic communication.

The necessity of integrating soft skills into cybersecurity training is underscored by studies such as Maennel et al. [4], which highlight the importance of emotional, social, and cognitive aspects in Cyber Defence Exercises (CDX). Psychological safety and multidisciplinary education are key factors in developing security professionals who can navigate complex crisis environments effectively. Similarly, [5] emphasize the role of active listening, empathy, and rapport-building in crisis negotiation, demonstrating that influence and behavioural change are contingent on trust-based interactions

The 11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25)
,September 17-18, 2025, Skopje, North Macedonia

EMAIL: thomarm@ntnu.no (Richard McEvoy); stewart.kowalski@ntnu.no (Stewart Kowalski)
ORCID: 0000-0001-7322-4257 (Richard McEvoy); 0000-0003-3601-8387 (Stewart Kowalski)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2025-12-20

rather than adversarial confrontation. This approach has been popularised by Chris Voss under the label Tactical Empathy© [6].

This shift towards socio-technical security analysis aligns with frameworks like Soft Systems Methodology [7] and Root Cause Analysis for socio-technical failures [8], both of which advocate holistic approaches that consider organizational behaviours and human factors alongside technical vulnerabilities. Furthermore, Mayer et al. [9] provide a foundational model for understanding organizational trust, distinguishing ability-based credibility from the longer-term evolution of trust through demonstrated integrity and benevolence. The dynamics of trust-building are particularly relevant in post-incident cybersecurity investigations, where punitive responses often undermine cooperation and engagement, as evidenced by Renaud et al. [10] in their critique of shame-based security cultures. Beyond this, they foreshorten the analysis of incidents and fail to take account of the requirement to analyse the incident "as it occurred" and not from the point of view of "20/20 hindsight"[2].

Drawing on these principles, this paper presents *Crisis in Syndstad*, a serious game designed to train cybersecurity professionals in post-incident investigation strategies comparing collaboration and empathetic understanding with logical analysis or blame assignment. By contrasting two investigative approaches—one based on logic-driven interrogation and the other on Tactical Empathy© —the game helps students examine how trust-building and interpersonal engagement can enhance security analysis. This approach to cybersecurity pedagogy seeks to foster professionals who not only diagnose technical failures but who can also navigate stakeholder dynamics to elicit critical information and drive meaningful incident resolution.

In this evolving security landscape, cybersecurity practitioners must become skilled communicators, negotiators, and trust-builders. As Sasse et al. [11] assert, security systems often fail not due to technical flaws but because of their misalignment with human behaviours and organizational processes. This paper proposes that post-incident investigation should no longer treat human elements as secondary factors but instead embrace them as central components of cybersecurity resilience. This means rejecting any concept that technology or processes are perfect and hence only the human can be at fault. Instead, by empathetic questioning, analysts come to understand why - what are "poor" decisions in hindsight - were made in the first place, and hence appropriately distributing causality across the sociotechnical structures in the organization and beyond.

2. Literature Review: Integrating Soft Skills and Narrative-Driven Learning in Cybersecurity Education

In this section, we review the literature on cyber security incident investigation and the role of sociotechnical skills and empathetic approaches to improving investigation outcomes. We highlight the role serious gaming plays in educating individuals in these skills.

2.1. Traditional Cybersecurity Narratives: The Limits of Systems Thinking and Logical Reasoning

Cybersecurity education has historically centred on technical expertise and systems thinking, emphasizing structured methodologies for identifying vulnerabilities, mitigating risks, and conducting post-incident investigations – for example, [12]. This traditional approach assumes that security failures stem primarily from technical weaknesses rather than social or psychological dynamics. However, researchers have increasingly critiqued this technical perspective for neglecting the human and organizational factors essential to incident response and to approaches to IT management in general [7, 13, 14].

Root Cause Analysis (RCA), adapted for socio-technical security incidents[8], highlights how traditional security investigations often overlook behavioural and emotional dimensions. Similarly, research reveals that employees frequently develop informal security practices (known as “shadow security”) when official protocols fail to align with workplace realities [15]. These findings suggest that security breaches are rarely attributable solely to technical misconfigurations but also include gaps in communication, trust, and organizational alignment. This can happen at the user interface or during the development and implementation processes.

Furthermore, failures need not simply be attributed to the operational level, but can arise from incomplete feedback loops at higher levels of the organisation, pointing to systemic shortcomings in the governance, management, design and implementation of systems[16]. Post-incident investigation is, therefore, not just about capturing weaknesses in terms of technical or user failure, but requires an investigative process which encompasses higher levels of the organisation and the social, economic and political context in which it operates.

2.2. The Role of Emotional Intelligence in Cybersecurity Incident Response

Recent studies advocate for a more people-centred approach to cybersecurity investigations, incorporating people skills, negotiation techniques, and trust-building strategies. For instance, Maennel et al. [4] propose a multidimensional Cyber Defence Exercise (CDX) model that integrates emotional, social, and cognitive aspects into cybersecurity training. By fostering psychological safety and intrinsic motivation, such exercises enhance learning outcomes beyond traditional technical drills.

