12-7-2022

Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training

Ashley O'Neill
The University of Melbourne, oneilla1@student.unimelb.edu.au

Sean B. Maynard
The University of Melbourne, seanbm@unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Justin Filippou
The University of Melbourne, justin.filippou@unimelb.edu.au

Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training

Full research paper

Ashley O'Neill
School of Computing and Information Systems
The University of Melbourne
Parkville, Victoria, Australia
Email: oneilla1@student.unimelb.edu.au

Sean B. Maynard
School of Computing and Information Systems
The University of Melbourne
Parkville, Victoria, Australia
Email: seanbm@unimelb.edu.au

Atif Ahmad
School of Computing and Information Systems
The University of Melbourne
Parkville, Victoria, Australia
Email: atif@unimelb.edu.au

Justin Filippou
School of Computing and Information Systems
The University of Melbourne
Parkville, Victoria, Australia
Email: justin.filippou@unimelb.edu.au

Abstract

Cybersecurity Incident Response (IR) teams mitigate the impact of adverse cyber-related events in organisations. Field studies of IR teams suggest that at present the process of IR is underdeveloped with a focus on the technological dimension with little consideration of practice capability. To improve IR capabilities, we develop a scenario-based training approach to assist organisations to overcome socio-technical barriers to IR. The training approach is informed by a comprehensive list of socio-technical barriers compiled from a review of the literature. Our primary contribution is a novel meta-level framework to generate scenarios specifically targeting socio-technical issues. As a first step towards demonstrating the utility of the framework, a proof-of-concept scenario is presented.

Keywords cybersecurity, incident response, SETA, training, scenarios

1 Introduction

The threat landscape is rapidly evolving and as technologies advance, attackers find new ways to penetrate organisations' digital defences in the hopes of obtaining information or sabotaging their IT infrastructures (Ahmad et al. 2019). Much research exists into how cyber-attacks can be prevented through digital fortifications (e.g., firewalls, intrusion detection systems, and anti-malware software), but less research studies how organisations engage in incident response (IR) - the practices conducted to address breaches to the digital fortifications. Computer security IR teams are at the forefront when digital defences fail and must step in to mitigate the damage and restore services (Cichonski et al. 2012). At present, the ability of IR teams to respond to cyber-attacks is being hampered by a broad range of socio-technical issues (Ahmad et al. 2020; Nyre-Yu et al. 2019).

In this paper, we argue that IR is, at its core, a team activity. Further, that key challenges facing incident responders are the high level of complexity and dynamism in the diverse scenarios of cyber-attack environment and the socio-technical barriers to agility (Nyre-Yu et al. 2019). To address these challenges, we propose to use scenarios in the context of training towards improving IR agility as they can improve team performance in cybersecurity through building skills and identifying potential weaknesses (Brilingaitė et al. 2020; Cichonski et al. 2012; Steinke et al. 2015). We, therefore, propose the following research question: *"How can scenarios be developed to improve cyber incident response in organisations?"*

Predominantly, research on developing scenarios comes from scenario planning, where scenarios are used to aid decision-makers in dealing with uncertainty (Varum and Melo 2010), but scenario-based training (SBT) also frequently appears in the literature. In the former, scenarios are described as "a product that describes some possible future state and/or that tells the story about how such a state might come about" (Bishop et al. 2007, p. 8) and in the latter, scenarios are used as training tools to test participants (Noori et al. 2017). In comparison to scenario planning, SBT is a much less formalised process. It goes beyond exploring possible versions of the future and instead uses the scenario itself as a training tool to develop and test participants' responses to the situation unfolding (Moats et al. 2008). SBT is already evident in cybersecurity and IR, where scenarios feature heavily in best practice training guides (Guerber et al. 2010; Kick 2014). However (and not unlike scenario planning) they rarely offer much in terms of how to develop a scenario and are instead more concerned with how the training exercise is executed. By demonstrating a process for creating such scenarios, it provides organisations with guidance on how to customise scenarios for their own unique threat landscape, thus resulting in more effective training.

To answer the research question, this research develops scenarios that can improve IR capabilities by focusing on the socio-technical issues being faced by organisations. To this end, training aspects of two Event-Based Approach to Training methodologies (Nguyen et al. 2016; Oser et al. 1999) have been combined with the unique cybersecurity scenario design methodology of Guerber et al. (2010). The resulting scenarios (and training programs) will draw on the SBT foundation of using scenarios to help organisations improve their reaction to a situation by training and testing participants' responses to it.

2 Literature Review

Although the importance of IR in organisations is widely acknowledged in the literature, the discourse is largely technology-centric (Ahmad et al. 2021a). Comparatively less attention is given to socio-technical perspectives of how IR is managed in real-world practice. We abstracted the issues in the literature impacting organisational IR and grouped them by people, process, and technology.

