From Fire Safety to Cybersecurity: Exploring the Role of Stress Exposure Training for Incident Response

Stefan Anthuber[0009−0008−9021−5676], Simon Rudhart[0009−0005−8807−5289], Uta Wagner[0000−0002−7885−5610], Sabrina Meindl[0000−0001−5065−713X], Michael Heigl[0000−0001−7303−113X], and Manfred Vielberth[0000−0002−1119−4715]

Faculty of Computer Science, Deggendorf Institute of Technology, Deggendorf, Germany
{stefan.anthuber, simon.rudhart, uta.wagner, sabrina.meindl michael.heigl, manfred.vielberth}@th-deg.de

Abstract. Cybersecurity incidents often catch decision-makers by surprise. Even when they know the risks, people can freeze, second-guess their knowledge, or unconsciously downplay the situation, blocking access to previously learned procedures. In these moments, humans can be both the most vulnerable and the key factor that shapes the outcome. Inspired by fire and rescue services, which train under realistic, high-stress scenarios, this study investigates the role of Stress Exposure Training in cybersecurity. The exploratory research draws on semi-structured interviews with six experts. It reveals a significant practice gap: current training methods leave practitioners without the routine-forged procedural confidence essential for high-stakes decision-making. Our findings reveal that while technical protocols exist on paper, they often remain dead knowledge during an actual crisis. Participants identify a clear organisational demand for training that moves beyond conventional e-learning toward experiential, stress-based exercises. Participants perceived stress-based training as a mechanism to reduce the initial shock of an attack, building the self-efficacy and serenity needed to transform passive victims into empowered first responders. This paper highlights the social and psychological drivers of security behaviour and provides insights into the management hurdles of implementing stress-based training.

Keywords: cybersecurity · human-centred Security · Stress Exposure Training · Decision-making · Human Factors.

1 Introduction

At least once a year, an alarm sounds in workplaces across nearly every industrialised country. Employees interrupt their activities and evacuate the building quickly yet in an orderly manner. The purpose of this exercise is to prepare for emergencies that, ideally, will never occur. Fire drills represent a widely adopted, and often legally mandated, method for training individuals to respond to critical situations as efficiently and safely as possible. Such drills are not limited to

employees. Emergency services, including ambulance personnel and firefighters, regularly engage in structured training scenarios. These exercises aim not only to reinforce adherence to predefined protocols but also to develop the ability to make sound decisions under stress and time pressure. This capability is particularly crucial for decision-makers such as fire brigade incident commanders, who must maintain situational control in dynamic environments under high mental pressure. Accordingly, training scenarios are often designed to deliberately induce stress to simulate realistic conditions.

In contrast, comparable practices remain largely underdeveloped in the field of cybersecurity. While it is clearly recommended that organisations maintain incident response plans and technical measures, these typically focus on predefined procedures and communication structures to be followed during an incident [23]. However, given the unpredictable and evolving nature of cyber threats, it is impossible to anticipate every potential scenario. Consequently, the ability of cybersecurity personnel to make effective, goal-oriented decisions under pressure is critical to minimising potential damage.

This gap becomes even more striking when comparing the scale of damage across the two domains. In Germany, the annual costs associated with fire damage amount to approximately €25 billion [31], whereas cyber incidents result in losses of around €202 billion [3], which is more than eight times higher, with a continuing upward trend. Despite this disparity, only 22% of German organisations report having conducted any form of cybersecurity emergency drill or simulation exercise [32]. While this figure does not measure the adoption of stress exposure training (SET) specifically, it indicates that structured cybersecurity emergency exercises remain uncommon. Rather than addressing all causes of cyber incidents, SET specifically targets the human component of incident response by preparing participants to make effective decisions and maintain performance under stress. This suggests a significant lack of stress exposure training within the cybersecurity domain. To take an initial step toward addressing this gap, this paper is guided by the following problem statement:

> *Despite the high-pressure and decision-intensive nature of incident response, stress exposure training is an underdeveloped yet promising component of cybersecurity practice.*

We first examine the need for SET in both research and practice within the cybersecurity domain. Then, we analyse existing literature on SET, drawing primarily on more established fields such as medicine and emergency services, where these approaches are more mature and systematically integrated. To evaluate the problem statement, six semi-structured expert interviews were conducted to assess current training methods of organisations and identify the need for new approaches, particularly SET. The evaluation of the interviews suggests a perceived need for SET to bridge the gap between theoretical knowledge and practical application, as well as to address all types of learners.

To address these challenges, this paper provides the following key contributions to the fields of human-centred security and crisis management:

- We establish a conceptual bridge between SET approaches in established high-risk domains - such as fire safety - and cybersecurity incident response, highlighting the relevance of practising decision-making under controlled stress conditions for digital crisis.
- Based on our qualitative interviews with cybersecurity and organisational decision-makers, we identify a perceived gap between formal incident response procedures and the ability to execute them effectively under conditions of stress, uncertainty, and time pressure.
- We show that decision-makers perceive current cybersecurity training approaches as primarily focused on procedural knowledge transfer, while practical rehearsal under realistic conditions is limited. This contributes to a perceived lack of operational readiness in high-pressure situations.
- We identify key organisational and psychological barriers that may hinder the adoption of stress-based cybersecurity training formats, including competing productivity demands, limited prioritisation at the management level, and employees' fear of making mistakes in socially visible settings.

2 Background and Related Work

In general, training user behaviour in cybersecurity is seen as a crucial part to enable secure behaviour [17]. Training people to adopt security-compliant behaviour is especially paramount in an organisational environment [26]. There exist several immersive or simulation-based training approaches in cybersecurity research, ranging from capture-the-flag (CTF) events, serious games, cyber range exercises, to virtual reality simulations, gamified learning platforms, hybrid escape rooms, and board games [30]. The goal of such training is, in most cases, to teach either technical knowledge, threat identification, or incident response. Over the last few years, it has become clear that acquiring non-technical and soft skills, such as stress resilience and reasoning, is equally important [2, 12, 28, 25].