Trust is a critical component of effective security responses, particularly in high-pressure crisis scenarios. Mayer, Davis, and Schoorman [9] conceptualize organizational trust as a dynamic interplay between ability, benevolence, and integrity, arguing that the willingness to be vulnerable to others' actions is foundational to collaborative problem-solving. This perspective aligns with research into cybersecurity investigations, where punitive blame cultures often obstruct meaningful information exchange[10]. A shift toward a "Just Culture" framework—where mistakes are analysed constructively rather than penalized—is necessary to foster more effective post-incident assessments. Furthermore, experience in the health and safety industry strongly suggests that the best way to understand an incident is to take the point of view of the individual in that incident, not with the benefit of hindsight, but rather seeking to understand their behaviour in the exact context of the when and where the incident occurred. We argue that this requires a practical approach to empathizing with the individual[1].

2.3. Crisis Negotiation and Tactical Empathy in Security Investigations

Studies on crisis negotiation techniques provide valuable insights for cybersecurity professionals seeking to improve post-incident investigative processes. Vecchi, Van Hasselt, and Romano[5] identify active listening, empathy, and rapport-building as core skills that facilitate de-escalation and influence in high-stakes scenarios. These techniques are commonly employed in hostage negotiations but have direct relevance to cybersecurity investigations, where adversarial confrontations can impede cooperation with the investigation.

Crisis negotiation research underscores the importance of emotional intelligence, particularly in settings where stakeholders may be defensive, distrustful, or unwilling to disclose critical information[17]. We argue that cyber security professionals trained in Tactical Empathy©—an approach that emphasizes understanding the psychological states and motivations of stakeholders—

would be more effective at eliciting intelligence and navigating complex security crises. This is not new in the sense that these techniques are recognisably part of what is labelled “consultancy skills”[18] but the difference is that these skills are provably trainable and have been tested in high stakes scenarios.

For example, the victim of a phishing attack on a corporation can be blamed twice – first, for being victim to the phishing attack, and second, for being the “cause” of the organization’s cybersecurity crisis. This double jeopardy makes it too easy to both foreshorten the investigation and to silence individuals who could otherwise usefully speak up, either forestalling the crisis or helping to comprehend its causes to improve processes in future. A wider conversation would cover how aware the individual was, what training they had received, how effective that training was, what other mechanisms (e.g., end point protection technologies) were employed and how effectively they might be in alerting the individual – and so forth!

Empathy should not be mistaken for compassion, or agreement. A Machiavellian individual can be empathic, but not motivated to respond to their understanding of others in a compassionate way[19]. Empathetic understanding, in this instance, should therefore be understood as a specific and pragmatic socio-communicative skill in establishing with another individual that their point of view has been clearly understood, both intellectually and emotionally. Nonetheless, even in individuals that might be perceived to be ruthless, demonstrating that their point of view is understood can be powerfully transformative in terms of future relations with them[5].

2.4. Serious Gaming as a Pedagogical Tool for Cybersecurity Training

Serious games have emerged as powerful tools for experiential learning in cybersecurity education[20]. Unlike conventional training methodologies that rely on theoretical instruction, serious gaming immerses participants in interactive simulations that mimic real-world challenges. These exercises foster active engagement, strategic thinking, and adaptability under pressure[21].

Recent systematic reviews affirm that serious games enhance cybersecurity awareness and retention by leveraging narrative immersion, feedback loops, and scenario-based problem solving. Moumouh et al. [22] highlight that serious games improve privacy and security knowledge among professionals, especially when tailored to specific sectors such as healthcare and critical infrastructure[7]. These games often incorporate gamified mechanics—such as role assignment, time pressure, and branching decision trees—that simulate adversarial conditions and ethical dilemmas.

Hill et al.[23] compare twenty serious games across cybersecurity domains, noting that effective game design aligns with recognized knowledge units (KUs) and instructional goals[8]. Their rubric emphasizes the importance of interface quality, scenario realism, and cognitive scaffolding in shaping learner outcomes.

The *Crisis in Syndstad* serious game aligns with this approach, integrating Tactical Empathy© principles into cybersecurity education. Players navigate ambiguous crisis scenarios where interpersonal trust and strategic negotiation can shape the success of post-incident investigations. This mirrors findings from the literature that underscore the role of emotional intelligence, psychological safety, and social cognition in cyber crisis response [5, 24].

At the same time, the role of logic and data analysis is explored as a rival strategy – to allow a comparison of the two methods, leading to a reflective discussion of when and how they should be used.

Finally, serious games serve as epistemic laboratories—spaces where learners can repeatedly rehearse complex decision-making under uncertainty, test hypotheses about adversarial behaviour, and reflect on the ethical dimensions of cyber defence. When embedded within a broader curriculum, they offer recursive opportunities for feedback, adaptation, and ritualized learning.

2.5. Reframing Cybersecurity Pedagogy: Toward a Narrative-Driven, Empathy Based Model

The literature suggests that cybersecurity education must move beyond traditional technical and socio-technical methodologies to embrace narrative-driven learning models. Sasse et al.[11] argue that security systems often fail due to misalignment with human behaviours rather than technological deficiencies. By incorporating insights from crisis negotiation research, trust-building frameworks, and serious gaming methodologies, cybersecurity educators can better equip professionals with the people skills necessary for effective incident response.