2.1 Challenges To Address with Training

Technology plays the role of both a barrier and an enabler to IR. As sophisticated attackers find new ways to penetrate organisations' digital defences, the cybersecurity community responds by developing new tools to detect and thwart them. There is a need for better tools in IR as existing tools are highly useful but suffer from a high false positive rate and lack of usability (Tøndel et al. 2014). Issues also arise in integrating output from multiple monitoring tools to create a bigger picture. These findings were backed by Ahmad et al. (2021a) and Kotsias et al. (2022) who labelled this "poor visibility" as a key challenge and further identified a lack of optics in non-IT domains, such as HR.

Organisational processes impact both technology and people, and vice versa. Nyre-Yu et al. (2019, p. 438) note that the issues affecting IR are "more than just a set of usability issues in software, or of technology development and deployment" and instead span multiple levels of an organisational hierarchy, with each interconnected. They found that capability was constrained by whether security

was identified as a priority in the organisational mission. If not, it was seen as a competition for operational uptime and restricted growth and resources available to IR teams. Ahmad et al. (2021a) and Kotsias et al. (2022) concur and report on IR being further constrained by its positioning in IT support operations (and thus seen as a cost-centre). Similarly, Tøndel et al. (2014, p. 53) report information security (InfoSec) being "viewed merely as a technical issue". This view leads to a technology-centric focus of IR, concerned more with restoring IT services than any bigger picture at play (Ahmad et al. 2020; Ahmad et al. 2021a).

The structure of the IR team can further constrain capabilities. IR teams in Security Operations Centres are often segregated into "tiers" with members grouped together according to experience (Kotsias et al. 2022). This restricts the expertise available to each tier and hinders information sharing between analysts (Nyre-Yu et al. 2019) and leads to a culture that erodes collaboration among team members, favouring individual achievement over teamwork (Ahmad et al. 2021a). Furthermore, incidents are often escalated up the chain and sometimes out of the team altogether, limiting the authority of the IR team (Nyre-Yu et al. 2019). Relationships between team units can also impact IR capability. InfoSec management teams also appear alongside IR in large organisations. Kotsias et al. (2022) argue that these teams are often disconnected and have weak process-level integration, which leads to a fragmented approach to incidents. This is manifested in a lack of communication, collaboration, and knowledge sharing, which degrades IR capabilities and extends to other business units inside the organisation, which cumulatively can result in a "strategic-level disconnect".

From a people perspective, closely linked to the integration of teams and processes surrounding the handling of incidents, is the ability of teams to collaborate and communicate effectively. Knowledge or information sharing was a frequent issue impacting IR capabilities reported in the literature. The Ahmad et al. (2021b) case study and Kotsias et al. (2022) clinical study are unique as they label the subject organisation as exhibiting "exemplar" practices. The key reason is its ability to effectively share knowledge across its security team and wider to other IT and business units. This is not the case reflected by Nyre-Yu et al. (2019), who cite information sharing as key to developing a shared awareness of incidents across IR teams, IT, and the wider organisation. Tøndel et al. (2014) and Ahmad et al. (2021a) also cite issues with information sharing, with personnel unsure of what they should report and whom they should report it to; and a lack of formal policies on what should be shared and which communication channels to use. A poor organisational culture of mistrust between teams and fear of over-reporting incidents for who would be held responsible were also acknowledged as fuelling poor communication and collaboration (Tøndel et al. 2014). Outsourcing of services created further barriers with suppliers often excluded in many phases of IR, or unwilling to take responsibility (Tøndel et al. 2014).

Training and formal policies for effective communication and knowledge sharing are cited as ways to overcome the barriers outlined above, but they were rare in practice (Tøndel et al. 2014). Furthermore, individual awareness of InfoSec was an issue, as training tended to focus on technical staff, not all employees — this becomes an issue in IR as people (and their resulting notifications) were relied on heavily in the literature in the detection of incidents (Tøndel et al. 2014). In addition, more training was required for skills beyond that of the technical nature, as they were crucial in cybersecurity (Van der Kleij et al. 2017). The identified issues outlined above are seen in the available literature as the major challenges to IR capabilities (summarised in Table 1). It is however important to note these issues are constrained to what is presented in the research on IR, and often it is not from exemplar organisations. Furthermore, as highlighted by Tøndel et al. (2014), the data collection methods vary widely and the absence of an identified practice does not necessarily mean it is not performed, only undocumented.

2.2 Scenario-based Training for Incident Response

SBT is a term that is at times well-defined but also more loosely applied to any form of training using a scenario as the curriculum (Oser et al. 1999). SBT uses the scenario itself as a training tool to develop and test participants' responses to the situation unfolding (Moats et al. 2008). Methodologically, SBT includes a scenario design phase, the delivery of the training session and debriefing afterwards (Moats et al. 2008). A critical aspect is to start by identifying learning objectives for the training event that are observable and measurable for later stages (Cannon-Bowers 2008). One approach is the Event-Based Approach to Training (EBAT), which takes the process further and systematically introduces exercise events that map to these learning objectives, as well as participant feedback (Fowlkes et al. 1998; Nguyen et al. 2016). These linkages allow training participants to demonstrate any learning objective proficiencies (or deficiencies) and allow facilitators to measure their performance and provide future learning opportunities through feedback (Fowlkes et al. 1998).