To build stress resilience, it is important to understand the term stress. It describes a process in which environmental demands (e.g., time pressure, new or threatening events) trigger an appraisal process in which the perceived demands exceed available resources, leading to undesirable physiological, psychological, behavioural, or social consequences [8]. This effect is also present in situations where a cybersecurity incident occurs, and immediate action and decision-making are needed to contain an attack and minimise damage [33].

In this context, it is crucial to distinguish between cybersecurity incident response management (IRM) and SET. IRM is the operational process for detecting, containing, eradicating, and recovering from a cyber incident [21]. SET, on the other hand, is not specific to cybersecurity; it provides an approach for integrated stress training that deliberately practices those skills under pressure to enable people to perform better in real incidents [7]. The SET as defined by Driskell and Johnston [7] is divided into three phases: (1) Information provision, (2) Skills acquisition, and (3) Application and practice. Thus, SET could

provide structure to any existing cybersecurity exercise to enable the induction and measurement of stress during training. The SET model is regarded as a key framework in applied psychology for reducing the negative impact of stress on performance and decision-making [8, 11, 16].

IRM is characterised by high-stakes decision-making, limited time, and significant uncertainty [21, 20, 1]. At the management level, the stakes often involve coordinating multi-agency efforts and strategically allocating resources [20]. Traditional training for these roles has historically relied on methods that do not adequately simulate the stress exposure found in real crises. Table-top exercises, while useful for procedural knowledge, are often criticised for their lack of realism and pressure [19]. On the contrary, large-scale physical simulations, though realistic, are expensive and difficult to scale [20]. As an overlap between the two areas, serious games and mixed-training approaches emerged [18, 22, 5].

The NIST SP 800-84 [13] is a guide worth mentioning in the context of leading organisations to improve IT contingency plans through structured testing, training, and exercise programs. It promotes scenario-driven exercises to test incident-response capabilities, though the framework does not explicitly address stress induction, measurement, or evaluation.

Table 1: Related work on stress exposure training approaches.

Approach	**Year**	**Target Group**	**Learning Outcome**	**Domain**	**Type**
DREAD-ED [14]	2010	Crisis managers, Students	Effective communication and group decision -making in disaster management	Dis.	SG
Pandora [20, 1]	2013/17	Gold commanders	Strategic planning under extreme pressure	Any	eL
Mayor Game [29]	2019	Mayors	Decision-making in crisis situations	Civil	SG
VROnSite [22]	2021	First responder squad leader	Decision-making in complex first responder scenarios	Emerg.	VR
eXtricate [5]	2022	Firefighters	Decision-making under stress	Emerg.	SG
DisasterPlay [15]	2024	Emergency responders	Disaster management resilience	Emerg.	SG

Abbreviations: SG = Serious Game; eL = eLearning; VR = Virtual Reality; Dis. = Disaster; Emerg. = Emergency

Related work in Table 1 displays that there are approaches that integrate SET. Since 2010, six relevant approaches have been identified in the literature. This landscape is mainly dominated by the emergency response domain, and

most are conceptualised as serious games. They all follow the common goal of training specifically in stressful situations, including induction and measurement of stress.

As Table 2 shows, all of these approaches aim to train participants under stressful conditions, but they differ significantly in terms of which stressors they operationalise and how they measure the resulting stress. We map the six related approaches against the stressors and their measurement dimensions relevant to this work. The four applied decision stressors: *time pressure*, *information overload*, *complexity*, and *uncertainty & risk*, follow the taxonomy proposed by Phillips-Wren & Adya [24]. They characterise the conditions under which high-stakes decisions are typically made. Since incident response is inherently a socio-technical activity, this taxonomy is extended with a fifth stressor, social pressure, drawing on the social-evaluative threat construct of Dickerson & Kemeny [6], to capture the interpersonal and evaluative demands (e.g., peer observation, accountability to a team or supervisor) that arise during incident handling but are not captured by decision stressors alone. Alongside the stressor dimensions, Table 2 reports whether and how each approach measures the resulting stress response, distinguishing three established measurement modalities as defined by Driskell & Salas [8]: *physiological* (e.g., heart rate, skin conductance), *self-report* (e.g., subjective stress or workload scales), and *behavioural* (e.g., performance degradation, response latency, error rate) indicators. Together, these columns allow the related work to be compared not only in terms of which stressors are elicited, but also in terms of whether the resulting stress was empirically validated, and through what modality.

Table 2: Mapping of related work to stressors and stress measurement.

	Decision Stressors					**Stress Measurement**		
Approach	Time pressure	Info overload	Comp-lexity	Uncert. & risk	Social pressure	Physio-logical	Self-report	Behav-ioral
DREAD-ED [14]	–	–	–	✓	✓	–	✓	–
Pandora [20, 1]	✓	✓	–	✓	–	✓	✓	✓
Mayor Game [29]	✓	✓	–	✓	✓	✓	✓	✓
VROnSite [22]	–	–	✓	✓	–	○	✓	✓
eXtricate [5]	✓	✓	–	✓	✓	✓	✓	–
DisasterPlay [15]	–	–	–	✓	–	✓	–	✓

✓ present; – not reported; ○ indirect/observational.