This paper builds on these principles by presenting *Crisis in Syndstad* as a serious game designed to shift security narratives—away from rigid logical assessment and toward collaborative, trust-based problem-solving. By embedding Tactical Empathy© into the investigative process, security professionals can enhance information flow, reduce conflict, and improve overall security resilience.

3. Research Motivation

Cybersecurity incident investigations remain dominated by logic-driven, technically structured methodologies that often obscure the human realities at play. Even sociotechnical approaches—while broader in scope—frequently fail to account for the emotional, psychological, and interpersonal complexities that shape post-incident dynamics and focus on analytical approaches to dealing with systemic social issues. In high-stakes scenarios involving human error, insider threats, and organizational breakdowns, investigators must navigate conflicting narratives, emotional defensiveness, and trust deficits that resist purely analytical treatment.

This research is motivated by the persistent gap between procedural analysis and empathetic engagement. Emotional responses such as shame, fear, and frustration can obstruct information flow and reinforce adversarial cultures, especially when investigations default to blame attribution. By contrast, crisis negotiation literature demonstrates that empathy, active listening, and rapport-building foster transparency and collaboration—skills that are critically underutilized in cybersecurity pedagogy.

Crisis in Syndstad emerges from this tension, offering a serious game framework that reimagines post-incident investigation as a socio-emotional process. It seeks to train cybersecurity professionals not only in technical diagnosis but in trust-building, stakeholder engagement, and the dignified handling of human complexity.

4. Problem Definition: The Limits of Logic in Cybersecurity Incident Investigation

4.1. The Dominance of Technical and Logic-Driven Approaches in Cybersecurity

Traditional cybersecurity methodologies have overwhelmingly prioritized structured logical reasoning and a technical focus to diagnose vulnerabilities, manage risks, and investigate incidents – for example, [12]. But even where approaches focus on sociotechnical analysis, widening the investigation beyond technical issues to embrace organizational factors such as [8, 14, 25], methodologies often fail to account for the emotional and psychological complexities that influence post-incident investigative processes that make a logical and systematic investigation difficult.

Cybersecurity incidents—particularly those involving human error, insider threats, and organizational failures—require more than mere technical, or even sociotechnical analysis. Decisionmakers must navigate conflicting narratives, engage with resistant stakeholders, and foster trust within crisis-stricken organizations. A purely logic-driven perspective, however, often frames investigations as adversarial processes, focusing on fault-finding rather than collaborative problem-solving. The methodology employed can also foreshorten the investigation under the assumption that the analysis approach used is sufficient, and ignoring its documented limitations[1].

4.2. The Sociotechnical Shift: Progress but Persistent Gaps

The adoption of sociotechnical methodologies has broadened cybersecurity investigations by integrating human and organizational factors into traditional analyses[7]. This shift acknowledges that security incidents rarely emerge from technical failures alone; rather, they arise from the interplay between technology, policy, and human behaviour. However, even within sociotechnical approaches, investigations frequently remain rigidly structured, relying on logical analysis and procedural frameworks.

The problem with this is that the human dimension, the need to empathize with the players in the situation, to understand the world from their perspective, which has been recognized in the health and safety world [1], is lost both in terms of the analysis itself and its investigation, and the barriers which human emotional responses put up to analytical approaches due to both blame shifting behaviours[26] and cognitive overload[24] are ignored in cybersecurity crisis handling and investigations.

As an example, research into “shadow security” behaviours[15] highlights how employees often bypass official security protocols due to usability constraints. Yet, instead of addressing underlying usability challenges, organizations frequently respond with compliance enforcement, reinforcing an adversarial culture and losing the opportunity to design away from a dysfunctional environment which inevitably results in continual and repeated future divergences from policy and process. Similarly, cybersecurity education often emphasizes rational analysis and engineering based thinking without sufficiently integrating psychological and social dynamics [21].

4.3. The Role of Emotion in Crisis Investigation

Security incidents provoke a range of emotional responses, from rage and disgust to fear and defensiveness to frustration and distrust. The failure to incorporate emotional intelligence into investigative processes can lead to communication breakdowns and obstruct the flow of information. Shame, in particular, has been identified as a counterproductive force in cybersecurity[10]. When incident response relies on punitive measures, or blame attribution, individuals are less likely to disclose critical information, instead engaging in avoidance behaviours that exacerbate security risks.

In contrast, studies on crisis negotiation emphasize the value of empathetic engagement, rapport-building, and trust-based communication [5]. These skills, commonly employed in hostage negotiations, are equally relevant in post-incident cybersecurity investigations. When investigators use pro-active listening and demonstrate empathy, they foster a collaborative environment that encourages transparency and constructive dialogue.

5. Changing the Narrative: Creating A Safe Space for Collaboration in Addressing the Causes of Incidents

Our approach to resolving this problem is to shift the thinking of professionals and students of cyber security, not to neglecting logical and technical approaches, but to enhancing their sociotechnical understanding and to employing empathy as a tool for both understanding and negotiating crisis situations and their investigation.

5.1. Psychological Safety in Cyber Defence Exercises

Building on the role of emotion in security investigations, Maennel et al. [4]propose a multidimensional Cyber Defence Exercise (CDX) model that incorporates psychological safety, intrinsic motivation, and interpersonal engagement. Their findings suggest that individuals perform more effectively in crisis scenarios when they feel psychologically safe—free from excessive scrutiny or punitive consequences. This principle aligns with the broader movement toward a "Just Culture" [27] security framework, where incident investigations focus on learning and systemic improvement rather than individual blame.