SBT is relevant to the research question in several ways. First, the exercise is largely driven by the identified learning objectives set at the beginning, which are then mapped to trigger events in the scenario. This provides an opportunity to "set the scene" with the issues identified from the literature. Second, the methodology allows for organisational learning in the latter stages when participants' performance is measured, and feedback is offered to improve overall performance. This speaks to the research goal of improving organisational IR. Third, both SBT and EBAT are widely used to develop and test team performance (Fowlkes et al. 1998; Oser et al. 1999). The Literature identified teamwork as a critical factor in successful IR team operation. And last, SBT is primarily focused on *training*, that is, how the scenario can help organisations improve their reaction to a situation by training and testing participants' responses to it (Cannon-Bowers 2008; Moats et al. 2008). This is a critical component of this paper's aim - improving organisational IR through scenario development.

Socio-technical Barrier	**Representative Citations**
Technology complexity	Ahmad et al. (2021a), Brown et al. (2016), Tøndel et al. (2014), Van der Kleij et al. (2017)
Poor field of vision in IR teams	Ahmad et al. (2021a), Brown et al. (2016), Tøndel et al. (2014)
Lack of appropriate tools	Ahmad et al. (2021a), Brown et al. (2016), Tøndel et al. (2014), Van der Kleij et al. (2017)
Organisational positioning within IT limits IR capabilities	Ahmad et al. (2020), Nyre-Yu et al. (2019), Tøndel et al. (2014)
Segregated nature of the IR team	Ahmad et al. (2021a), Nyre-Yu et al. (2019)
Weak process-level integration between teams	Ahmad et al. (2021a), Nyre-Yu et al. (2019)
Poor fit between process and incident	Ahmad et al. (2020), Nyre-Yu et al. (2019), Tøndel et al. (2014), Van der Kleij et al. (2017)
Lack of documentation when reporting, handling, and following up incidents	Ahmad et al. (2015), Bartnes et al. (2016), Nyre-Yu et al. (2019), Tøndel et al. (2014), Van der Kleij et al. (2017)
Inadequate intra-team and inter-team collaboration and communication	Ahmad et al. (2020), Bartnes et al. (2016), Grispos et al. (2015), Hove et al. (2014), Nyre-Yu et al. (2019), Van der Kleij et al. (2017)
Insufficient training and development of information security awareness	Bartnes et al. (2016), Grispos et al. (2015), Hove et al. (2014), Tøndel et al. (2014), Van der Kleij et al. (2017)
Lack of focus on developing soft skills	Steinke et al. (2015), Van der Kleij et al. (2017)
Lack of technical expertise in IR teams	Ahmad et al. (2021a), Nyre-Yu et al. (2019), Tøndel et al. (2014)

Table 1. Socio-technical Barriers identified in the literature review

SBT is evident in cybersecurity and IR, where scenarios feature heavily in best practice training guides (Guerber et al. 2010; Kick 2014). However, they rarely offer much in terms of how to develop a scenario, being more concerned with how training is conducted. Guerber et al. (2010) is the exception and their method is the most rigorous identified for developing cybersecurity scenarios. The three phases of scenario development provide a highly detailed methodology and cumulatively is a process unlike any other identified in this research. We, therefore, conclude that SBT, and more specifically, EBAT, are highly applicable to this research. Further, the method proposed by Guerber et al. (2010) is useful in developing scenarios, but in isolation, none of these approaches fulfill the research goal of developing scenarios to address the socio-technical barriers being faced by organisational IR.

3 Methodology

We propose an adapted six-step framework (Table 2) to allow organisations to develop highly tailored scenarios of cyber-attack, but to also improve IR capabilities by utilising these scenarios in an encompassing training program. This research enables the development of scenarios that can improve IR capabilities by focusing on the socio-technical issues being faced by organisations. To this end, training aspects of two EBAT methodologies (Nguyen et al. 2016; Oser et al. 1999) have been combined with the unique cybersecurity scenario design methodology of Guerber et al. (2010). In doing so, the resulting scenarios (and encompassing training programs) draw on the SBT foundation of using scenarios to help organisations improve their reaction to a situation by training and testing participants' responses to it. Drawing on the deficiencies in current practice outlined above, we create a scenario derived from the framework (see Appendix A) to help organisations improve their IR capabilities. The

scenario is a basis for a training exercise as per the framework, but for this paper, we only focus on the scenario creation, not the training exercise. As such, the steps directly related to the exercise will be omitted (steps 5 and 6). Furthermore, the scenario will be created to be as generic as practical to allow for increased utility in organisations, but at the same time will require some constraints, namely that it is designed for organisations with large heterogeneous technology estates, spanning multiple jurisdictions. Lastly, the scenario will be developed as a tabletop exercise (TTX), one of two common SBT exercises in cybersecurity. A TTX was chosen as they are typically much shorter in duration than their functional exercise counterparts and require less planning and technical resources (Kick 2014). Table 2 outlines our proposed framework.