Several patterns emerge from this mapping. *Uncertainty & risk* is the only stressor present across all six approaches, suggesting it functions as the baseline condition for stress-based training in incident response, while *complexity* remains the most neglected dimension overall. The two stressors, *time pressure* and *information overload*, are found in only half of the approaches, indicating a connection to the underlying training scenario. *Social pressure*, despite its relevance to team-based incident response, is similarly addressed in only half of the approaches, attributing that interpersonal stress is still under-elicited rela-

tive to individual cognitive stressors. On the measurement side, *self-report* is the most consistently applied modality, while *physiological* and *behavioural* measurements follow right after. This points out that, in related work, induced stress is also objectively validated. Notably, no approach combines all five stressors with all three measurement modalities, underscoring that comprehensive coverage of both stressor elicitation and empirical validation remains an open challenge for SET in incident response. Taken together, most stress training approaches are serious games targeting emergency response, leaving organisational cybersecurity underexplored. While research shows stress can be induced and measured, existing methods fail to address the full spectrum of decision and social stressors or span all organisational roles. To bridge this gap and ground the need for a new SET approach, we consult expert practitioners to establish whether and why SET is perceived as necessary in cybersecurity.

3 Methodology

We designed a qualitative study based on semi-structured interviews to examine how prepared organisations are for cyber incidents and to determine whether there is a practical need for SET. Instead of running a large-scale survey to obtain statistical generalisations, we interviewed six high-level experts and organisational decision-makers, as shown in Table 3, to gather deep, context-rich insights. Fire protection exercises were used as a contextual reference rather than a direct comparison, as they are regularly conducted in organisations. This raises the question of why comparable practice-oriented training is common in physical safety contexts but less established in cybersecurity. To explore this, our interviews covered the participants' personal experiences with cyberattacks, their current organisational training setups, and their perceptions of stress-based simulations. To address our core problem statement, these aspects were operationalised into three central research questions:

Firstly, **RQ1:** *How do decision-makers assess the current capability of their organisations to respond to cybersecurity stress situations?*

We use fire drills as a reference to compare perceived preparedness with real-world stress demands.

Secondly, **RQ2:** *What opportunities and added value do decision-makers see in stress-based training?* We explore perceived benefits and relevant target groups for this training method.

And thirdly, **RQ3:** *What barriers and concerns exist regarding the adoption of such training formats?* Here, we investigate practical and organisational obstacles, as well as willingness to invest.

3.1 Participants

A total of *six* individuals from different organisations participated in separate interviews. This included *five* male (m) and *one* female (f) participants, aged

between 33 and 60 years. Participants were recruited from organisations of different sizes in Germany to capture diverse perspectives on cybersecurity preparedness and training. Table 3 presents key anonymised information about the respondents, needed to contextualise their statements within the scope of this paper.

Table 3: Demographic characteristics of the participants.

ID	Current Position	Age	Gen.[a]	Exp.[b]	Domain	Employees
P1	Consultant	60	m	35	Woodworking company	51–250
P2	CFO	46	m	10	Manufacturer in building industry	51–250
P3	Head of IT	53	m	30	Public administration	251–1000
P4	Head of IT	39	m	8	Manufacturing of IT components	51–250
P5	Product Owner	43	m	16	Automotive and machinery supplier	100 k–250 k
P6	CY [c] Researcher	33	f	9	Defence	100 k–250 k

[a] Gender, [b] Experience in IT: Years, [c] CY: Cybersecurity.

3.2 Procedure and Ethical Considerations

In the process of participant recruitment, we ensured that we got an overview of different domains and also a variation in the number of employees of the organisations. For this, we used an expert-sampling approach using the authors' contacts to find individuals in charge of cybersecurity or the IT department (or equivalent positions).

The interview guideline with further details is presented on GitHub[1]. We utilised a semi-structured interview approach to balance comparability with the flexibility to explore individual experiences. By using open-ended questions, we enabled participants to provide rich, descriptive explanations of their actual situation. To ensure high quality, the interview guideline was developed by all authors and field-tested before conducting the interviews. All interviews were conducted via Microsoft Teams.

After transcription, all audio files were deleted, and all personal data were removed to ensure the anonymisation of the data.

Access to the information gathered during the interviews is limited to a small number of people. The interviews were conducted in March and April 2026, and none of the participants received monetary or non-monetary compensation for it. The interviews lasted between 30 and 45 minutes. All participants were informed about the conditions of the interview, data use, and further processing.

[1] https://github.com/stress-exposure-training/interview-guideline

3.3 Data Analysis

We used Qualitative Content Analysis to get structured insights from these conversations. Our analysis followed a strict privacy-first workflow to ensure that the sensitive organisational vulnerabilities discussed remain secure:
Local Transcription and Manual Refinement: We processed all audio recordings locally using *Whisper*[2]. All interviews were transcribed locally using Whisper and manually validated. Following the automated pass, we manually reviewed and corrected each transcript to ensure that technical terms and context details were captured accurately.
Systematic Coding: We used *MAXQDA* [3]to manage the coding (deductive and inductive), where our initial coding frame was derived directly from our RQs and core hypotheses, shown in Table 4. This allowed us to identify clear patterns and differences across the organisations. Two people performed the coding and discussed it with the interviewer, who reviewed and approved it. The coding scheme evolved iteratively. As this was an exploratory qualitative study, no formal inter-coder reliability score was calculated.
Categorisation: We synthesised the coded data into the primary thematic clusters, each designed to map the raw interview insights directly back to our research objectives.
Analysis: We used *Summary Grid* to compare all six interviews with each other.

Table 4: Overview of thematic clusters and associated codes.

Thematic Cluster	Core Focus	Key Codes & Hypotheses
Response Capability (RQ1)	Gap between "theoretical compliance" and real-world crisis readiness.	**1.1** Theory vs. Practice **1.2** Self-Assessment Deficits **1.3** Fire Drill Analogy **1.4** Impact of Past Incidents
Training Evaluation (RQ2)	Perceived value and sustainability of immersive, stress-based training.	**2.1** General Acceptance **2.2** Long-term Learning Efficacy **2.3** Target Group Identification
Barriers & Investment (RQ3)	Organisational hurdles and willingness to fund non-traditional training.	**3.1** Resource Constraints **3.2** Management Support

4 Findings

The qualitative analysis of the semi-structured interviews with six decision-makers (n=6) resulted in the following findings, organised by primary research questions (Methodology 3).