By fostering an investigative approach rooted in psychological safety and trust-building, cybersecurity professionals can move beyond adversarial methodologies, turning the “just culture” approach into a pragmatic tool. Empathy-based information elicitation, strategic negotiation, and interpersonal engagement should complement technical analysis to create a holistic framework for post-incident security response.

5.2. Toward an Empathy-Driven Security Narrative

Cybersecurity education must likewise evolve to integrate emotional intelligence, trust-building, and negotiation techniques as core competencies in post-incident investigation. A rigid logic-based investigative model limits the ability of security professionals to navigate the complexities of crisis response. An approach which is based on empathy and on building trust relationships, aiming for collaborative outcomes provides a firmer basis for successful post-incident investigations.

5.3. Reframing Post-Incident Investigation: From Logic to Tactical Empathy

To resolve the limitations of traditional cybersecurity post-incident investigations, this paper advocates for a transformative approach—one that shifts the focus from rigid logic-driven analysis to an empathy-based model. The *Crisis in Syndstad* serious game embodies this paradigm, providing a structured environment where security professionals practice Tactical Empathy© in high-pressure investigative settings. By integrating trust-building and interpersonal engagement into cybersecurity pedagogy, the game challenges conventional blame-centric narratives, fostering collaborative problem-solving and improving crisis resolution outcomes.

5.4. Leveraging Serious Games for Human-Centered Cybersecurity Training

Serious gaming (see Section 2.4) offers an experiential learning framework for cybersecurity professionals to develop critical soft skills necessary for effective post-incident investigations. Role-playing simulations facilitate the application of interpersonal negotiation techniques, active listening strategies, and trust-building methodologies within adversarial security scenarios. Our approach builds on existing research in crisis negotiation and cybersecurity education, drawing from studies on tabletop cyber exercises[21] and crisis resolution methodologies to enhance security training.

6. Crisis in Syndstad: Scenario Design and Gameplay Structure

6.1. Scenario Design

Crisis in Syndstad is a multiplayer serious game designed to simulate the emotional, political, and technical complexities of post-incident investigation. Set in the fictional Norwegian city of Syndstad—recently devastated by unprecedented flooding—the game challenges players to uncover the layered causes behind the crisis. These range from infrastructure fragility and climate-induced weather anomalies to cyber-attacks on SCADA systems and failures in risk communication.

AI (Microsoft Copilot 2025) was used to support the scripting of the game scenarios and the roles of non-Player Characters(NPCs), drawing on real-world incidents which were relevant to the fictional incident we invented. The structure and plotting of the game were original to the authors.

The game scenario extends the investigation beyond the purely technical aspects of a cyber security failure, due to an alleged cyber attack which may have led to failures in the city's water management system resulting in severe flooding with high impact costs.

The players are confronted with a range of possible contributory factors: the severity of the storm, which is a once in a hundred years event; failures to take into account predictions about storm severityand frequency changing due to climate change; potential over-development of the city in advance of the capacity of its water management system – due to pressure from business and tourist sectors as well as families seeking new homes; the nature of the SCADA system with old, but unreliable, pumps on the one hand, and new, but cyber vulnerable, pumps on the other. The game play scenario even hints at corruption in high places. All factors were taken from real-world scenarios – for example, the flooding of Chicago's millionaire district[28], incidents with water management systems potentially caused by cyber attacks[29], and the role of climate change in altering weather patterns[30].

The NPCs include the city mayor, a climate scientist, the head of IT, the head of the risk team, the chief engineer and the town planner – giving the team choices about who to interview in the short period of time allowed by the game. Furthermore, the NPCs as well as explaining and justifying their own actions (based on scripts provided) can also blame the members of the investigation team for their "failures" during the crisis.

Finally, we introduce joker options and wild cards to spice up game play (see section 6.2).

6.2. Gameplay Structure

The gameplay unfolds over multiple rounds, each structured into four distinct phases:

Briefing Phase: Players receive evolving updates, including technical reports, witness statements, and contextual data. These updates reflect real-world uncertainty and information asymmetry, preparing players for the ambiguity inherent in crisis response.

Interrogation Phase: Teams engage with scripted NPCs representing diverse stakeholders—mayors, engineers, urban planners, climate scientists, and IT security leads. These interactions are designed to simulate political defensiveness, blame-shifting, and emotional latency. NPCs may offer justifications, deflections, or partial truths, requiring players to navigate complex interpersonal terrain.

Analysis Phase: Players synthesize the collected data, weighing individual accountability against systemic failure. The phase emphasizes the tension between technical diagnosis and sociotechnical interpretation, inviting players to consider whether the crisis stems from isolated negligence or embedded structural vulnerabilities.

Decision Phase: Using the CATWOE framework (Customers, Actors, Transformation Process, Worldview, Owners, Environmental Constraints), teams assign responsibility—not merely to identify fault, but to explore how worldview, governance, and environmental constraints shape outcomes. The framework scaffolds structured reflection while resisting simplistic blame narratives.