Scenario-development Steps	**Scenario-building Activities**
Step 1: Develop learning objectives	Identify the goals of the training program
Step 2: Craft trigger events	Provide opportunities for participants to demonstrate proficiencies/deficiencies for all learning objectives
Step 3: Develop scenario storyline	
3.1: Determine key scenario elements	Determine scenario intent, threat, target, operational effect, and business impact
3.2: Develop backstory	Develop detail of threat actors, necessary intelligence and background information
3.3: Finalise storyline	Revisit each scenario element and add in any extra storyline details
Step 4: Develop event threads	
4.1: Craft event synopsis	Craft an event synopsis by outlining the chronological event thread that will stimulate the storyline
4.2: Craft events	Fill in event details from the previous step
4.3: Event thread walkthrough	Walkthrough to flesh out final scenario details
Step 5: Identify targeted responses to events and performance measures	Identify target responses to events or measures to observe performance for evaluation and feedback
Step 6: Operationalise learnings	Put learnings from exercise into practice to improve IR

Table 2: Scenario Development Framework

4 Discussion

The following sub-sections explore each of the steps outlined above in more detail and provide an understanding for practitioners developing SBT programs on how to implement the steps for their own context.

4.1 Develop learning objectives

Step1: As this example focuses on the creation of a scenario, and not the encompassing training exercise, the issues identified from the literature review (Table 1) are used in place of learning objectives. The identification of these issues is the cornerstone of this research and by explicitly linking them to trigger events, the scenario created will exploit any deficiencies in these areas. These issues would have been turned into learning objectives if the full training framework was being followed.

4.2 Craft trigger events

Step2: We map learning objectives (or IR issues), as described in Section 2.2, to trigger events to be used in the scenario. Trigger events were identified for each issue, by drawing on the literature and our knowledge of real-world cyber incidents, which was used to link the trigger events and issues to allow the resulting scenario to expose any weaknesses that may exist in these areas. Table 3 shows the outcome of this process, with the learning objectives or issues identified in section 2 listed in the left-hand column, along with the trigger events created in this step listed in the right-hand column. The list of trigger events is not exhaustive but is a useful starting point in crafting training scenarios that address deficiencies in "best practice" IR.

4.3 Develop scenario storyline

Step 3: Adapted from the cybersecurity training methodology proposed by Guerber et al. (2010), this step has three sub-phases: determine key scenario elements; develop backstory; and finalise storyline.

4.3.1 Determine key scenario elements

In Step 3.1, the key scenario elements of scenario intent, threat, target, and operational effect are determined. A fifth key element, "business impact", is introduced which is purposely excluded by Guerber et al. (2010) but is relevant here as the context for the scenario is cybersecurity in *organisations*. The *scenario intent* is described by Guerber et al. (2010) as the overall objective of the scenario. For this research, the scenario intent is twofold: to develop a scenario that exploits the issues impacting IR capabilities; and to use such a scenario in a training exercise to help organisations to improve their IR capabilities (although this paper does not cover this).

IR Issue	**Trigger Event**
Technology complexity	*A. attack affects a high number of diverse devices*
Poor field of vision	*B. attackers employ a high volume of known attacks* *C. contradictory notifications of attack among IR tools*
Lack of appropriate tools	*D. multipronged attack whereby later attacks offer cover for earlier ones, deleting logs/evidence* *E. attacks part of infrastructure where the IR team does not have full optics because of inappropriate tools* *F. attack has a physical aspect*
Organisational positioning in IT operations	*G. attackers target non-IT services or assets, such as the business side or a business asset, a physical domain, or HR*
Segregated nature of the IR team	*H. incident responder working in isolation and does not seek team collaboration to thwart the attack* *I. attackers employ a high volume of known attacks*
Weak process-level integration between teams	*J. attackers target obscure business asset*
Poor fit between process and incident	*K. attackers misdirect the IR team to cause a misdiagnosis of incident classification*
Lack of documentation when reporting, handling, and following up incidents	*L. un- or inadequately documented information becomes relevant to the IR team*
Poor intra- and inter-team collaboration and comms	*No specific trigger. Tested in other trigger events*
Insufficient training and development of security awareness	*M. attacker targets end user, who encounters a problem they don't perceive as a threat and logs incident through help desk* *N. attackers target employee's personal device* *O. attack duration exceeds 24 hours requiring incident responders to cope with a prolonged state of "emergency"* *P. attackers target shadow IT*
Lack of focus in developing soft skills	*Q. attack puts strain on the relationship between IR and business units by targeting business only*
Lack of technical expertise	*R. IR team required to conduct forensic evidence collection*