[2] https://github.com/Const-me/Whisper/releases
[3] https://www.maxqda.com

RQ1: Assessment of Organisational Response Capabilities. The interviews reveal a persistent gap between theoretical knowledge and confident action under pressure. While all organisations claim to foster a transparent error culture — with P4 noting that *"no one gets their head ripped off"* for making a mistake — this psychological safety does not yet equate to technical competence during an incident.

The Efficacy of Current Training Formats. Participants perceived traditional training as inadequate. P2 dismisses current webinars as a *"tick-the-box"* exercise that fails to engage different learning types, suggesting only realistic simulations, like controlled ransomware, could trigger a meaningful learning curve: *"that would really be great because it brings the learning curve extremely up"*(P2). P6 adds a behavioural layer to this critique, observing that webinars are often favoured by less motivated or overburdened employees because they can *"run in the background"* without requiring active engagement. This lack of practical experience is reflected in the participants' sobering self-assessments. P3 explicitly distinguishes between having an emergency plan on paper and being able *"to execute it,"* ultimately rating their team's readiness at a 2 out of 5 due to *"zero practical exercises"* (P3). P5 observes that despite frequent theoretical instructions, errors remain *"conspicuously frequent,"* leading to the conclusion that knowledge transfer is currently *"medium at best."*

Fire Drill Paradox. A striking finding is the universal use of fire safety drills as a gold standard for what cybersecurity training lacks. Participants view fire drills as a professionalised, annual routine where employees know exactly how to behave, such as *"meeting at the assembly point"* (P4). P1 notes that while fire safety is mandated by *"legal regulations"*, comparable cybersecurity drills *"do not exist as of today"* (P1). P6 provides a crucial socio-economic explanation for this deficit: fire drills protect *"life and limb,"* a concept intuitively understood by everyone, whereas cyberattacks are perceived as abstract threats to **"company value"**. Furthermore, P6 highlights a *"Productivity-Loss Bias"*: while a 10-minute fire drill is an accepted social routine, a 10-minute cyber-exercise that *"freezes the screen"* is viewed as a costly disruption of billable labour time. While P5 remains more critical, questioning if the rarity of actual fire makes these routines more effective, the overall sentiment is a desire to institutionalise cybersecurity with the same *"live factor"* and regularity as physical safety drills.

Post-Incident Learning. Currently, organisational change is largely reactive, driven by the *"permanent learning process"* of handling real-world attacks (P1). However, the interviews show a positive shift in how these incidents are handled. Rather than top-down reprimands, leaders like P2 have adopted a *"workshop character"* where teams analyse errors collectively. P6 emphasises that an open error culture is vital not just for morale, but for operational intelligence; it allows for the anonymous handling of mistakes, preventing employees from *"blocking"* or hiding vulnerabilities out of fear of retribution. Both P3 and P5 emphasise that the most effective way to keep training grounded in reality is to integrate these local, visible examples of attacks back into the next *"sensitisation"* phase, turning every failure into a shared learning opportunity.

RQ2: Opportunities and Added Value of Stress-based Training. The feedback regarding stress-based training was overwhelmingly positive, with experts viewing it as a necessary evolution of current security strategies. Rather than viewing simulations as just another compliance task, participants described the approach as a way to build situational *"muscle memory."* P2 characterised this shift as *"exactly what is needed"* to fix a training landscape that is currently *"lagging"* behind real-world threats. Most notably, P4 described this type of high-pressure simulation as a *"vaccination"* against the paralysis that often occurs during a real attack. This involves a deliberate departure from what P4 called *"feel-good, cuddling training"* in favour of scenarios that force users to confront the *"initial shock"* of an incident. This sentiment was echoed by P3, who identified the concept as a direct solution to a long-standing structural weakness, stating that the method *"goes exactly in the direction where we have a gap"* (P3). P6 complements this by noting that *"playing through"* a scenario once ensures better retention across all learning types, transforming abstract knowledge into an *"experienced event."*

Simulations as an Operational Toolbox. A recurring theme throughout the interviews was that stress in a crisis often stems from a lack of clear agency. P1 argued that simulations should serve as a *"toolbox"* providing users with concrete *"checklists for stress situations"*—such as immediate contact points and the first steps of technical analysis. Without such resources, users are prone to the paralysis P4 observed during real-world ransomware incidents, where even those who *"think they know what to do"* are immobilised by the actual event. P6 agrees, emphasising that stress factors—such as time pressure and urgency—are essential *"active ingredients"* because they reveal mistake patterns that remain hidden during relaxed, conventional exercises. Furthermore, experts highlighted the importance of *"forced engagement."* P5 pointed out that traditional e-learning often allows for *"passive consumption,"* where users might let a video play while *"getting something to eat"* or checking emails. Multisensory or high-pressure approaches (like escape rooms or timed drills) prevent this multitasking, ensuring that the training requires genuine cognitive processing and active participation.

Learning Efficacy and Target Group. For P2, the value of stress-based training is measured by *"serenity,"* the ability to stay calm and immediately initiate correct measures, such as *"pulling the network plug"* (P2). Regarding target groups, the consensus was that the end-user serves as the critical *"first responder"* (P1) who needs physical, actionable instructions. However, P3 suggests that training should not be individual but a team exercise involving the top executives, IT, and end users to test coordination under pressure. While P1 and P2 focus on the general staff, P6 identifies the highest impact among those in positions of responsibility, arguing that simulated pressure allows decision-makers to remain calmer and act more decisively when *"Day X"* arrives.

RQ3: Barriers and Concerns Regarding Adoption Despite the high acceptance of stress-based simulations, the interviews revealed several practical and organisational hurdles. The primary challenge is not a lack of general ap-

proval, which most experts described as high—but rather a constant conflict with operational priorities.