A key gameplay element involves the analysis of a cyber-attack targeting SCADA systems that manage drainage pumps. Players must evaluate whether the attack exploited unpatched vulnerabilities, involved zero-day exploits, or reflected deeper organizational failures in IT governance. This scenario links the fictional crisis to real-world cybersecurity threats, such as the

Oldsmar water treatment incident, and invites players to consider the fragility of cyber-physical systems under stress.

To heighten realism and emotional engagement, players role-play as investigative teams who may themselves be implicated in the crisis. This recursive framing introduces moral tension: players must fairly apportion blame while resisting the instinct to deflect responsibility. NPCs may mirror this defensiveness, creating a dynamic interplay of trust, shame, and strategic disclosure. Additional gameplay stressors include:

Wild Cards: Randomized information drops that may be misleading, irrelevant, or revelatory—simulating the chaos of real-time crisis investigation.

Joker Option: A limited-use whistleblower mechanic that provides anonymous insider information, challenging players to weigh credibility against strategic advantage.

The experimental setup contrasts two investigative paradigms:

- Team *Blue* employs Tactical Empathy©, drawing on FBI negotiation techniques to foster rapport, reduce defensiveness, and enhance information flow.
- Team *Red* uses logic and forensic question, focusing on evidence-based reasoning and adversarial refutation.

By comparing outcomes, the game explores whether soft skills—empathy, listening, and trust-building—can outperform traditional logic-driven inquiry in high-pressure, emotionally charged environments.

Expected learning outcomes include:

- Mastery of structured investigative reasoning.
- Practice in de-escalation and empathetic engagement.
- Critical reflection on the ethics of blame, responsibility, and systemic failure.
- Application of CATWOE as a tool for nuanced accountability.

Ultimately, *Crisis in Syndstad* reframes post-incident investigation not as a fault-finding exercise, but as a collaborative, emotionally intelligent process of truth-seeking and systemic understanding.

6.2. Use of Tools versus Human Input

The support provided by AI to create the game raises a question over whether the game should be administered purely by humans or if artificial intelligence could take over some of the roles. Our own opinion is that the usefulness of AI lies in its ability to generate and alter game scenarios rapidly so that the game can be played several times with fresh problems. However, because the game is about learning to use Tactical Empathy© as opposed to purely relying on logical analysis, it is important that key roles are played by humans who can act naturally and accurately reflect the range of human emotions. This, of course, does not prevent the use of AI for recording and helping with the analysis of game play.

7. Post-Game Analysis: Debriefing and Discussion

Following the gameplay, participants are required to engage in structured post-game analysis and discussions. This involves reflecting on their investigative tactics, assessing the effectiveness of empathetic communication, and comparing the outcomes of different approaches such as logic-based interrogation versus trust-driven negotiation. Participants are encouraged to draw connections to real-world security challenges, integrating insights from crisis negotiation literature and trust-building models to contextualize their reflections and improve their understanding of cybersecurity dynamics.

8. Evaluating the Effectiveness of the Approach

Gameplay will be captured through observation and notetaking, with the support of AI tools (with consent) where appropriate. Participants will also provide qualitative feedback through semi-structured interviews, surveys, and group discussions, capturing their perceptions of trust-building, collaboration, and security decision-making in contrast to using analytical approaches. This feedback will be analysed thematically to identify common patterns and insights.

We will also draw on empirical data collected on the participants' performance during the game. Key metrics will include the accuracy of information gathered, the effectiveness of stakeholder engagement, and the resolution of complex crisis scenarios. These metrics will be quantitatively assessed to measure the impact of the game on investigative proficiency. This will require us to create score sheets for assessing players' progress and also perceptions of players' performances.

A comparative analysis based on the reflections of the participants will be conducted between the Tactical Empathy© approach used by Team Blue and the logical assessment approach used by Team Red. This will involve comparing outcomes such as information elicitation, comprehension of causality, and stakeholder interaction. Participants' experiences with both approaches and their reflection them will be documented and contrasted to help participants evaluate the strengths and weaknesses of each methodology.

Longitudinal studies will be designed to assess the long-term impact of the game on participants' cybersecurity skills. Follow-up assessments will be conducted at multiple intervals post-gameplay to determine the retention and application of empathetic investigative techniques in real-world scenarios. The effectiveness of the *Crisis in Syndstad* game will also be evaluated by in relation to existing cybersecurity training programs. Feedback will be gathered from trainers and participants on how well the game complements traditional training methods and enhances overall learning outcomes.

By adhering to these detailed requirements, the evaluation of the Crisis in Syndstad game will provide comprehensive insights into the utility and impact of empathy-driven investigative approaches in cybersecurity education.

Beyond these approaches, we need to look for a group transformation in how organizations communicate and how they deal with blame. It might be argued that evolutionarily speaking, humans are doomed to act solely in their self-interest (the "selfish gene" trope) but recent research suggests that responses to blame and the establishment of cooperative relations are situationally driven and can be strongly influenced by cultural shifts[31, 32].

9. Discussion, Conclusion and Future Work: Expanding the Security Narrative Through Empathy-Driven Investigations

9.1. Discussion

The *Crisis in Syndstad* game is intended to demonstrate the value of incorporating people skills into an educational exercise in cybersecurity post-incident investigations. By shifting investigative methodologies from rigid logic-driven analyses to an empathy-based framework, participants engaged in collaborative problem-solving that improved information flow, trust-building, and crisis resolution compared to purely logical approaches. The exercise seeks to encourage reflection on the principle that cybersecurity incidents—particularly those involving human factors—require investigative strategies that blend technical expertise with emotional intelligence.