Table 3. Mapping between IR issue and trigger events

The *threat* element encompasses both the actor and their method of attack. For this scenario, a highly sophisticated and organised attacker, who belongs to an advanced persistent threat (APT) group, was chosen over the selection of a low-skilled attacker as that would have limited the applicability of the scenario to address the range of issues identified. As they belong to an APT group they also represent the most formidable threat (Ahmad et al. 2019) and would use both known exploits and zero-day attacks in a prolonged endeavour. As this scenario is a TTX and is designed to be as generic as practical to allow for increased utility in organisations, all key scenario elements are discussed only in high-level detail. Some constraints are needed to derive a meaningful scenario, and as such, the scenario has been created from the perspective of a large organisation with a core research and development (R&D) function. An R&D organisation is an example of an organisation where it not only has IT services that could be the target of a cyber-attack, but also intellectual property (IP). In this way, the resulting scenario will exercise as many identified deficiencies as possible. It also means we can update the threat actor to be a nation-state threat actor or a competitor to the organisation — or more than likely, both.

Similarly, the *target* from a high-level perspective is the IP of the organisation, but numerous intermediary assets and services along the way will be affected in the prolonged attack, such as shadow

IT, servers, and other business assets. It is difficult to discuss targets in any finer detail, as the organisation being targeted is purely hypothetical.

Operational effect and *business impact* are clearly separated by Guerber et al. (2010) with the former relating to the effect on the target and organisation, concerning the CIA triad of confidentiality, integrity, and availability. For this scenario, as the organisation's IP is the target, the effect then becomes a total loss of confidentiality and disruption in the availability of IT services as a secondary vector in the attack. For business impact, Guerber et al. (2010) define it as the effect on the organisation's ability to carry out its mission. In this instance, the scenario has been created from the point of view of an organisation whose primary function is R&D, and as such, the theft of its IP would be catastrophic, destroying its competitive advantage at the least.

4.3.2 Develop backstory

Guerber et al. (2010, p. 34) describe this Step 3.2 as the general context or "state of the world" for the scenario and it encompasses threat actor details and necessary background information on the organisation and nation. For the context of this scenario, only high-level detail will again be provided.

The *threat actor detail* comprises both motives and level of expertise. As determined previously, the threat actor belongs to an APT group and has high levels of expertise, and the attack is a nation-state sponsored with the motive of stealing the organisation's IP to get a financial or commercial advantage. The *necessary background information* can be viewed from both inside the organisation and outside. Internally, the scenario is presented during a time of considerable growth for the organisation, where its R&D operation has expanded significantly and remains busy. This has resulted in the organisation employing new staff across the board and hiring contractors to upgrade systems in a manner to ensure minimal downtime. Externally, there is high interest in the organisation's newest developments in R&D, from both competitors and potential buyers. At the same time, the threat landscape is rapidly evolving, with highly skilled attackers increasingly going undetected.

4.3.3 Finalise storyline

Step 3.3 revisits each scenario element to add storyline details including: locations of specific systems, information or processes being targeted; the methods of discovery employed by the attacker to access a target; and an attacker's source location (see Guerber et al. (2010, p. 34) for more examples). Once again, as the scenario being developed here is based on a hypothetical organisation, it is difficult to provide such granular detail. As such, no extra information will be added to the scenario.

4.4 Develop event threads

Step 4 has also been adapted from the methodology proposed by Guerber et al. (2010) to handle TTXs. It encompasses three sub-phases: craft event synopsis; craft events; and event thread walkthrough. Cumulatively, the sub-phases are designed to develop event threads, which are chronological sets of events that relate to a specific focus area of the training program.

4.4.1 Craft event synopsis

Step 4.1 crafts an event synopsis, or multiple synapses, in the case where an exercise has multiple cyber incidents. Each event synopsis provides a chronological list of all the events that make up the cyber incident (see Guerber et al. (2010, p. 36)). As much of this phase involves the technical detail required of functional exercises, it is inapplicable here. But at a high level, it is still possible to use the list of trigger events identified in Table 3 to craft event synopses for the scenario being created. The scenario will have multiple related cyber incidents, and thus multiple synopses, to include as many of the trigger events as practical. It is impossible, however, to incorporate all of them in one cyber incident.

To craft these event synopses, selected trigger events were clustered together to form a plausible cyber incident. These trigger events were then arranged in the order they would expect to be seen in the determined cyber incident. The outcome is shown in Table 4, where each event synopsis represents one cyber incident that will be observed in the scenario.

Two or more trigger events can occur at the same time in each cyber incident, but for the purposes of the table, they are still listed one after the other. Of the 18 trigger events identified in Table 3, all but two have been included in the cyber incidents to keep the resulting scenario both plausible and to an acceptable length. The two that were excluded, however, map to issues that are already represented in the included 16 trigger events, so no issue has been left out of the resulting scenario.