Resource and Time Constraints. Time is identified as the enemy of training. P4 notes that even 30 min of an employee's time can be too much because *"daily business"* and operational tasks always take precedence. P6 echoes this, identifying the *"time factor"* as the biggest hurdle for management. Stress training needs to be adopted; its success must be "measurable" (e.g., through metrics) to justify the investment over cheaper, passive formats. Smaller organisations face even greater hurdles, as P1 put it, *"you cannot do everything at once."* P2 estimates that creating high-quality, individualised training requires at least *"one man-week of intensive work"* (P2), a massive burden for IT capacities.

Management Support and the "Fear of Exposure". A significant finding introduced by P6 is the psychological barrier of *"Performance Anxiety."* Unlike passive webinars, live stress-based training forces employees to *"show their weakness."* P6 identifies this *"Fear of Exposure"* as a major adoption hurdle, suggesting that organisations must proactively foster a *"no-blame culture"* to ensure employees don't feel pre-emptively defeated by the challenge. While management support exists in principle-since, as P1 noted, it is *"their company"* at risk a notable gap remains in how that support translates into action. Unlike occupational safety, which is accepted as a basic necessity, the value of cyber training often has to be justified. P4 explains that it requires *"cost-benefit comparison"* just to prove that the cost of a hack far outweighs the price of the training. The real bottleneck is often middle management. P2 identifies department heads as the *"biggest obstacles"* because they fear the loss of productivity and complain about *"too many trainings"* (P2). This lack of prioritisation is exemplified by P3, who admitted that despite institutional support, their cybersecurity training has been *"pushed to the back for two years"* because it never felt as urgent as other operational tasks. Ultimately, P5 concludes that adoption is a *"question of will"* (P5). If the executive in charge is personally convinced that the format *"really achieves something"*, the necessary budget and resources usually follow.

Findings on Psychological Dynamics and Stress Perception. A key theme throughout the interviews involves the psychological mechanism of learning under pressure and how experts evaluate staff reactions during a crisis.

Authenticity of Stress-Inducing Simulations. The data reveals a debate regarding whether *"artificial"* stress can truly replicate a real cyberattack. P4, drawing on personal experience from a *"Red vs Blue exercise,"* argues that even in a controlled environment, *"brutal pressure"* is achievable through strict time limits and competitive elements: *"you know it wasn't real, but you still had brutal pressure [...] because of the limited time"*(P4). P6 supports this, noting that simulating the *"initial shock"* helps users stay calmer in the future. In contrast, P5 remains sceptical, stating that true stress only arises when there are tangible, high-stakes consequences, such as *"shutting down a plant"*(P5). P2 suggests a middle ground, focusing less on *"stress"* and more on the *"practical aspect,"* as most users have no mental image of what a real attack actually looks like and thus cannot react effectively.

The Confidence Gap and "Serenity." The experts drew a sharp line between technical staff and general users. P5 rates the IT department's reaction speed at a perfect 5 out of 5, noting that non-IT users often fail to grasp the gravity of a situation. This is reflected in the assessments of P4 and P6, who both rate the ability of general staff to react under severe pressure as only 2 or 3 out of 5.

To bridge this gap, P2 argues that the goal of training should be *"serenity."* The aim is for the employee to become an empowered *"first instance"* responder who can act (e.g., pulling a network plug) without panicking (P1). To prove the value of this empowerment, P1 suggests an experimental approach: *"Measure the pulse of two groups... one with a checklist, one without... and see how it looks."*

Social Pressure and Team Dynamics. Finally, both P3 and P6 point to the *"fear of exposure"* as a key psychological driver. P6 warns of this as a barrier to participation, but also notes that an anonymous error culture can mitigate this *"blocking"* behaviour. P3 observes that in the public sector, the dread of being *"the one who clicked the link"* in front of the department can act as a powerful, albeit stressful, motivator for sensitivity.

5 Discussion

Cybersecurity often overlooks the fact that even the best policies are worthless at the moment of an acute attack if those affected block under stress. It is of little use to know what to do if fear prevents it from being carried out. The result is a glaring gap between what's on paper and what actually works under pressure. To find out how stress-based training (SET) needs to be structured to close this gap, we compared existing concepts from crisis research – such as the Pandora platform [20, 1] or serious games such as DREAD-ED [14] and eXtricate [5] – with the real experiences from our expert discussions. In the following, we discuss the most important findings in relation to our three research questions.

RQ1: How do decision-makers assess the current capability of their organisations to respond to cybersecurity stress situations? Our findings reveal a gap between awareness and action. Participants consistently described their organisations as maintaining a supportive error culture; this psychological safety did not appear to translate into confidence during an active security incident. Several participants distinguished between the existence of documented response procedures and the ability to execute them under pressure [P3]. This suggests that formal guidance alone may be insufficient for developing reliable response behaviour. Instead, organisational knowledge appears to remain largely declarative when opportunities for practical application are limited [P3, P5].

This observation can be interpreted through the three-phase SET model of Driskell and Johnston [7, 8]. SET proposes that effective performance under stress emerges through repeated practice under progressively demanding conditions rather than through knowledge acquisition alone. Our interview data indicates that many current awareness activities emphasise information transfer, while opportunities for active application remain scarce. Participants frequently

characterised webinars as passive compliance exercises that require little engagement beyond attendance [P2, P6]. From a SET perspective, such approaches may support initial knowledge acquisition but provide limited support for developing procedural skills that can be recalled during an incident. This interpretation aligns with participants' reports of limited practical preparedness despite regular awareness efforts [P3, P5]. The recurring comparison between cybersecurity exercises and fire drills provides additional insight into organisational perceptions of risk. Participants described fire drills as established and legitimate organisational practices, whereas comparable cybersecurity exercises were largely absent [P1, P4]. One explanation offered by participants is that physical emergencies are directly associated with personal safety, while cyber incidents are often perceived as threats to organisational assets rather than individuals [P6]. Participants also highlighted concerns about productivity loss, suggesting that simulated cyber incidents are often viewed as interruptions to daily work rather than as preparedness activities [P6]. Together, these observations point to organisational and cultural barriers that may limit the adoption of experiential cybersecurity training. Finally, our findings highlight the role of post-incident reflection as a mechanism for organisational learning. Participants emphasised the value of collaboratively reviewing incidents without assigning blame [P2, P6]. Such practices appear to facilitate open discussion of vulnerabilities and uncertainties while reducing incentives to conceal mistakes. Several participants further noted that incorporating locally relevant incidents into subsequent awareness activities increases the perceived relevance of training and grounds learning in concrete organisational experiences [P3, P5].