The literature underscores the potential for empathy-driven investigative techniques to enhance cybersecurity training and the importance of adopting an empathetic lens when analysing how crises unfold. Dekker's reframing of human error as a symptom of deeper systemic conditions [1], along with Dekker and Conklin's advocacy for "safety differently"[2], challenges traditional blame-centric paradigms and invites a more compassionate, context-sensitive approach to incident analysis. This is echoed in Covarrubias' emphasis on effective communication as foundational to crisis management in cybersecurity[3], and further supported by Maennel et al.'s multidimensional cyber defence exercises, which foreground emotional, social, and cognitive factors in training design[4].

In the context of the *Crisis in Syndstad* game, these insights suggest that empathy is not merely a pedagogical nicety but a strategic imperative. The game's design must reflect the complexity of human decision-making under pressure, as explored in crisis negotiation literature [5, 6], and integrate systems thinking to capture socio-technical interdependencies [7, 8, 13, 14]. However, to refine and enhance its effectiveness, it is crucial to gather feedback from industry professionals and domain experts. Their lived experience and operational insight will be invaluable in shaping scenario realism [21], calibrating emotional and cognitive load[24], and ensuring the game's alignment with authentic learning outcomes. Such feedback loops will also help mitigate the risk of reinforcing shame-based responses [10, 13, 17], and instead foster trust[9], dignity, and adaptive capability—core values in both cybersecurity pedagogy and behavioural support.

By engaging with experts in cybersecurity, game design, and educational psychology, the development team can ensure that the game meets the highest standards of quality and relevance. Additionally, this collaborative approach will foster a deeper understanding of how empathy-driven methodologies can be integrated into broader cybersecurity curricula.

Our work has general implications for the management in dealing with cyber security. The literature consistently reveals that cybersecurity training, and by extension organizational decision-making, cannot rely solely on logic, analysis, and procedural abstraction[1, 4, 7, 19]. Our extension of this argument foregrounds the necessity of empathetic handling—recognizing that human beings are not deterministic processors, but predictive, emotionally attuned agents shaped by bias, expectation, and affective feedback [3, 10, 24]. This reframing has profound implications for management at all levels.

Managers must move beyond the mechanistic treatment of personnel as "human resources" to a more human-centred ethic of engagement. The human brain is predictive and corrective[33] rather than logical, and does not respond optimally to coercion, shame, or rigid protocol—it thrives in environments of trust, dignity, and adaptive support which underpin good prospective decision making[9, 17, 20, 33]. To put it simply, if an individual expects opprobrium for speaking up about failures or taking responsibility for some aspect of their work which has gone wrong, they will not speak up and the organisation will not learn. Tactical Empathy© applied as a genuine, not manipulative, enabler of communication helps create this kind of supportive framework.

This shift is not far from emerging trends in modern management, which increasingly reject exploitative models in favour of relational stewardship, psychological safety, and embodied empathy[34]. Organizations that embrace this paradigm—treating employees as recursive, emotionally complex agents—will be better equipped to navigate adversarial uncertainty, foster innovation, and enact integrity in practice.

The feedback obtained from these critiques will be meticulously analysed and incorporated into future iterations of the game. This iterative and reflective development process will help in fine-tuning the game mechanics, enhancing the narrative, and aligning the educational objectives with real-world requirements. The goal is to create a robust, engaging, and educational tool that effectively prepares participants for the multifaceted challenges of cybersecurity investigations.

9.2. Limitations

One potential limitation in the purpose of the *Crisis in Syndstad* game lies in its framing of empathy. While the game seeks to cultivate empathy-driven crisis response, it risks reducing empathy to a set of scripted choices rather than modelling it as a dynamic, context-sensitive capability.

Ren et al. [19] highlight the complexity of empathic response, noting its entanglement with neurostructural traits and perceived social risk, which suggests that empathy cannot be reliably taught through static interactions alone. The game goes part way to addressing that but risks making empathy purely about conversational tricks, rather than properly negotiating understanding of the other's viewpoint. Similarly, Lu and Huang's [24] emotion-cognition dual-factor model underscores the need for nuanced emotional calibration in crisis communication, warning against oversimplified pedagogical approaches that fail to engage deeper affective reasoning.

Design-level limitations also emerge in the realism and emotional granularity of the game's scenarios. Maennel et al.[4] emphasize the importance of integrating emotional, social, and cognitive dimensions into cyber defence exercises, arguing that authentic stressors and interpersonal dynamics are essential for effective learning. If the scenarios lack operational fidelity or emotional depth, players may disengage or default to superficial decision-making. Moreover, the absence of robust feedback mechanisms—particularly those that reflect trust dynamics[9] or mitigate shame-based responses [10, 17]—can flatten the learning experience into binary outcomes, undermining the development of adaptive reasoning.

