Scenario-Based Incident Response Training: Lessons Learnt from Conducting an Experiential Learning Virtual Incident Response Tabletop Exercise.

Journal:	*Information and Computer Security*
Manuscript ID	ICS-05-2022-0085.R2
Manuscript Type:	Original Article
Keywords:	Incident Response, Virtual Incident Response Tabletop Exercise, Disaster Recovery, Cyber Security, Scenario-Based Learning, Experiential Learning

Scenario-Based Incident Response Training: Lessons Learnt from Conducting an Experiential Learning Virtual Incident Response Tabletop Exercise.

Abstract:

Purpose - *This paper discusses our experiences designing and conducting an experiential learning virtual incident response tabletop exercise (VIRTTX) to review a business's security posture as it adapts to remote working because of the Coronavirus 2019 (COVID-19). The pandemic forced businesses to move operations from offices to remote working. Given that this happened quickly for many, some firms had little time to factor in appropriate cyber-hygiene and incident prevention measures, thereby exposing themselves to vulnerabilities such as phishing and other scams.*

Design/methodology/approach - *The exercise was designed and facilitated through Microsoft Teams. The approach employed included a literature review and an experiential learning method that used scenario-based, active pedagogical strategies such as case studies, simulations, role-playing, and discussion-focused techniques to develop and evaluate processes and procedures used in preventing, detecting, mitigating, responding, and recovering from cyber incidents.*

Findings – *The exercise highlighted the value of using scenario-based exercises in cyber security training. It elaborated that scenario-based incident response (IR) exercises are beneficial because well-crafted and well-executed exercises raise cyber security awareness among managers and IT professionals. Such activities with integrated operational and decision-making components enable businesses to evaluate IR and disaster recovery (DR) procedures, including communication flows, to improve decision-making at strategic levels and enhance the technical skills of cyber security personnel.*

Originality - *This paper underlines the importance of practical, scenario-based cyber-IR training and reports on the experience of conducting a virtual IR/DR tabletop exercise within a large organisation.*

Keywords: Incident Response, Virtual Incident Response Tabletop Exercise, Disaster Recovery, Cyber Security, Tabletop Exercises, Scenario-Based Learning, Experiential Learning

1. Introduction

The coronavirus 2019 (Covid-19) pandemic forced many businesses to move operations from office premises to remote working. The migration of entire workforces from offices to homes for many happened quickly. Within a short period, and often under stressful and demanding circumstances, businesses increased their capacity and capabilities for remote working. In accelerating their digital transformation, companies had little or no time to factor in appropriate cyber-hygiene and incident prevention measures (Freedman, 2021). Nabe (2020) and Alawida (2022) share this view, maintaining that cyber security is not always seen as a critical priority in the fast deployment of remote working capabilities. The researchers noted that in responding to the COVID-19 pandemic, many organisations either consciously or inadvertently did not provide a 'cyber-safe' remote-working environment for their staff. Wang (2021) holds that this lack of security awareness and training and the absence of proper cyber security measures during the COVID-19 pandemic posed various challenges for employers and their employees. Gafni & Pavel (2022) share this view, maintaining that there was an increase in cyber security attacks of diverse kinds, such as phishing, malspams and ransomware attacks, during the first wave of the pandemic in 2020. They argue that attacks targeted many businesses and end-users, including the healthcare sector. Additionally, pharmaceutical companies and their staff working remotely became a target for malicious actors, with many falling victims to such cyberattacks (Gafni & Pavel, 2022). In a study focusing on the cyber security behaviours of remote workers during the COVID-19 pandemic, Alawida et al. (2022) found that staff displayed a lax and even risky attitude toward cyber security.

One such risky behaviour was sharing company devices with family members, with over a fifth of survey participants, 22 per cent, stating that they allowed others to use their devices and ignored how they used them Wang & Alexander (2021). Another 44 per cent of participants indicated that they had used work-issued devices daily for personal matters since the start of COVID Wang & Alexander (2021). Such risky behaviours from home workers, coupled with the lack of proper security measures put in place by some businesses during the pandemic and the intelligence and persistence of threat actors, made businesses and their staff susceptible to cyber-attacks. Companies must introduce their entire workforce to good cyber security practices to deal with these challenges and minimise the risks to users and businesses. One such measure is cyber security awareness training, which according to Wilson & Hash (2003 p.7), can help staff gain essential knowledge on how to identify simple but effective security threats such as social engineering scams, recognise phishing and detect spam websites. In this paper, we articulate some cyber security challenges businesses working remotely experienced during the pandemic. We discuss why investing in appropriate cyber security preventative measures, such as IR and DR awareness training, is essential. We also elaborate on our experience designing and conducting a virtual incident response scenario-based tabletop exercise (VIRTTX) for IR/DR training geared towards assisting our business in assessing processes and procedures for preventing, detecting, mitigating, responding to, or recovering from cyber incidents is also discussed.

1.1 Motivation

This study examines cyber security challenges, such as the lack of adequate cyber security awareness training and the increased cyber-attacks faced by businesses and their staff while working remotely during the COVID-19 pandemic. We used a cyber threat scenario that mimicked a real-world threat that employees may face in their specific roles and proposed possible solutions to some of the challenges highlighted. The practical, real-life learning scenario encouraged participants to learn from the initial experience, assess their knowledge, and develop and retain necessary skills. It also enabled them to use existing multimedia applications such as MS Teams to harness strategies to detect and prevent future threats during challenging circumstances such as the COVID-19 outbreak.

The rest of the paper is structured as follows; section 2 provides a background to the study, while section 3 outlines the methodology employed in the article. Section 4 gives an overview of VIRTTX, including a detailed presentation of the scenario and how it was conducted. Section 5 discusses the literature's findings and explains how the virtual scenario-based tabletop discussion exercise helped tackle remote working challenges. Section 6 presents the study's practical and academic implications and the conclusion and offers pointers to future work.

2. Background

In a recent study, Gafni & Pavel (2022) noted that the COVID-19 pandemic forced most of the working force in the world to shift from the customary workplace to a home or remote working environment. Similarly, research on the challenges facing remote workers by Nabe (2020) found that the increased reliance on remote working calls for a greater focus on cyber security because of greater exposure to cyber risks. The study established that 47% of individuals surveyed fell victim to phishing scams while working remotely during the COVID-19 pandemic. This indicates that threat actors are taking advantage of the pandemic, especially since businesses are relying on a remote workforce as an opportunity to step up their criminal activities. Nabe (2020) maintained that cybergangs took advantage of this and embarked on exploiting unsuspecting employees working from home. Security researchers established that cybercriminals capitalised on people's strong interest in coronavirus-related news to set up links to files and malicious websites. Once these hyperlinks were clicked, threat actors took advantage to either install malware or harvest the credentials of their victims (Nabe, 2020) and Wang & Alexander (2021).

Furthermore, Gafni & Pavel (2022) found that many remote workers did not have relevant home working security knowledge. Some were not trained about cyber security risks associated with remote working, while others did not feel confident about cyber protection. Similarly, a survey of cyber security awareness training, including during the pandemic, found that decision-makers recognise that security awareness training, especially IR/DR training is a cheaper option. It argues that it was a better way to deal with increasing cyber security threats. However, it is often ignored (Georgiadou et al., 2022). The study maintained that employees are either not given adequate training or that the training is not frequent enough, given the ever-changing cyber security landscape. Moreover, many businesses failed to advise, enforce, and train their workforce during COVID-19. They argue that during this period, cybercrimes spiked, with security threats, frauds and breaches targeting medical facilities and home workers, making it incredibly demanding, stressful and worrisome Georgiadou et. (al, 2022). On the other hand, a survey by Chouliaras et al. in (2021) showcased that most current cyber ranges are moving towards more realistic and competitive scenarios that can help users receive focused experiential learning. Based on these findings, we designed and conducted a virtual security awareness training to review our business' security posture in the wake of the new ways of working in response to the COVID-19 pandemic.