RQ2: What opportunities and added values do decision-makers see in stress-based training? Our findings suggest that one perceived benefit of stress-based training may be the development of situational self-efficacy. The expert reports overlap with the psychological principle of Stress Inoculation Training (SIT). Saunders *et al.*[27]. Stressors such as time pressure, unclear data or false alarms under controlled conditions are described as a form of psychological "vaccination" [P4]. Such exposure is perceived as potentially reducing the likelihood that individuals become overwhelmed when encountering a real incident.

While security research often sees stress only as a pure risk of error, areas such as disaster control have long used targeted stress induction as a tool. Research on serious games for emergency situations shows very clearly how important the interactive experience is compared to passive media. Chittaro and Sioni [4] emphasise in their research that purely traditional presentations, printed materials or videos are often used only for convenience and cost reasons. However, their findings suggest that only the active, interactive re-enactment of a crisis situation profoundly shapes the behavioural patterns and self-efficacy of those affected. Participants argued that these established principles should finally be used to replace the ineffective "cuddle training" [P4] in IT security with interactive, stress-based simulations. Several participants framed stress as a consequence of limited agency rather than merely emotional pressure. Simulations were therefore not only viewed as training environments but also as opportunities

to rehearse concrete response procedures and decision pathways [P1, P4]. This suggests that experiential cybersecurity training may reduce stress by increasing users' perceived ability to act, rather than solely by increasing awareness. To underline this, the study by Ali Fauzi et al. [10] indicates that stressful situations negatively affect secure cybersecurity behaviour. Therefore, an approach such as SET may improve security-compliant behaviour even under pressure through repeated practice and experiential learning. Considering that social engineering remains one of the primary attack vectors used (phishing 60%) by threat actors [9], cybersecurity interventions should address all stakeholder groups. In this regard, SET may help improve behaviour in stressful situations through acclimatisation and procedural reinforcement. As one participant explained: "It's not a bad idea for the user, as it helps reinforce processes and routines, similar to a fire drill. That way, you know, 'Aha, this is what I need to do now,' instead of, I don't know, just unplugging something or switching it off" (P5).

Our findings indicate that stress-based training is most effective when embedded in collaborative, multi-user settings. Participants highlighted that real incidents require coordination across roles and hierarchies, which is rarely reflected in individual training formats [P3]. Multi-user simulations therefore enable the reproduction of communication structures and decision dependencies under pressure. Related work on cooperative crisis environments similarly suggests that shared stress can support coordination when properly scaffolded [20, 1]. In this context, stress is not primarily a disruptive factor, but a mechanism that reveals coordination requirements and reinforces structured communication practices. SET may benefit different stakeholder groups, from end users facing phishing attacks to IT staff and executives requiring specialised incident response training. Training formats should be adapted to the specific needs of each group.

RQ3: What are the barriers and concerns regarding the adoption of stress-based training? While prior work on cybersecurity training emphasises its importance for behavioural change [17, 26], our findings show that training interventions are frequently deprioritised in favour of operational KPIs at the middle-management level. This aligns with broader observations in incident response contexts, where time-critical decision environments often conflict with routine productivity demands [21]. Participants highlighted that even relatively short training sessions are perceived as an annoying disruption to daily, billable working hours [P6], particularly when the long-term strategic benefits are not immediately quantifiable to management. Furthermore, participants described stress-based training as a setting in which individual performance becomes visible, thereby introducing what can be interpreted as *performance exposure*. In contrast to passive training formats, such as e-learning or table-top exercises [19], stress-based approaches inherently require active decision-making under observation. Our findings indicate that this visibility can generate avoidance behaviour when social evaluation pressure exceeds a tolerable threshold, driven by a distinct fear of negative consequences or institutional stigma trailing potential mistakes [P6]. This extends prior work on serious games and crisis simulations by highlighting psychological safety as a critical adoption factor, which is often

underexplored in existing cybersecurity training literature. These observations connect directly to SET theory [7, 8], which emphasises that stressors must be carefully calibrated to support rather than inhibit learning. While SET has been successfully applied in emergency response and crisis management domains (e.g., [20, 1, 5]), our findings suggest that cybersecurity training introduces an additional layer of social evaluative stress that is less prominent in other domains. This includes fear of embarrassment in front of colleagues or perceived reputational damage after incorrect actions.

These barriers do not contradict the value of stress-based training but instead define its design constraints. In line with prior crisis training systems such as Pandora [20, 1], our findings suggest that stress can function as a productive learning trigger only when embedded in a supportive organisational environment. Within such an environment, the focus of stress exposure shifts away from inducing panic and toward cultivating operational *serenity* [P2]. This state of calm composure enables individuals to overcome the initial shock of an attack and confidently execute basic mitigation protocols—such as rapidly disconnecting a network cable—rather than collapsing into cognitive paralysis [P1, P2]. Without such supportive conditions, increased stress may shift learning into avoidance behaviour rather than improved performance.