4.4.2 Craft events

Step 4.2 exists to fill in the event details from the previous step. For each event synopsis outlined in Table 4, a storyline has been crafted to utilise the respective event triggers.

4.4.3 Event thread walkthrough

Step 4.3 is a walkthrough of the scenario to flesh out the final details. It is a team exercise and Guerber et al. (2010) identify it as the most time-consuming phase of scenario development. Expected responses from players are also included in this sub-phase, however, for the proposed framework, it is included in Step 5 in keeping with the EBAT methodologies.

Trigger Event	Story Line
Event synopsis 0	
G. attackers target a non-IT service or asset, such as the business side or a business asset, a physical domain, or HR F. attack has a physical aspect	• a new hire at the organisation is actually working for the attackers • attackers gain physical access to systems being upgraded by posing as contractors
Event synopsis 1	
P. attackers target shadow IT N. attackers target employee's personal device M. attacker targets end user, who then encounters a problem they don't perceive as a threat and logs incident through help desk L. un- or inadequately documented information becomes relevant to the IR team R. IR team required to conduct forensic evidence collection	• attackers compromise an R&D worker's personal device in the hunt for IP • R&D worker doesn't realise as they lack InfoSec awareness and instead log resulting technical issues through the help desk • IR team eventually detects the incident but must deal with a lack of information and processes around personal devices
Event synopsis 2	
G. attackers target non-IT service or asset, such as the business side or a business asset, a physical domain, or HR J. attackers target obscure business asset K. attackers misdirect the IR team to cause a misdiagnosis of incident classification Q. attack puts strain on relationship between IR and business units by targeting business only R. IR team required to conduct forensic evidence collection	• attackers take the R&D server offline (along with others) to hide the theft of IP • IR team must decide between focusing on restoration or exploring the root cause of the incident
Event synopsis 3	
B. attackers employ high volume of known attacks I. attackers employ high volume of known attacks C. attack results in contradictory notifications among IR tools O. attack duration exceeds 24 hours requiring incident responders to cope with a prolonged state of "emergency"	• attackers launch a high-volume attack designed to confuse and fatigue incident responders and provide cover via misdirection/interference • IR team cannot cope with the sustained increase in volume, and it impacts team culture
Event synopsis 4	
A. attack affects a high number of diverse devices C. attack results in contradictory notifications among IR tools D. attack is multipronged, whereby later attacks offer cover for earlier ones, deleting logs and forensic evidence	• attackers launch a large-scale attack, e.g. distributed denial of service, to wipe out any evidence left behind • notifications confuse incident responders as to the motives of the attack, tools give conflicting messages • IR team must decide between focusing on restoration or exploring the root cause

Table 4. Event Synopsis

In the context of the scenario being developed here, the storylines have been "fleshed out" with finer details to create a cumulative scenario of five incidents or event threads. The scenario has been presented

as a TTX (Appendix A), consistent with best practice guidelines (Guerber et al. 2010; Kick 2014) and examples of TTXs found online (e.g. WSOC (2014)).

5 Conclusion

Returning to the research question of "how can scenarios be developed to improve cyber incident response in organisations?", the first part of the research identified a comprehensive list of socio-technical issues facing organisational IR through the literature review. The second part of the research identified a lack of an appropriate methodology to develop scenarios to address these issues, and as such, proposed a new framework that is rooted in the previous work of EBAT and best practice cybersecurity guidelines. A scenario was then created from this framework, which systematically mapped the socio-technical issues identified in the first part of the research to events in the resulting scenario. Owing to the previous work on the utility of EBAT and SBT overall, it is argued that such a scenario would not only enable organisations to assess their IR capabilities but also improve them by following the extra steps to implement the encompassing training program.

5.1 Significance

This research is significant to both the practice and theory of IR. The meta-level framework developed, the proof-of-concept scenario, the comprehensive list of socio-technical issues, and the event triggers derived from them, all take strides to address a real-world problem. That is, organisations cannot currently carry out effective IR as the process is technology-focused and underdeveloped. By focusing on the socio-technical barriers we argue organisations can improve their IR capability.

This research is significant to practice as it provides organisations with a ready-made scenario to improve IR capability and teaches them how to create their own. The framework developed and the two "ingredients" created – the list of IR deficiencies and the event triggers derived from them – combine into a training tool that, to the best of our knowledge, is the first of its kind in cybersecurity. It targets the socio-technical barriers impacting IR teams, allowing organisations to assess whether they are facing the same issues. But the framework doesn't solely rely on these barriers — it is flexible enough to allow organisations to choose specific deficiencies to focus on, or they can create their own learning objectives. The encompassing training program leads to better-aligned outcomes for IR and all six areas of InfoSec management: IR; policy; risk management; education, training, and awareness; technical management; and intra-organisation liaison management (Alshaikh et al. 2014; Lim et al. 2012; Maynard et al. 2011). From a theory perspective, the research addresses a literature gap with no comparable methodology identified for organisations to develop scenarios (and resulting training programs) that target socio-technical issues. The training framework draws on established methodologies to systematically link the socio-technical issues with events in the resulting scenario. The comprehensive range of deficiencies we identified consolidates the available literature on IR practice, which is at present dispersed and disconnected. New research regarding the study of IR in practice is needed. Furthermore, IR literature on socio-technical issues is lacking, with the focus currently mainly on technology aspects of IR.