This paper presents our experience conducting a virtual scenario-based cyber incident response training during the era of remote working caused by COVID-19. 'Scenario-based learning' (SBL), called 'case-based learning', is an experiential learning approach that uses interactive scenarios to support active learning strategies (Stewart, n.d). Most SBL activities require students, learners, or participants to work through a scenario or storyline. SBL storylines are typically based on a complex problem that learners must solve. Stewart (n.d) maintains that throughout the SBL process, learners must apply their subject knowledge and critical thinking or problem-solving skills in a safe, real-world context. The remote scenario-based exercise in VIRTTX was conducted through Microsoft Teams, often called MS Teams.

Teams is a contemporary multimedia web conferencing application (CMWCA). Though not new or unique, MS Teams is described as a 'contemporary multimedia or an ultra-modern web conferencing application' because it is one of those applications that make use of present-day technologies and ideas which set them apart from traditional conferencing applications. MS Teams is hosted entirely over the Internet so that participants do not need to get together in a physical conference room. CMWCAs allow remote participants to participate in live onsite meetings and events from their computers, mobile phones, or tablets from diverse geographical locations (Brown, 2021). They are called CMWCAs because participants can use various media sources for communication, such as video, voice, and chat. During multimedia virtual conferences, participants can easily join through a conference website or video conferencing applications designed specifically for the virtual experience. Due to the ever-increasing threat landscape, with attacks such as phishing, malware, and ransomware, coupled with the fact that since 2019 it is near impossible to organise in-person, hands-on cyber-IR/DR exercises due to the pandemic, APMG International (2021), this paper sets out to summarise how we conducted a remote cyber security awareness training using MS Teams and elaborate on the outcome of our training exercise. It details how through this practice-based VIRTTX, we brought staff together from across a large business to use a scenario-based experiential learning approach to evaluate existing IR/DR processes to determine if they are fit for purpose. It enabled them to establish current gaps and identify strategies to prevent future threats during challenging circumstances such as the COVID-19 outbreak.

Due to technological advances like the Internet and mobile connectivity, more people, businesses, and governments are increasingly going digital. While this is good for business, it also poses many challenges (Angafor et al., 2020). One such obstacle is the fast-evolving cyber security threat landscape, with attacks on networks and data breaches growing in number and sophistication (Angafor et al., 2020). The problem is further compounded by the fact that there is a shortage of experienced personnel with the right skills to defend against incidents resulting from increased connectivity and the continually evolving threat landscape (Angafor et al., 2020). Horne (2014) corroborates this view, maintaining that many industries have a diverse cyber talent deficit. Moreover, he argues that threat actors are amazingly coordinated while there is a cyber security staff shortage (Horne, 2014). Due to this talent shortage and the sophisticated nature of modern attacks, government agencies and businesses are struggling to defend themselves against phishing scams, data breaches, denial-of-service (DDoS) attacks, ransomware, and other threats of a similar nature (Lyon, 2020).

This exponential growth and expansion of digital services offerings, according to Tobarra et al. (2020) and the lack of skilled cyber security professionals to effectively secure these platforms provide opportunities for threat actors, especially serious organised transnational crime syndicates (Angafor et al., 2020). It enables them to exploit loopholes in business networks, often-breaching customer data, trade, and other secrets Angafor et al. (2020) and (Tobarra et al., 2020). One such infringement of international proportion was the 2017 "WannaCry" ransomware attack, which affected over 250,000 computers in more than 150 countries. In this attack, a cybercrime gang encrypted victim files and demanded payment in cryptocurrency as a condition for the release of the files (Fordoński & Kasprzak, 2019, p.47). Threat actors are constantly succeeding in breaching cyber defences by switching and adapting to new tactics, techniques, and procedures (ENISA, 2020). Their ability to change and adapt to new tricks, often covering their paths to avoid being caught, makes it difficult for businesses already struggling to hire and retain qualified cyber security personnel (Vogel, 2016).

Many government bodies, such as the UK parliament and security scholars, such as Angafor et al. (2020) and Borges et al. (2021), have called for increased uptake in cyber security education and training to meet the talent shortfall. Despite that, researchers like Hadley (2019) hold that teaching and training methods in cyber security courses have continued to lag, failing to keep pace with the technology development and deployment rate, which gives threat actors an advantage. Furthermore, FitzGerald (2019) contends that current training often focuses on the wrong skills, with some courses concentrating on skills in the hacking domain while not paying attention to controls such as business processes. Hadley (2019) supports this view, stating that education and training providers emphasise training certificates and academic qualifications over practical hands-on experience, which is more valuable in the workplace. In line with such findings, Beyer et al. (2015) maintain that although higher education and training institutions have invested in and improved their cyber security courses, a gap remains between the knowledge and skills graduates possess and those employers seek. In the same light, Angafor et al. (2020) established that while some graduates lacked essential hands-on skills required by hiring managers, many struggled to explain the goal of cyber during interviews. In addition, Vogel (2016) noted that some businesses, especially their human resource departments, argued that formal education programs did not appropriately prepare students for cyber security careers. This lack of employability skills from graduates and the continually changing threat landscape prompted security professionals and academics associations like the Business-Higher Education Forum (2017 p.22); Hadley (2019); FitzGerald (2019), and Angafor et al. (2020) to argue that cyber security training should provide opportunities for students to gain practical skills through experiential learning approaches such as serious games, tabletop exercises (TTX) or (TTEs) and other scenario-based simulations.

TTEs or TTXs are discussion-based exercises where team members meet in an informal setting to discuss different risk scenarios. A TTX focuses on existing plans, policies, mutual aid agreements, and procedures used among multiple agencies (US Homeland Security, 2021). They enable organisations to review, discuss and assess their emergency preparedness and response capabilities in an informal, low-stress environment. Wendelboe et al. (2020) maintain that they are designed to simulate cyber and other emergency scenarios and are used as a tool to address some or all the phases of emergency management: such as mitigation, preparedness, response, and recovery. Garzón & Garzón (2020) assert that a TTX or TTE presents a realistic cyber security incident scenario to which an enterprise must respond. They maintain that TTX participants review scenarios and describe how they would react during the incident, what tools they would use and what procedures they would follow (Garzón & Garzón, 2020).

TTXs are designed to include the participation of stakeholders from diverse and complementary departments, such as command, operations, logistics, planning, and finance. Effective TTXs provide practical, real-life scenarios that require cooperation and communication from these functional areas (Angafor et al., 2020) and (Wendelboe et al., 2020). They can provide a basis to help decision-makers anticipate future challenges, which may provide the mental model encompassing knowledge, skills, and insights that inform current and future emergency management decisions (Wendelboe et al., 2020). Garzón & Garzón (2020) posit that at the end of the exercise, participating businesses can determine where their incident response plans and policies are working well, where there is room for improvement, and how they can refine their cyber incident response plans. Angafor et al. (2020) hold that TTXs may involve simulations, role-playing, and other exercises in both digital and non-digital forms designed for use by single or multiple participants. According to Madani et al. (2017), Angafor et al. (2020), and Marome et al. (2021), TTXs enable interactive storytelling. They allow participants to use examples of real-life scenarios to simulate actions where they may be faced with circumstances that require them to think critically and analyse issues from a new perspective. They help participants to review and reconsider their actions, the consequences, and the roles they may play in the face of different situations.