Gameplay itself may be constrained by structural rigidity. Linear progression models, while pedagogically convenient, can inhibit recursive adaptation and emergent strategy—key features of real-world crisis evolution[26] [32]. Static role assignments further limit players' ability to shift between technical, emotional, and strategic viewpoints, reducing the opportunity for cross-domain insight and systems-level reflection [11, 25]. Additionally, without explicit safeguarding protocols, neurodivergent players may struggle to interpret ambiguous cues or navigate social appropriateness, echoing concerns raised by Renaud et al. [10] and AlSabbagh & Kowalski[7] regarding the need for clarity and dignity in behavioural design. Although we would also argue that neurodivergent players would greatly benefit from the social skills which the game seeks to impart and that selected scenarios where players "lost" due to neurodivergent traits could be re-framed as role plays[35] and social stories[36] to address their training needs.

In short, we need to be careful not to make the game overly complex, socially or emotionally overwhelming, or try to dictate the outcome. The aim is to let the players experience the complexities of a real-life incident and to reflect on the different skills which can be brought to bear in its resolution.

Taken together, these limitations suggest that while *Crisis in Syndstad* holds promise as an training tool for imparting empathy as a learned behaviour, its effectiveness depends achieving emotional realism, systemic feedback, and willingness to adapt gameplay structures to the needs of players. In short, the game needs itself to be a living demonstration of Tactical Empathy© in practice.

9.3 Conclusion

Crisis in Syndstad is currently in development as a serious game for helping with post-incident analysis of root causes. As such it represents an opportunity to engage students in recursive investigation techniques to uncover the causal hierarchy behind the occurrence of incidents and to help them comprehend that such causes are not simply technical in nature but arise from socio-technical artefacts of the organisation and the environment in which it is situated.

Our argument in designing the game is that the analysis of cyber security incidents must not simply move from a logical and forensic examination of technical causes to a logical and forensic examination of socio-technical causes, but also employ a methodology which introduces empathetic skills which do more than simply facilitate the analysis process but actually provide a safe psychological space for participants to explore causality and associated problem solving as a joint enterprise, turning a "no blame" culture into a culture of radical responsibility taking[37], promoting joint learning. Although we point out that much of what we are discussing represents what is known about good consultancy skills and is already practised in health and safety management and our approach is simply a well-founded extension of those skills to cybersecurity, based on high-stakes simulations of real world situations[5, 6].

At the current stage, we are seeking both academic and professional feedback on the game design to ensure that the game does indeed facilitate the aims we have. We recognise the potential dangers of trying to enforce learning outcomes, where we need to ensure that the game experience allows students to recognise the strengths and weaknesses of both rational analysis and empathetic knowledge elicitation. We recognise, therefore, that the game itself needs to create a safe place to engage with the problems it creates for the student and that its use should be adaptive, reflective and recursive.

9.4 Future Research

The goal of future research is to focus on incorporating human and social aspects into the design of cybersecurity educational materials (and, consequently, into the design and implementation of cybersecurity systems). Serious games represent one way of achieving these goals and research in this area will focus on refining game play mechanics. There needs to be an emphasis on fostering safe environments to teach post-incident investigation. Game play scenarios need to be sociotechnically rigorous, while game play rules need to create a space which challenges but does not overwhelm.

In parallel, there is a need to design and develop new serious games that model other aspects of cybersecurity management through diverse operational and interpersonal lenses. These games should be conceived not merely as instructional tools, but as structured enactments of complex human behaviour under adversarial conditions—where psychological safety, reflective judgment, and adaptive coordination are treated as core design imperatives.

By narrowing the research agenda to gameplay refinement and targeted invention, the field can move beyond generic gamification toward a principled methodology—one that integrates behavioural nuance, emotional fidelity, and strategic realism into the architecture of cybersecurity education.

Declaration on Generative AI

Any use of generative AI in this manuscript adheres to ethical guidelines for use and acknowledgement of generative AI in academic research. Each author has made a substantial contribution to the work and it has been thoroughly reviewed for accuracy, and they assume full responsibility for the integrity of their contributions [38].

References

1. Dekker, S., *The field guide to understanding'human error'.* 2017: CRC press.
2. Dekker, S. and T. Conklin, *Safety differently.* 2014: CRC Press London.
3. Covarrubias, J.Z.L., *Effective Communication as A Pillar of Cybersecurity: Managing Incidents and Crises in the Digital Era.* Journal of Risk Analysis and Crisis Response, 2025. **15**(34).
4. Maennel, K., et al., *A multidimensional cyber defense exercise: Emphasis on emotional, social, and cognitive aspects.* SAGE Open, 2023. **13**(1): p. 21582440231156367.