The foundation of this research is the literature contribution. The results are influenced by not only what was *available*, but also the *scope* of such literature and the *context* of the organisations studied (e.g., typically not exemplar organisations). Research is needed into the real-world practice of IR to remedy this. Further, data collection methods vary widely in the literature. The absence of an identified practice does not necessarily mean it is not performed, only undocumented (Tøndel et al. 2014).

5.2 Limitations

The project was subject to several limitations. First, the scenario was a hypothetical rather than an actual organisation. Second, the proof of concept was focused on scenario creation rather than the training program. The framework needs to be tested and implemented by organisations, creating not only a scenario driven by socio-technical issues but an encompassing training program to operationalise learnings from the scenario. The results would enable researchers to measure the effectiveness of the framework towards improving organisational IR.

The research presents opportunities for future work. First, case study research is needed to examine the practice of IR teams towards understanding the socio-technical challenges of organisational IR. It could do this by both confirming or denying the presence of the issues identified in this literature review and identifying new issues. Second, the framework could be extended for use in functional cybersecurity exercises as well as discussion-based ones like TTXs. Last, the suggested list of event triggers could be enhanced through greater research into past cyber-attacks, bringing more depth to the scenarios.

6 References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., and Baskerville, R. L. 2020. "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning," *Journal of the Association for Information Science & Technology* (71:8), pp. 939-953.

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., and Baskerville, R. L. 2021a. "How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice," *Computers & Security* (101).

Ahmad, A., Maynard, S. B., Motahhir, S., and Anderson, A. 2021b. "Case-Based Learning in the Management Practice of Information Security: An Innovative Pedagogical Instrument," *Personal and Ubiquitous Computing* (25:5).

Ahmad, A., Maynard, S. B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management* (35:6), pp. 717-723.

Ahmad, A., Webb, J., Desouza, K. C., and Boorman, J. 2019. "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," *Computers & Security* (86), pp. 402-418.

Alshaikh, M., Ahmad, A., Maynard, S. B., and Chang, S. 2014. "Towards a Taxonomy of Information Security Management Practices in Organisations," *25th Australasian Conference on Information Systems*, Auckland, New Zealand, p. 10.

Bartnes, M., Moe, N. B., and Heegaard, P. E. 2016. "The Future of Information Security Incident Management Training: A Case Study of Electrical Power Companies," *Computers & Security* (61), pp. 32-45.

Bishop, P., Hines, A., and Collins, T. 2007. "The Current State of Scenario Development: An Overview of Techniques," *foresight*).

Brilingaitė, A., Bukauskas, L., and Juozapavičius, A. 2020. "A Framework for Competence Development and Assessment in Hybrid Cybersecurity Exercises," *Computers & Security* (88), p. 101607.

Brown, J. M., Greenspan, S., and Biddle, R. 2016. "Incident Response Teams in It Operations Centers: The T-Tocs Model of Team Functionality," *Cognition, Technology & Work*:4), p. 695.

Cannon-Bowers, J. A. 2008. "Recent Advances in Scenario-Based Training for Medical Education," *Current Opinion in Anesthesiology* (21:6), pp. 784-789.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. "Computer Security Incident Handling Guide," NIST.

Fowlkes, J., Dwyer, D. J., Oser, R. L., and Salas, E. 1998. "Event-Based Approach to Training (Ebat)," *The international journal of aviation psychology* (8:3), pp. 209-221.

Grispos, G., Glisson, W. B., and Storer, T. 2015. "Security Incident Response Criteria: A Practitioner's Perspective," *arXiv preprint arXiv:1508.02526*).

Guerber, A., Fogle, C., Roberts, C., Evans, C., MacDougald, B., and Butkovic, M. 2010. "Methods for Enhanced Cyber Exercises." Carnegie Mellon University.

Hove, C., Tarnes, M., Line, M. B., and Bernsmed, K. 2014. "Information Security Incident Management: Identified Practice in Large Organizations," *IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on*, pp. 27-46.

Kick, J. 2014. "Cyber Exercise Playbook," MITRE Corp, Bedford MA, USA.

Kotsias, J., Ahmad, A., and Scheepers, R. 2022. "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation," *European Journal of Information Systems*), pp. 1-17.

Lim, Chang, S., Ahmad, A., and Maynard, S. 2012. "Towards an Organizational Culture Framework for Information Security Practices," in *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*. IGI Global, pp. 296-315.