Security training, including IR/DR courses, have often occurred in in-person settings such as classrooms or physical training spaces like IT department laboratories. Such as collaborative IR/DR TTXs, which Chang & Hwang (2019) and Sena et al. (2021) argue enable teaching to be conducted as practical, team-based, collaborative exercises. During these exercises, participants undertake incident preparedness activities that provide opportunities to experience how to manage security incidents in real-time. The tabletop training exercise discussed in this paper is a virtual or remote exercise. It is based on a simulated, real-life scenario, which takes participants through a systematic approach to dealing with incidents through MS Teams, a contemporary web conferencing application (CWCA) with video and voice conferencing capabilities. The virtual exercise encourages teamwork and group problem-solving skills, allowing the testing and evaluation of IR/DR plans and procedures. The exercise encourages participants to learn from and react to threat actors' strategies and actions, such as adversaries, helping them learn to collaborate and share information needed to manage incidents in a real-life situation (Abbott, 2018).

3. Methodology

3.1 Research Questions

The specific research questions that this study seeks to address are as follows:

RQ1: What are some cyber security challenges encountered by remote workers during the COVID-19 pandemic?

RQ2: Can a virtual IR tabletop training exercise improve the cyber security challenges experienced by remote workers during the COVID-19 pandemic?

To address the queries raised by the research questions, a twofold approach was employed. The first stage involved a literature review. In stage two, we applied an experiential learning approach that used a practical, scenario-based tabletop exercise in which participants reviewed a real-life incident and discussed strategies to manage the challenges posed by the pandemic.

3.2 Literature review methodology.

To answer RQ1 and RQ2, we conducted a literature review using a ‘keyword search’ strategy. In his guide for conducting literature reviews, Okoli (2015) maintains that a literature review should ensure vigour and adequate documentation of the review process, including the details of the search process. The keyword search in this study targeted traditional academic data sources, including bibliographic databases supplemented by a generic web search. The generic web search enabled us to gather relevant ‘grey literature’. Grey literature is material issued external to the traditional academic commercial and circulation networks (Khurshid et al. (2021). Grey literature incorporates vast collections of papers and documents such as case reports, policies, ethical and practice guidelines, theses, dissertations, conference abstracts, newsletters, and Blogs. Grey literature contributes to research by providing current updates on scientific research interventions and developments in various fields of study, thereby reducing publication bias (Khurshid et al., 2021). Overall, 58 papers were used in our study. The Data collection and systematisation process is summarised in table 1 below.

Item	Description
Research Strings	String 1:TTEs or TTXs String 2: "Virtual Conference" or "Virtual Training Exercises" String 3: "Incident Response Training" String 4: "Cybersecurity and "Coronavirus" or ''COVID-19 pandemic" or ''coronavirus crisis and network security." String 5: "Digital services" or "Digitisation." String 6: "Cybersecurity Skills shortage" or "Skills gap in cybersecurity."
Online Databases	IEEE ScienceDirect Emerald Insight SCOPUS Google Scholar Springer Elsevier Taylor and Francis, World of Science (WoS) ACM Digital Library Others include a resources list from COVID-19 research journals, websites, and bibliographies
Period of search	March 2022 to January 2023
Area of research	Incident Response Training and Cyber-attacks and COVID-19 crisis
Language	English
Documents	Articles and Reviews and Editorials

Table 1: Data collection and systematisation

The database searches returned 117 articles initially reviewed by abstract, and papers that were unclear or required further analysis were reviewed in full. The full-text review found that 39 articles did not discuss the subjects in the keywords used for the search in dept and were therefore eliminated. We reviewed the remaining 78 articles and established that 11 addressed the topic of virtual reality rather than the subject of virtual conferences and virtual training exercises. At the same time, another 9 concentrated on physical exercises. This process left us with 58 articles that were found relevant for inclusion in the paper.

3.3 Outcomes of the Practical Experiential Learning Exercise

The approach employed in the practical, hands-on scenario is an experiential learning approach. Experiential learning is an educational approach that integrates theoretical and practical learning elements and emphasises the importance of experience for learning. Murray (2018) maintains that learning centres on scenario-based, active pedagogical strategies such as simulations, role-playing, practical hands-on experiences, and case studies. The experiential learning approach also encompasses problem or inquiry-based learning and concept mapping to engage students in the learning process. Murray (2018) elaborates that Dewey brought experiential learning as a methodology to prominence in 1938 by asserting that learning occurs through experience. This theory was further refined by Kolb (1984 p.26), who stated that learning is created through the transformation of experience. Both hypothesised that experiential learning differed from other types of learning used in the classroom in that it was learning that occurred during and from experience. It is the knowledge that involves learners in concrete activities, and such knowledge enables them to experience what they are learning. This type of learning requires processing knowledge and skills through experience, reflection, experimentation, and application (Murray, 2018).

Unlike traditional classroom-based learning with passive activities that include didactic lectures, memorisation and note-taking, experiential learning is an active, learner-centred process. The experiential learning approach provides learners with practical knowledge, activities, and experiences to apply to their work environment. Wingfield and Black (2005) elaborate that experiential learning activities like case studies, simulations, role-play, and problem-based learning allows learners to interact with peers and learn through 'other means' and enable instructors to meet various learning needs or styles. It allows for personal interactions, communication and socialisation between learners, their peers, and the phenomena they may encounter in a real-life professional setting. Figure 1 below outlines the experiential learning methodology used in VIRTTX.

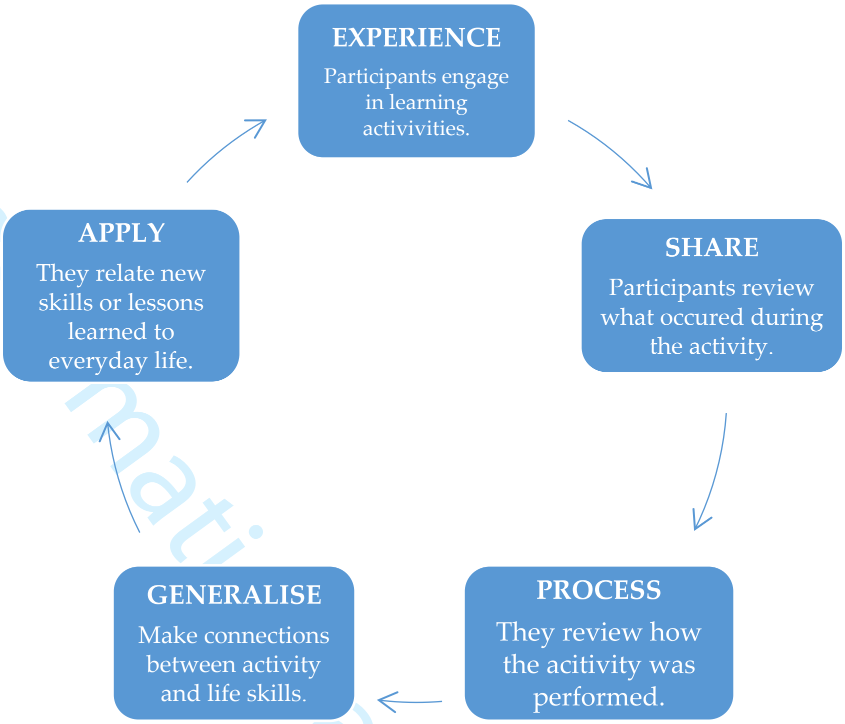

EXPERIENCE
Participants engage in learning activivities.
SHARE
Participants review what occured during the activity.
PROCESS
They review how the acitivity was performed.
GENERALISE
Make connections between activity and life skills.
APPLY
They relate new skills or lessons learned to everyday life.

Figure 1: A diagrammatic representation of the experiential learning methodology.