6 Limitations and Future Work

When analysing our results, there are a few points to keep in mind. First, we focused on six high-level experts in their domain. While this approach precludes statistical generalisation, it allowed us to gather the kind of deep, context-rich insights into corporate realities that large-scale surveys often miss. To build upon this, future research should implement comparative, controlled experiments to quantify how these stress-based formats impact long-term knowledge retention and operational behaviour compared to conventional approaches.

Second, there is a clear gender imbalance among our participants. This is not a recruitment flaw, but a reflection of the industry reality, where women remain highly underrepresented in senior cybersecurity roles. Future work should intentionally sample more diverse cohorts to explore how different backgrounds and team cultures affect stress perception.

Third, we focused primarily on time pressure as the main stressor. However, the design space for stress training includes many other variables—like information overload or audio-visual effects — that warrant future exploration. Although prior research identifies broader stressor categories, participants mainly emphasised time pressure and perceived stress. As these categories were not explicitly introduced during the interviews, future studies should examine additional stressors through targeted interviews or experimental designs. A key objective for future research is to evaluate and quantify SET success. Drawing on an insight from P1, who suggested comparing the heart rates of individuals working with and without checklists, a promising avenue for next-generation cyber-ranges is the integration of biometric sensors, such as those measuring heart rate vari-

ability or galvanic skin response. Incorporating these metrics allows researchers to empirically monitor physiological stress loads and validate whether SET successfully translates into long-term operational serenity. It would also be valuable to test hybrid models that combine standard e-learning with periodic stress simulations, to examine whether this training helps employees stay calm during everyday, lower-intensity workplace stress.

Fourth, organisational aspects need to be considered. Appropriate safeguards for participants in SET training must be established. Future research should investigate the potential effects of training-related stressors, such as time pressure, audio and visual stimuli, or other interventions. In addition, suitable procedures for debriefing participants and analysing training outcomes should be developed to ensure that results are not used to benchmark or disadvantage individual participants. These considerations are equally important for research contexts involving human participants or for use in companies. It is essential to further analyse the barriers to SET adoption identified in this paper and to evaluate potential solutions with responsible parties. This would support a better understanding of factors influencing acceptance and help identify additional barriers and enablers for the implementation of SET and related training approaches.

7 Conclusion

This paper presents a qualitative study of cybersecurity incident response and uses fire drills as a motivational analogy for preparedness. While cybersecurity incidents differ substantially from physical emergencies, both require recurring practice to build effective responses under pressure. The study therefore argues for a shift from occasional awareness activities toward specialised, recurring training exercises that establish cybersecurity preparedness as a routine organisational capability and identifies organisational barriers that require further examination in future research.

Based on in-depth insights from six domain experts, we identify a critical practical gap: documented incident response protocols consistently fail to translate into confident action under acute pressure. As conventional training models rely almost exclusively on passive knowledge transfer, organisational readiness remains largely theoretical. Our findings indicate a perceived need for improved training methods in cybersecurity exercises. Participants frequently identified targeted and realistic SET approaches as one possible way to address this gap. Crucially, we show that the primary barrier to adopting such frameworks is not a lack of management buy-in, but rather a direct clash between daily productivity demands and long-term behavioural resilience - a friction further complicated by employees' performance anxiety during live exercises. All in all, our work highlights a necessary paradigm shift in security training. To transform passive end-users into resilient first responders, the status quo of purely awareness-focused cybersecurity must be augmented by calibrated stress simulations designed for the chaotic reality of real-world crisis.

References

1. Bacon, L., MacKinnon, L.M., Kananda, D.: Supporting Real-Time Decision-Making Under Stress in an Online Training Environment. Rev. Iberoam. de Tecnol. del Aprendiz. **12**(1), 52–61 (2017)
2. Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., Shinoda, Y.: Integrated framework for hands-on cybersecurity training: CyTrONE. Comput. Secur. **78**, 43–59 (2018)
3. Bitkom e.V., Wirtschaftsschutz 2025: Lagebild der deutschen Wirtschaft, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Berlin (2025). https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutz (visited on Apr. 2, 2026)
4. Chittaro, L., Sioni, R.: Serious games for emergency preparedness: Evaluation of an interactive vs. a non-interactive simulation of a terror attack. Comput. Hum. Behav. **50**, 508–519 (2015). https://doi.org/10.1016/J.CHB.2015.03.074
5. Daylamani-Zad, D., Spyridonis, F., Al-Khafaaji, K.: *A framework and serious game for decision making in stressful situations; a fire evacuation scenario*, (2022).
6. Dickerson, S.S., Gable, S.L., Irwin, M.R., Aziz, N., Kemeny, M.E.: Social-evaluative threat and proinflammatory cytokine regulation: an experimental laboratory investigation. Psychological science **20**(10), 1237–1244 (2009)
7. Driskell, J.E., Johnston, J.H.: Stress exposure training. (1998)
8. Driskell, J.E., Salas, E.: Stress and human performance. Psychology Press (2013)
9. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025. Tech. rep., European Union Agency for Cybersecurity (ENISA) (2025). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (visited on Aug. 7, 2026)
10. Fauzi, M.A., Yeng, P., Yang, B., Rachmayani, D.: Examining the Link Between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia. In: Proceedings of the 16th International Conference on Availability, Reliability and Security. ARES '21. Association for Computing Machinery, Vienna, Austria (2021). https://doi.org/10.1145/3465481.3470094
11. Garris, R., Ahlers, R., Driskell, J.E.: Games, motivation, and learning: A research and practice model. In: Simulation in aviation training, pp. 475–501. Routledge (2017)
12. Glas, M., Böhm, F., Schönteich, F., Pernul, G.: Cyber Range Exercises: Potentials and Open Challenges for Organizations. In: Furnell, S., Clarke, N.L. (eds.) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, pp. 24–35. Springer (2023)
13. Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T.: NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, (2006). https://csrc.nist.gov/pubs/sp/800/84/final (visited on Aug. 6, 2026).
14. Haferkamp, N., Krämer, N.C.: Disaster Readiness through Education - Training Soft Skills to Crisis Units by Means of Serious Games in Virtual Environments. In: Wolpers, M., Kirschner, P.A., Scheffel, M., Lindstaedt, S.N., Dimitrova, V. (eds.) Sustaining TEL: From Innovation to Learning and Practice - 5th European Conference on Technology Enhanced Learning, EC-TEL 2010, Barcelona, Spain, September 28 - October 1, 2010. Proceedings. LNCS, pp. 506–511. Springer, Heidelberg (2010)