Maynard, S. B., Ruighaver, A. B., and Ahmad, A. 2011. "Stakeholders in Security Policy Development," *Proceedings of the 9th Information Security Management Conference*, Perth, Australia: Edith Cowan University, pp. 182-188.

Moats, J. B., Chermack, T. J., and Dooley, L. M. 2008. "Using Scenarios to Develop Crisis Managers: Applications of Scenario Planning and Scenario-Based Training," *Advances in Developing Human Resources* (10:3), pp. 397-424.

Nguyen, N., Watson, W. D., and Dominguez, E. 2016. "An Event-Based Approach to Design a Teamwork Training Scenario and Assessment Tool in Surgery," *Journal of surgical education* (73:2), pp. 197-207.

Noori, N. S., Wang, Y., Comes, T., Schwarz, P., and Lukosch, H. K. 2017. "Behind the Scenes of Scenario-Based Training: Understanding Scenario Design and Requirements in High-Risk and Uncertain Environments," *ISCRAM*, pp. 948-959.

Nyre-Yu, M., Gutzwiller, R. S., and Caldwell, B. S. 2019. "Observing Cyber Security Incident Response: Qualitative Themes from Field Research," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*: SAGE Publications Sage CA: Los Angeles, CA, pp. 437-441.
Oser, R. L., Gualtieri, J. W., Cannon-Bowers, J. A., and Salas, E. 1999. "Training Team Problem Solving Skills: An Event-Based Approach," *Computers in human behavior* (15:3-4), pp. 441-462.
Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., Zaccaro, S. J., Dalal, R. S., and Tetrick, L. E. 2015. "Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research," *IEEE Security & Privacy* (13:4), pp. 20-29.
Tøndel, I. A., Line, M. B., and Jaatun, M. G. 2014. "Information Security Incident Management: Current Practice as Reported in the Literature," *Computers & Security* (45), pp. 42-57.
Van der Kleij, R., Kleinhuis, G., and Young, H. 2017. "Computer Security Incident Response Team Effectiveness: A Needs Assessment," *Frontiers in psychology* (8), p. 2179.
Varum, C. A., and Melo, C. 2010. "Directions in Scenario Planning Literature–a Review of the Past Decades," *Futures* (42:4), pp. 355-369.
WSOC. 2014. "Tabletop Exercises," Washington State Office of Cybersecurity, Washington Technology Solutions.

7 Appendix A: Proof-of-Concept Scenario

Preamble: Your organisation has just gone through a period of considerable growth within its R&D operations, hiring new staff across the board and employing contractors to upgrade systems both virtually and physically. The organisation is gaining a lot of attention for its recent developments and there is plenty of interest in the work currently being undertaken. At the same time, cyber threats are rapidly becoming realised, with highly skilled attackers successfully penetrating well-respected organisations and operating for quite some time undetected.

***First Scenario**:* An R&D employee working from home on their personal laptop notices their computer acting oddly. It is late at night, they are fatigued from a busy period at work, but they try everything they can think of to fix this issue themselves. Eventually, they concede it is beyond their capabilities and retire for the night. The next morning when they clock on at work, they contact the organisation's help desk from their employee laptop, which works just fine. **Question:** How would you respond?

***Optional inject**:* Upon escalation to the IR team, it is revealed the employee was the victim of a social engineering attack, where they clicked on an attachment in a spear phishing email to their work address. **Question:** Does this new information change your earlier response? If yes, how so?

***Optional inject**:* The IR team now requires physical access to the compromised laptop. The employee is uncontactable, and the laptop remains at their house. **Question:** How would you respond?

***Second Scenario**:* It is a long weekend; a few staff are at work when several servers stop responding. Calls are placed to the help desk from a selection of the skeleton staff, including a business executive, an R&D employee, and a call centre worker, frustrated as they cannot do their job while the servers are offline. **Question:** How would you respond?

***Optional inject**:* One of the server asset owners has not been contactable for three days. **Question:** Does this new information change your earlier response? Explain.

***Third Scenario**:* The IR team has noticed an increase in the volume and frequency of known, low-impact attacks. It is unclear what the reason for the increase is. **Question:** How would you respond?

***Optional inject**:* The high frequency of attacks continues beyond 24 hours and level two analysts are assisting fatigued junior employees to manage the workload. Some staff members are beginning to become disgruntled at the extra "trivial" work and voice their grievances, not the least of which is missing the send-off afternoon tea for a valued staff member. **Question:** How would you respond?

***Fourth Scenario**:* It is Friday afternoon – the end of the work-week when a large-scale distributed denial of service attack hits the organisation. IT systems are crippled, including communication channels such as email and mobile phones. **Question:** How would you respond? What takes first priority?

***Optional inject**:* Systems are restored, and services are beginning to be recovered across the organisation. **Question:** What happens next?