To implement the practical, experiential learning approach, see figure 1 above; we used a cyber threat scenario that mimicked a real-world business problem that employees may face in their specific roles. Through a facilitated discussion, we engaged participants to reflect on what was unfolding from the progressive incident taking note of how they would address it. Once they had discussed and reflected on different approaches to dealing with the situation, participants were encouraged to review their responses and think about what they could do to improve them. The study challenged them to produce a plan of action that included new ideas or what they would do differently if they were to respond to the scenario again. By doing this, the practical, real-life learning scenario encouraged participants to learn from the initial experience, assess their knowledge practically, and then develop and retain necessary skills (Kolb, 1984 p.36).

This experiential learning approach is deemed appropriate for our VIRTTX because experiential learning is helpful for work-based learning. It facilitates practical education and teaching. It enables communications and collaborative capabilities through the discussion of a plausible scenario and the sharing of observations. The Department for Homeland Security, DHS (2011) maintains that experiential learning is helpful for on-the-job training as it uses realistic exercise scenarios. It adds that such scenarios enable businesses to assess actual response processes and procedures, seeking to identify lapses in operating procedures and implement necessary improvements to the process. Besides, it helps companies review existing emergency

IR/DR controls to identify gaps and enhance response capabilities (Garzón & Garzón, 2020). Moreover, it has been chosen as the appropriate approach for this exercise because the VIRTTX encapsulates all the critical elements stipulated by the experiential learning methodology and therefore makes it a perfect fit for this methodology. It presents a high-impact, evolving disaster scenario in which participants communicate, share real-time data, and describe their actions to respond to the evolving incident (DHS, 2011).

4. Overview of Virtual Incident Response Tabletop Exercise – VIRTTX

This section presents an overview of the "virtual incident response tabletop exercise" (VIRTTX). The exercise was designed and conducted in a large organisation operating within the law enforcement industry. It was developed following the experiential learning approach outlined in section 3. An inter-departmental team of Process Assurance, IT Security, and IR/DR coordination teams planned and designed the exercise. Planning activities included but were not limited to scenario design, formulation of discussion points, development of injects and selecting the facilitation team, amongst others. The exercise, which is based on an actual progressive incident, had five aims (i) to assess the likelihood or probability of its occurrence within the business, (ii) to identify existing controls that would mitigate such an attack at each stage, and (iii) identify additional controls that would be needed to mitigate similar incidents further, (iv) review current response plans and (v) agree on an Action Plan to prevent breaches of a similar nature from occurring within the business. VIRTTX participants came from various disciplines and departments. 20 participants, managers, and team leaders from across the business participated in the exercise. They included management representatives from Business Continuity, Service Desk, Process Assurance, Customer Management, Customer Liaison, IT Security, Corporate Communications, Corporate Governance, Information Governance, Strategy and Research, IT Systems Engineering, Business Partner Management, Networks, Internal Communications, Information Assurance, and external partners representatives.

4.1 VIRTTX Scenario

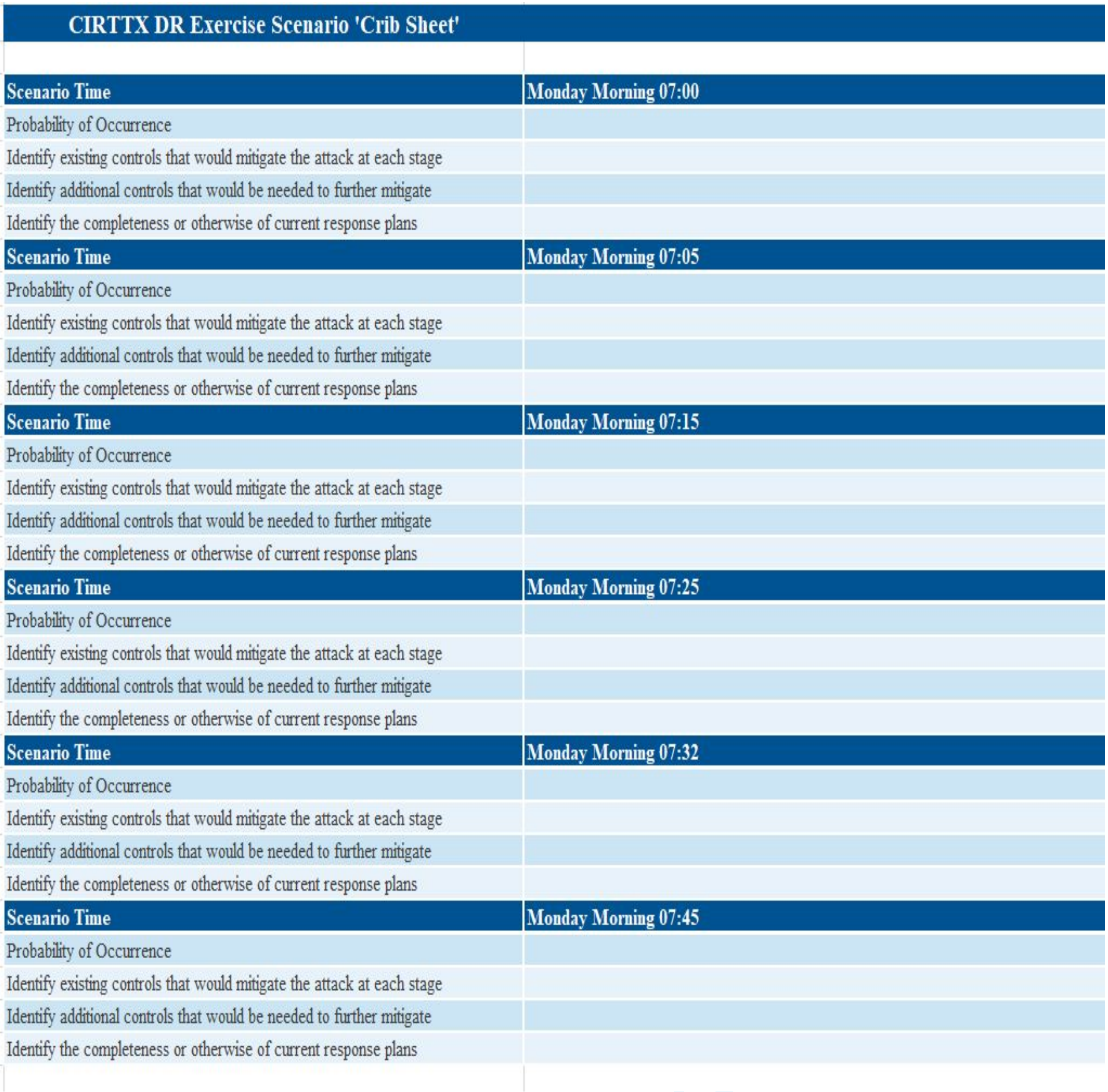
Due to the nature of the exercise and constraints such as time limitations and work commitments, the decision was made to have all participants in a single virtual conference room. At the start of the exercise, the facilitators introduced VIRTTX, defined its scope and objectives and laid down basic expectations. The training provided participants with an avenue to discuss and explore the full range of options that could be implemented to address the crisis scenario in figure 1. Following the scope and objectives, the facilitators presented participants with a scenario. They also coordinated the exercise activities, guiding discussions by asking questions designed to address the exercise's objectives.

VIRTTX scenario and 'injects' were designed to be a functional exercise intended to allow participants to review plans and procedures to discuss and agree on actionable techniques or ideas for incident management within the business (Theodoridis et al., 2021). As a facilitated scenario-based tabletop discussion exercise, it simulated the real-life experience of dealing with an incident. The injects following the scenario increased the urgency of the incident and required participants to react in a way that advanced the exercise, making it a hands-on practical and dynamic scenario. Figure 2 below illustrates the initial scenario that kicked off VIRTTX.