15. Hayette, H., Hemmje, M., Zineb, H., Vu, B., Abdelkrim, M.: Applied Gaming-Based Emotion-Driven on Disaster Resilience Training. In: 1st Int. Conference on Innovative and Intelligent Information Technologies (IC3IT), pp. 1–6 (2024)
16. Johnson, G.G., LaPorta, A.J.: Stress Exposure Training. In: Trauma Team Dynamics: A Trauma Crisis Resource Management Manual, pp. 89–96. Springer (2025)
17. Kävrestad, J., Fallatah, W., Furnell, S.: Cybersecurity Training Acceptance: A Literature Review. In: Furnell, S., Clarke, N.L. (eds.) Human Aspects of Information Security and Assurance - 17th IFIP WG 11.12 International Symposium, HAISA 2023, pp. 53–63. Springer (2023)
18. Linehan, C., Lawson, S., Doughty, M., Kirman, B.: There's no 'I' in 'Emergency Management Team: ' Designing and evaluating a serious game for training emergency managers in group decision making skills. In: Proceedings of the 39th Conference of the Society for the Advancement of Games & Simulations in Education and Training. Innovation North-Leeds Metropolitan University (2009)
19. MacKinnon, L.M., Bacon, L.: Developing realistic crisis management training. In: Rothkrantz, L.J.M., Ristvej, J., Franco, Z. (eds.) 9th Proceedings of the Int. Conf. on Information Systems for Crisis Response and Management, Vancouver, Canada, 2012. Simon Fraser University, Vancouver, Canada (2012)
20. MacKinnon, L.M., Bacon, L., Cortellessa, G., Cesta, A.: Using Emotional Intelligence in Training Crisis Managers: The Pandora Approach. Int. J. Distance Educ. Technol. **11**(2), 66–95 (2013)
21. Maras, M.-H.: Cybersecurity: Incident Response. In: Encyclopedia of Security and Emergency Management, pp. 197–203. Springer (2021)
22. Mossel, A., Schönauer, C., Froeschl, M., Peer, A., Göllner, J., Kaufmann, H.: Immersive training of first responder squad leaders in untethered virtual reality. Virtual Real. **25**(3), 745–759 (2021)
23. Nelson, A., Rekhi, S., Souppaya, M., Scarfone, K.: Incident response recommendations and considerations for cybersecurity risk management : a CSF 2.0 community profile. en. Tech. rep. NIST SP 800-61r3, NIST SP 800–61r3. National Institute of Standards and Technology (U.S.), Gaithersburg, MD (2025)
24. Phillips-Wren, G., Adya, M.: Decision making under stress: the role of information overload, time pressure, complexity, and uncertainty. Journal of Decision Systems **29**(sup1), 213–225 (2020)
25. Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R.G., Bonders, M.: Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach: R. Pirta-Dreimane et al. Technology, Knowledge and Learning **30**(3), 1577–1606 (2025)
26. Reittinger, T., Glas, M., Aminzada, S., Pernul, G.: Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality. In: Clarke, N.L., Furnell, S. (eds.) Human Aspects of Information Security and Assurance. HAISA 2024. Pp. 3–16. Springer (2024)
27. Saunders, T., Driskell, J., Johnston, J., Salas, E.: The Effect of Stress Inoculation Training on Anxiety and Performance. Journal of Occupational Health Psychology **1**, 170–186 (1996). https://doi.org/10.1037/1076-8998.1.2.170
28. Schramm, L.T., Lin, R., Wei, H.: Beyond Technical Training: A Cybersecurity Skills Framework for Non-Professionals. In: Riemenschneider, C.K., Sullivan, Y.W., Dinger, M., Bantan, M., Roberts, N. (eds.) Proceedings of the 2025 Computers and People Research Conference, SIGMIS-CPR 2025, Waco, TX, USA, May 28-30, 2025, 14:1–14:8. ACM (2025)

29. Steinrücke, J., Veldkamp, B.P., de Jong, T.: Determining the effect of stress on analytical skills performance in digital decision games towards an unobtrusive measure of experienced stress in gameplay scenarios. Comput. Hum. Behav. **99**, 144–155 (2019)
30. Svábenský, V., Vykopal, J., Cermák, M., Lastovicka, M.: Enhancing cybersecurity skills by creating serious games. In: Polycarpou, I., Read, J.C., Andreou, P., Armoni, M. (eds.) Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, ITiCSE 2018, pp. 194–199. ACM (2018)
31. TÜV-Süd, Nach Bränden droht die Insolvenz: So unverzichtbar ist der betriebliche Brandschutz, https://de-brandschutz-informationsportal.tuvsud.com/artikel/Branschutz-fuer-Unternehmen.html (visited on Apr. 2, 2026).
32. TÜV-Verband e.V., Jedes siebte Unternehmen gehackt – Risiken werden unterschätzt, de (2025). https://www.tuev-verband.de/pressemitteilungen/cybersecurity-studie-jedes-siebte-unternehmen-gehackt-risiken-werden-unterschaetzt (visited on Apr. 2, 2026).
33. Yazdinejad, A., Karimipour, H., Halabi, T.: Toward Stress-Adaptive Cyber Defense: Cognitive–Physiological Synchronization in IoT Environments. IEEE Internet of Things Journal **13**(7), 13832–13848 (2026)