5. Vecchi, G.M., V.B. Van Hasselt, and S.J. Romano, *Crisis (hostage) negotiation: Current strategies and issues in high-risk conflict resolution.* Aggression and Violent Behavior, 2005. **10**(5): p. 533-551.
6. Voss, C. and T. Raz, *Never split the difference: Negotiating as if your life depended on it.* 2016: Random House.
7. AlSabbagh, B. and S. Kowalski. *Security from a systems thinking perspective-applying soft systems methodology to the analysis of an information security incident.* in *Proceedings of the 58th annual meeting of the ISSS-2014 United States.* 2014.
8. Ferreira, A., et al. *In Cyber-Space No One Can Hear You S CREAM: A Root Cause Analysis for Socio-Technical Security.* in *International Workshop on Security and Trust Management.* 2015. Springer.
9. Mayer, R.C., J.H. Davis, and F.D. Schoorman, *An integrative model of organizational trust.* Academy of management review, 1995. **20**(3): p. 709-734.
10. Renaud, K., R. Searle, and M. Dupuis. *Shame in cyber security: effective behavior modification tool or counterproductive foil?* in *Proceedings of the 2021 New Security Paradigms Workshop.* 2021.
11. Sasse, M.A., S. Brostoff, and D. Weirich, *Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security.* BT technology journal, 2001. **19**(3): p. 122-131.
12. Huluka, D. and O. Popov. *Root cause analysis of session management and broken authentication vulnerabilities.* in *World Congress on Internet Security (WorldCIS-2012).* 2012. IEEE.
13. Soomro, Z.A., M.H. Shah, and J. Ahmed, *Information security management needs more holistic approach: A literature review.* International Journal of Information Management, 2016. **36**(2): p. 215-225.
14. Salim, H.M., *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks.* 2014, Massachusetts Institute of Technology.
15. Kirlappos, I., S. Parkin, and M.A. Sasse. *Learning from "shadow security".* in *NDSS Workshop on Usable Security.* 2014.
16. Leveson, N.G., *Engineering a safer world: Systems thinking applied to safety.* 2016: The MIT Press.
17. National Cybersecurity Alliance, i.p.w.A.F.W.N. *Don't Blame the Victim: 'Fraud Shame' and Cybersecurity.* 2023; Available from: https://www.staysafeonline.org/articles/don-t-blame-the-victim-fraud-shame-and-cybersecurity.
18. Banai, M. and P. Tulimieri, *Knowledge, skills and personality of the effective business consultant.* Journal of Management Development, 2013. **32**(8): p. 886-900.
19. Ren, H., et al., *"High empathic response but low interest": Machiavellianism and its neurostructural basis relate to perceived risk of social exclusion and workplace deviance.* Journal of Research in Personality, 2024. **113**: p. 104548.
20. Ahmed, A., et al., *How universities teach cybersecurity courses online: a systematic literature review.* Frontiers in Computer Science, 2024. **6**: p. 1499490.
21. Skytterholm, A. and G. Hotvedt. *Criteria for Realistic and Expedient Scenarios for Tabletop Exercises on Cyber Attacks Against Industrial Control Systems in the Petroleum Industry.* in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales.* 2023. Springer.
22. Moumouh, C., et al., *Serious Games to Improve Privacy and Security Knowledge for Professionals: a Systematic Literature Review.* International Journal of Serious Games, 2025. **12**(1): p. 3-24.
23. Hill, W., M. Fanuel, and X. Yuan. *Comparing serious games for cyber security education.* in *Proceedings of the 2020 ASEE Southeastern Section Conference, Auburn, AL, USA.* 2020.
24. Lu, Y. and Y.-H.C. Huang, *Getting emotional: An emotion-cognition dual-factor model of crisis communication.* Public Relations Review, 2018. **44**(1): p. 98-107.
25. Kaberuka, J. and C. Johnson. *Case Studies in the Socio-technical Analysis of Cybersecurity Incidents: Comparing Attacks on the UK NHS and Irish Healthcare Systems.* 2023. Singapore: Springer Nature Singapore.

26. Resodihardjo, S.L., *Crises, inquiries and the politics of blame.* 2020: Springer.
27. Reason, J., *Managing the risks of organizational accidents.* 2016: Routledge.
28. Boiarsky, C., *Risk Communication and Miscommunication: Case Studies in Science, Technology, Engineering, Government, and Community Organizations.* 2016: University Press of Colorado.
29. Hassanzadeh, A., et al., *A review of cybersecurity incidents in the water sector.* Journal of Environmental Engineering, 2020. **146**(5): p. 03120003.
30. Muller, M., *Adapting to climate change: water management for urban resilience.* Environment and urbanization, 2007. **19**(1): p. 99-113.
31. Svensson, E.I., *Understanding the egalitarian revolution in human social evolution.* Trends in Ecology & Evolution, 2009. **24**(5): p. 233-235.
32. Rodríguez, R., *From anticipatory strategies to reactive blame games in multi-level settings: the role of structure and politics in stability and policy change.* Journal of Public Policy, 2022. **42**(4): p. 802-826.
33. Clark, A., *Whatever next? Predictive brains, situated agents, and the future of cognitive science.* Behavioral and brain sciences, 2013. **36**(3): p. 181-204.
34. Carmeli, A., Gittell, J. H., *High-quality relationships, psychological safety, and learning from failures in work organizations.* Journal of Organizational Behavior, 2009. **30**(6): p. 709–729.
35. Valorozo-Jones, C., *Neurodiversity, Dungeons, and Dragons: A guide to transforming and enriching TTRPGs for neurodivergent adults OR the neurodivergent player's handbook.* 2021.
36. Gray, C., *Social StoriesTM*, in *Using Storytelling to Support Children and Adults with Special Needs.* 2012, Routledge. p. 104-110.
37. Maull, F., *Radical Responsibility: How to Move Beyond Blame, Fearlessly Live Your Highest Purpose, and Become an Unstoppable Force for Good.* 2019: Sounds True.
38. Porsdam Mann, S., et al., *Guidelines for ethical use and acknowledgement of large language models in academic writing.* Nature Machine Intelligence, 2024. **6**(11): p. 1272-1274.