> A member of staff receives an email with an attached pdf advertising an upcoming tournament at their tennis club which they redistribute to colleagues using their business email.
>
> The hyperlinks to the tournament registration page do not appear to work unless “edit mode” is started.
>
> After enabling edit mode those interested in the tournament are able complete their registration.
>
> During registration they discover that the £25 registration fee can be discounted to £10 if participants nominate 5 other colleagues via email. Within 24 hours several colleagues register, nominate others, and congratulates themselves for obtaining the discount.
>
> Not long after they have completed registration the Service Team undertaking routine monitoring notice that backup servers are running slow. They blame the sluggish servers on delayed updates and several other reasons usually given when backups are running slow.
>
> As it is an hour to the weekend it is decided that the slow backups will be investigated on Monday morning.

Figure 2. An outline of the initial VIRTTX Scenario

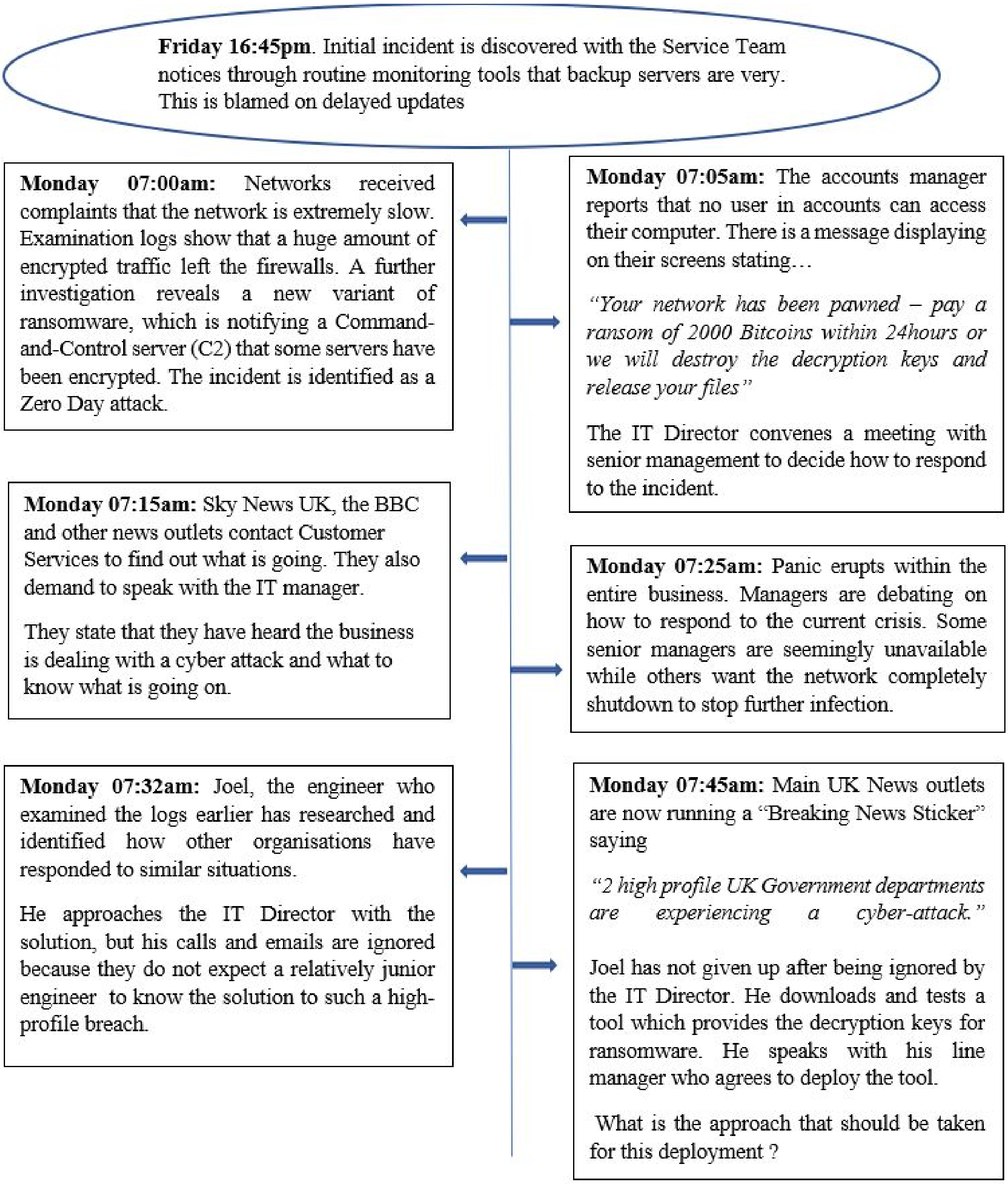
Participants were given a 'crib sheet' to record their responses or formulate suitable reactions to each step taken by the threat actors represented within the scenario and injects. Figure 3 below is an illustration of the 'crib sheet'.



CIRTTX DR Exercise Scenario 'Crib Sheet'	
Scenario Time	**Monday Morning 07:00**
Probability of Occurrence	
Identify existing controls that would mitigate the attack at each stage	
Identify additional controls that would be needed to further mitigate	
Identify the completeness or otherwise of current response plans	
Scenario Time	**Monday Morning 07:05**
Probability of Occurrence	
Identify existing controls that would mitigate the attack at each stage	
Identify additional controls that would be needed to further mitigate	
Identify the completeness or otherwise of current response plans	
Scenario Time	**Monday Morning 07:15**
Probability of Occurrence	
Identify existing controls that would mitigate the attack at each stage	
Identify additional controls that would be needed to further mitigate	
Identify the completeness or otherwise of current response plans	
Scenario Time	**Monday Morning 07:25**
Probability of Occurrence	
Identify existing controls that would mitigate the attack at each stage	
Identify additional controls that would be needed to further mitigate	
Identify the completeness or otherwise of current response plans	
Scenario Time	**Monday Morning 07:32**
Probability of Occurrence	
Identify existing controls that would mitigate the attack at each stage	
Identify additional controls that would be needed to further mitigate	
Identify the completeness or otherwise of current response plans	
Scenario Time	**Monday Morning 07:45**
Probability of Occurrence	
Identify existing controls that would mitigate the attack at each stage	
Identify additional controls that would be needed to further mitigate	
Identify the completeness or otherwise of current response plans	

Figure 3. A sample copy of the 'crib sheet used for recording responses and discussion points.

The facilitators further stimulated discussion by injecting modifications to the scenario, see figure 3. Participants were also encouraged to ask questions or seek clarification if needed. An illustration of the incident and injects timeline.



Friday 16:45pm. Initial incident is discovered with the Service Team notices through routine monitoring tools that backup servers are very. This is blamed on delayed updates

Monday 07:00am: Networks received complaints that the network is extremely slow. Examination logs show that a huge amount of encrypted traffic left the firewalls. A further investigation reveals a new variant of ransomware, which is notifying a Command-and-Control server (C2) that some servers have been encrypted. The incident is identified as a Zero Day attack.

Monday 07:05am: The accounts manager reports that no user in accounts can access their computer. There is a message displaying on their screens stating…

"Your network has been pawned – pay a ransom of 2000 Bitcoins within 24hours or we will destroy the decryption keys and release your files"

The IT Director convenes a meeting with senior management to decide how to respond to the incident.

Monday 07:15am: Sky News UK, the BBC and other news outlets contact Customer Services to find out what is going. They also demand to speak with the IT manager.

They state that they have heard the business is dealing with a cyber attack and what to know what is going on.

Monday 07:25am: Panic erupts within the entire business. Managers are debating on how to respond to the current crisis. Some senior managers are seemingly unavailable while others want the network completely shutdown to stop further infection.

Monday 07:32am: Joel, the engineer who examined the logs earlier has researched and identified how other organisations have responded to similar situations.

He approaches the IT Director with the solution, but his calls and emails are ignored because they do not expect a relatively junior engineer to know the solution to such a high-profile breach.

Monday 07:45am: Main UK News outlets are now running a "Breaking News Sticker" saying

"2 high profile UK Government departments are experiencing a cyber-attack."

Joel has not given up after being ignored by the IT Director. He downloads and tests a tool which provides the decryption keys for ransomware. He speaks with his line manager who agrees to deploy the tool.

What is the approach that should be taken for this deployment ?

Figure 4: Outline of the incident scenario and injects timeline.

5. Findings.

This section presents the findings of both the literature and outcomes from the hands-on practical, experiential exercise.

5.1 Findings from Literature

Findings from the literature review established that during the COVID-19 pandemic, most businesses changed their working routines, with many forced to shut their doors and send staff home (Furnell & Shah, 2020). According to Gafni & Pavel (2022), the abrupt and almost unprepared personnel shift from offices to remote working during the COVID-19 pandemic caused many challenges. They hold that many organisations were unprepared for the sudden and unexpected transition to home working. According to Furnell & Shah (2020), staff across several businesses had no idea how to protect themselves from harmful cyber activity. Gafni & Pavel (2022) elaborate that there was an increase in spam and phishing email attacks, while Ferreira & Cruz-Correia (2021) argue that there was a significant increase in false messages associated with the COVID-19 pandemic. Ferreira & Cruz-Correia (2021), Khan, Brohi & Zaman (2021) insist that threat actors took advantage of the fear and isolation of COVID-19 and the lack of cyber security awareness turn the confined population into a vulnerable target on which they perpetrated attacks. Many of these attacks, such as phishing and fake news sites, ransomware, and false fundraising campaigns, tricked victims into giving away money, their personal data, and even login credentials which were used to perpetrate more attacks (Ahmad, 2020) and (Bayl-Smith et al., 2021). Apart from the challenges elaborated above, there was an increase in cyberbullying, fake profiles, impersonation and 'Zoombombing,' a word used to describe the disruption of zoom conferences. According to research by Chen et al. (2020), these were specific cyber challenges posed by the COVID-19 pandemic because it forced people to engage in frequent telephone or video calls, and they may often forget to consider the environment they are in and who may be listening.

Other challenges included targeted ransomware attacks like those experienced by the Brno University Hospital in the Czech Republic at the heart of the pandemic in 2020 (Pranggono et al., 2020). During this attack, the university's COVID-19 laboratory, which was used for testing COVID-19 patients, was hit by a ransomware attack, and forced to shut down its entire network. In another targeted attack, the systems of a group of hospitals in Paris that were at the centre of the COVID-19 pandemic were attacked in a denial of service (DDoS) attack (Pranggono et al., 2020). In this case, the attackers flooded the hospital's email server with more requests than they could handle, causing it to fall over. As a result of these and other challenges, Hakak et al. (2020) maintained that cyber security during the COVID-19 pandemic was a genuinely concerning issue because of the emerging cyber threats it posed and the security incidents that were perpetrated against vulnerable people and systems globally.

Despite that, Fleming (2020), Furnell & Shah (2020) and Gafni & Pavel (2022) noted that many homeworkers were unprepared and that some faced challenges dealing with some of the threats and trials due to a lack of proper planning, including little or no training. For example, research by Gafni & Pavel (2022) maintained that more than half of the remote workers surveyed did not have relevant knowledge and were not adequately trained about cyber security risks associated with home or remote working. They argued that in some cases, staff noted they did not feel confident enough about their cyber protection as some businesses decreased their cyber security budgets to cope with other costs due to the pandemic (Gafni & Pavel, 2022). Ferreira & Cruz-Correia (2021) maintain that such discoveries reiterate that cyber security literacy, including awareness as well as workforce education and training, is essential, even more so during pandemic times. Moreover, during challenging circumstances such as the COVID-19 pandemic, cyber security practice requires solutions that can be personalised, targeted, and adapted to the situation. This argument explains why we propose a virtual incident response tabletop exercise, VIRTTX, as a targeted, adaptive solution to dealing with the challenge of cyber security awareness training during challenging circumstances such as the coronavirus pandemic.

5.2 Result of the scenario-based tabletop exercise

One of the main aims of the VIRTTX was to establish if a practical, scenario-based IR exercise could assist businesses in addressing the challenges of remote working during the pandemic. One crucial observation enabled participants to participate in much-needed cyber security awareness training. Being a virtual session, VIRTTX provided opportunities for participants to use scenario-based practical, experiential exercises to review and understand their roles better, including what they must do to mitigate the impact of an attack. In this particular instance, it assisted the business leverage exercise scenario in reflecting on whether they could experience breaches of a similar nature. This is crucial, given that some studies observed that a critical challenge during the pandemic was the disruption of education and training. This claim is made by Sadek & Kora (2020), whose attendance at workshops, conferences, and training courses halted in almost all countries worldwide. They argued that the pandemic seriously disrupted some academic courses and that teachers and trainers who were less versed in technology found it challenging to teach through the Internet (Sadek & Kora (2020). VIRTTX allowed the business to review its existing controls and test its IR capabilities. According to Furnell & Shah (2020) and Gafni & Pavel (2022), this testing is essential because several businesses had little or no opportunity to undertake training or adequately plan for the challenges of remote working during the pandemic. The training allowed the company to conduct essential security awareness training targeted at managers and heads of departments which the CMA

(2020) maintain is a critical investment for business leaders. This kind of security awareness training supports businesses in hardening their systems and equips staff with skills to identify and avoid common yet effective cyber-attacks such as phishing and credential harvesting (CMA, 2020). Sections 5.1 to 5.4 provide a detailed account of how a VIRTTX assisted this particular corporation and could help others address the cyber challenges of remote working during the COVID-19 pandemic.

5.2.1 Probability of Occurrence.

The exercise helped participants to interrogate their company's cyber security posture. It did this by providing opportunities for them to question whether such a breach is possible or likely to occur within the business. Using the questions from the crib sheet, see fig 2, training participants discussed and agreed that an incident like the example in the VIRTTX scenario is possible. There was 100% agreement amongst exercise participants that this or similar scenarios are a common phenomenon. Some observed that similar breaches had been reported in other organisations at different scales. One such attack highlighted by participants was a recent cyber-attack on Redcar & Cleveland Borough Council in 2020, which cost around £10m in recovery costs. It was a ransomware attack in which threat actors encrypted massive amounts of data and caused online public services to be unavailable for 135,000 locals for over a week (Raywood, 2020). Other participants opined that breaches like these are highly likely in this age, especially as many businesses have been forced to work from home, sometimes without appropriately adjusting their security procedures. In some cases, ensuring adequate protection for employees working from home was impossible as they were not offered the necessary training (Pranggono & Arabo, 2020). Participants' observation indicates that the business is aware of the current cyber threat landscape, including common threats that could affect them.

VIRTTX participants equally established that there is a probability that this scenario could occur within this company because a study by the National Cyber Security Centre (NCSC) (2020) noted that scams and phishing have not only increased but were the most common attack vector the COVID-19 pandemic. They maintained that though common, phishing attacks were highly influential during the pandemic, with a success rate of 30% or higher (NCSC, 2020). This increase, they argued, was due to people's interest in pandemic-related news which caused them to click on links without taking time to check if they could be malicious. The UK National Fraud Office (2020) and Ahmad (2020) highlighted a significant increase in cyberattacks during the pandemic's peak. One study found that victims in the UK lost over £800,000 to coronavirus scams, with one unlucky victim losing up to £15,000 after buying face masks that never arrived (UK National Fraud Office, 2020). The fact that participants know that such a scenario can occur in their business confirms that they are aware of and recognise that, like all businesses, this company can be susceptible to attacks. Such awareness and recognition also indicate that VIRTTX enabled the business and exercise participants to review their security posture, helping them to be cyber-aware. Such awareness and education, particularly of threats and potential cyber security challenges to a business, according to New Zeeland National Cyber Security Centre (NCSC) (2013), is an essential first step to effective cyber risk management. They maintain that awareness of potential threats should be a regular part of cyber risk management across organisations.

5.2.2 Existing controls that would mitigate the attack.

Scenario-based, practical exercises assist companies in reviewing existing cyber security controls to establish if they are fit for purpose. Using our VIRTTX scenario, participants walked through various cyber controls put in place by the business to defend against cyber threats. Participants demonstrated an awareness of existing controls that would mitigate such an attack, including people, processes, and technical controls, such as hardware and software components, which can be deployed to protect against cyberattacks. Regarding individual or specific controls, all 20 participants, 100%, stated that staff vetting, and regular monitoring are excellent mitigations, especially for insider attacks. All 20 participants, 100% observed that antivirus and anti-malware applications were deployed on end-user devices to help combat threats such as malicious hyperlinks and unsafe attachments. 16 individuals, 80% of participants, identified that Exchange Online Protection could protect the business against breaches such as phishing emails and malware protection. They argued that it is designed to proactively scan email attachments, aiming to identify and block malicious code which could potentially harm systems and applications from executing. This is consistent with research from the NCSC (2016), which maintains that malware protection is an essential security control which can detect and respond to known attacks, such as remote code execution threats. 16 individuals, 80% of participants, claimed that regular backups were a vital control that would be useful against a breach, like the training scenario example. They argued that this would enable the business to restore its systems and data and keep operations unperturbed quickly. Thomas & Galligher (2018) support this view, maintaining that backups are a robust IR/DR tool, handy for dealing with ransomware once a system becomes infected. Participants' demonstration of awareness and understanding of existing controls and their role in addressing cyber challenges suggests that exercises like VIRTTX can assist remote workers in establishing possible threats to their systems and deploying required countermeasures to manage them.

70% of participants, which is 14 individuals, noted that the regular patching of systems, tools and applications is an important control that would be useful to combat similar breaches. They stated that the most vulnerable systems or applications are those the patches are outdated and can easily be exploited. The NCSC (2016) corroborates this view by insisting that businesses must patch known vulnerabilities with the latest software version to prevent attacks that exploit software bugs. 14 participants, 70% highlighted people and process-centred controls like security awareness education. They insisted that this is an essential component of the cyber security controls mechanism that businesses must deploy to protect their data and information systems. The NCSC (2016) support this view, emphasising that user awareness training is crucial in incident response. They argue that user training, education, and awareness help users understand how published information about a business's systems and operations can reveal potential vulnerabilities. Security awareness educates users on the risks of discussing work-related topics on social media and the potential for them to be targeted by phishing attacks. Awareness training also helps users understand the risks of releasing sensitive information in general conversations, unsolicited telephone calls and email recipients (NCSC, 2016).

5.2.3 Review and Testing and Update of IR/DR Plans and Procedure

One of the single and most important results or outcomes of VIRTTX is that it enabled remote participants to test their IR/DR controls. Notably, only 11 individuals, 55% of participants, during the exercise survey recognised the importance of constant testing, reviewing, and updating IR/DR plans and procedures. Moreover, cyber risk management scholars insist that regular testing of IR plans must be an essential part of a business' risk management program. Dupont (2019) holds this view, stating that testing can assist firms in identifying gaps in resilience. It encourages a learning and constantly evolving mindset, which in turn enables firms to adapt their plans to the ever-fluid and dynamic threat landscape. Though it is concerning to note that only 55% of participants in this exercise recognised the importance of testing their IR plans, it is a common phenomenon across several industries. In a study of cyber risk management within the financial sector, Dupont (2019) established that cyber-resilience regulation acknowledges that not all organisations are willing or able to voluntarily adopt the standards and practices that would improve their capacity to sustain a cyber shock. One such practice that is regularly ignored is the reluctance to review their IR plans and procedures constantly.

That notwithstanding, the 11 individuals who voted for testing argued that testing IR plans and processes are an essential control, insisting that regular testing of incident response processes can enhance the business' security posture. Table 1 below provides an overview of participants' awareness and identification of existing attack mitigation controls. The fact that most participants are aware and can articulate at least some of the business's existing controls that may be used to mitigate breaches, such as the example in the training scenario, is significant. It indicates that the company recognises its increasing dependency on technology, relying on internet-facing systems, tools, and applications and is therefore vulnerable to cyber-attacks. Secondly, it highlights that this business, like many others, is taking positive strides to increase its security posture in recognition that if insufficiently protected, businesses can be rendered more vulnerable to emerging cyber security threats (Lošonczi, 2018).

Staff awareness or not of existing attack mitigation controls

Controls	Yes	Maybe	Do not Know
Staff vetting and regular staff audit monitoring.	20	0	0
Antivirus and anti-malware applications deployment on end-user devices.	20	0	0
Exchange Online protection.	16	3	1
Regular backup of systems, data, and applications	16	3	1
Patching of systems, tools, and applications with the latest updates.	14	3	3
Security awareness education.	14	4	2
Regular testing of IR/DR plans and procedures.	11	6	3
Staff with the right skills and qualifications.	12	6	2
Effective risk management (identification, classification & control).	15	3	2
Technical controls (deployment of hardware & software solutions).	20	0	0
Role-based access control (RBAC).	12	3	5
Maintaining compliance (IT Systems, Processes) with regulatory bodies.	15	2	3

Table 2: A representation of participants' awareness levels of existing attack mitigation controls

5.2.3 Additional controls that would be needed to mitigate the breach.

Apart from the controls already discussed, the VIRTTX training scenario identified additional controls needed to mitigate similar incidents further. For example, it was noted that there might be a need for a criminal investigation to be launched to bring the culprits to justice. 20% of participants, 4 out of 20, noted that this is important because investigating breaches, like the example in the scenario, is an essential part of incident management because it can help recover costs and serve as a deterrent to those planning similar operations. 3 out of 20 individuals, 15% of training participants, identified the need for closer coordination between departments. They stated that this is an additional control that can ensure that response activities are aligned and properly coordinated, with resources shared effectively to avoid duplication of efforts. Another 15% noted that an additional control is to have a proactive, clear, and consistent communications plan. Such a plan will enable the business to communicate clearly with stakeholders, who have a right to know what is happening. It also allows the business to hold press conferences deemed necessary to provide coordinated responses to media groups, given that such breaches are usually a subject of interest for the media. 35% or 7 participants noted that staff affiliation to professional bodies and industry-specific organisations is an additional control. They argued that staff from one business could gain from the knowledge, experience and expertise of other professionals who have been through a similar experience if they are part of specific industry organisations. Table 2 below provides a graphical representation of additional controls identified by participants.

Additional controls that would be needed, as highlighted by participants

Type of Control	Number of participants	Percentage
Staff affiliation to professional bodies and industry-specific organisations for knowledge sharing and professional development.	7	35%
Good inter-business and cross-departmental collaboration.	3	15%
Clearly articulated incident processes, including communication plans.	3	15%
Contact with regulatory, law enforcement and investigative bodies.	4	20%
Contact with or access to subject knowledge experts such as the National Cyber Security Centre (NCSC), National Crime Agency (NCA) and others.	3	15%

Table 3: Participants' opinions about additional attack controls to mitigate attacks.

5.2. 4 Completeness or otherwise of current response plans.

As far as the review of current response plans and the formulation of an Action Plan to prevent breaches of a similar nature from occurring within the business is concerned, 8 out of 20 or 40% of participants identified that the business' IR/DR plans and procedures were not easily accessible. It was noted that most response plans are stored electronically and may not be accessible during a system outage. This was a challenge or a drawback, as it is vital for response plans to be visible as it may be challenging to access electronic devices during a breach as systems may be shut down. Goings et al. (2016) corroborate this by highlighting that the inability to access plans during an incident is a serious issue that, if not addressed, can hinder a business' response capability. They maintain that because many IT security organisations are characterised by segmented functions such as vulnerability scanning, patching, and system administration, if IR/DR processes are not synchronised, it can be a significant challenge to find, coordinate, and communicate with the key parties involved in responding to an incident (Goings et al., 2016). To mitigate this, participants agreed that the business should consider storing copies of IR/DR plans at critical locations that are easily accessible in the event of system loss.

Still, on the completeness or otherwise, of current response plans, 5 out of 20 or 25% of participants argued that it is necessary to include more scenario-based exercises in IR/DR training. They advanced that training programs should be designed to fit practical scenarios of common and easily overlooked yet effective breaches such as phishing attacks, sextortion emails, ransomware attacks, and the dangers of edit mode, amongst others. This observation aligns with IR scholars' views. Sena et al. (2021) argued that practical, scenario-based IR/DR training provides real-time opportunities for participants to experience how to manage security incidents. Following that, 4 or 20% of participants highlighted the need for regular testing of IR/DR plans. They maintained that the cyber threat landscape is constantly changing, and plans can quickly become obsolete and need regular testing. Another 15% or 3 out of 20 participants identified the need to review membership of the business' cyber security incident response team (CSIRT) to ensure that membership is current and includes all departments, a range of skilled personnel, and contact details, amongst others. Goings et al. (2016) insist that this is especially important as it has been observed that some businesses may assign incident response duties to systems and network administrators. These people possess technical knowledge and a historical understanding of systems operating procedures but have no experience making business-impacting decisions during a crisis or breach. They recommend that companies who find themselves in this situation should consider additional training of staff to help foster the proper level of experience on the incident response team. Figure 5 below provides an outlook of participants' feedback on the completeness of current controls.

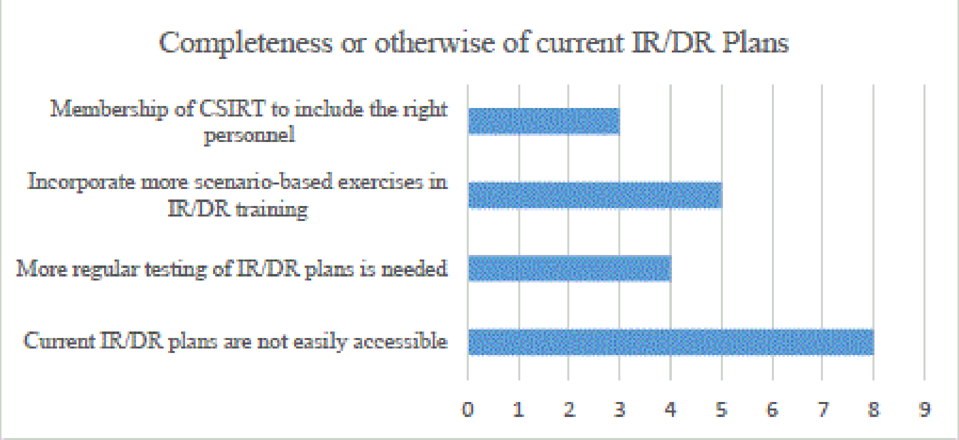


Figure 5: Participants' feedback on the completeness of current controls.

6. Conclusion and Future Work

In this paper, we have summarised our experience conducting a virtual tabletop incident response training exercise during the age of home working as a response to the COVID-19 pandemic. We highlighted some security challenges experienced by businesses as they rushed to relocate staff to work remotely. The paper also discussed threats such as phishing scams targeting remote workers during the pandemic and highlighted risky behaviours exhibited by staff, such as sharing company devices with family members. It noted that some of these challenges be addressed through practical security awareness training, which the CMA (2020) argue would significantly improve a business' security posture. Despite that, Georgiadou et al. (2022) found that business managers recognised that security awareness training, especially IR/DR training is a crucial and better way to deal with increasing cyber security threats. The same studies also maintained that training was often ignored. The study reported that staff across several businesses surveyed reported not having received any security training or guidelines from their employers regarding working from home during the COVID-19 pandemic.

The paper presented an overview of the scenario-based VIRTTX designed and conducted through Microsoft Teams. It maintained that the primary implication for practice is that they enhance security awareness through practical, experiential, hands-on exercises such as this VIRTTX. These exercises bring together staff from across a business to evaluate existing IR/DR processes to determine if they are fit for purpose, establish current gaps, and identify strategies to prevent future threats, including during challenging circumstances such as the COVID-19 outbreak. Furthermore, using TTXs or TTEs for scenario-based incident response exercises was extremely useful for cyber security practice. Some studies found that well-crafted and well-executed exercises are valuable and practical tools for raising cyber security awareness among senior leadership, managers, and IT professionals (Ulmanová, 2020).

Moreover, TTEs with integrated operational and decision-making components can help businesses assess the IR and DR procedures, including communication flow, to improve decision-making at strategic levels and enhance the technical skills of cyber security operators (Ulmanová, 2020, p.29). Furthermore, they can help organisations test new technology, tools, processes for IR and expose any areas of weakness, and enhance cyber education and awareness at all levels. In the academic milieu, games and exercises for education and training have been noted to have significant implications. A study by Angafor et al. (2020) established that games and exercises for teaching and learning were more effective than traditional, conventional classroom teaching methods. They noted that TTXs and other GBL approaches brought education to life, made learning practical, gave students hands-on experience, and helped them learn by doing. In so doing, these scenario-based practical, experiential, hands-on training exercises blended theory and practice. They served as a form of apprenticeship that prepared students for the cyber security industry.

The paper also presented an outline of the VIRTTX and discussed the results vis-à-vis its objectives and existing literature. It noted that while the exercise fulfilled some of the goals. For instance, it enabled management to review their security posture, documenting existing controls that would be useful in mitigating real-world breaches like the scenario in VIRTTX. It also helped them formulate an Action Plan to guide future incident management initiatives and help prevent breaches of a similar nature from occurring in the future. Despite that, it highlighted that while most participants were aware they could be susceptible to security breaches, not all managers were conversant of most or all existing IR/DR controls within their business. Most were aware of what would transpire within their areas but did not know the processes or procedures for other departments or the contact persons. To address this issue, Goings et al. (2016) argued that management, especially within large corporates, must fully support the incident response team, its mission, and its activities during an investigation. Incident response should be communicated and marketed as a service that maintains the integrity of the organisation and its departments. Additionally, the incident response teams within large corporations should engage other satellite teams to nominate a primary contact to facilitate participation in the incident response process Goings et al. (2016).

In future, we plan to refine the exercise to incorporate lessons learnt from running this session to develop a comprehensive, mandatory cyber security awareness training program for staff at all levels within a business. The new program should be broad enough to cover cyber security-related scenarios such as phishing, ransomware, social engineering, denial of services (DDoS) and other common attacks.

References

1. Freedman, L., F. (2021). Consider Conducting a Virtual Tabletop Exercise. Robinson & Cole LLP. National Law Review, Volume XI, Number 77. Available at: https://www.natlawreview.com/article/consider-conducting-virtual-tabletop-exercise (Accessed: 12 June 2022).
2. Nabe, C. (2020). Impact of COVID-19 on Cybersecurity, Deloitte Switzerland. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html. (Accessed: 18 July 2022).
3. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences.
4. Wang, L., & Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, *5*(2), 146-157.
5. Gafni, R. and Tal P. (2022). Cyberattacks against the healthcare sector during the COVID-19 pandemic. Information & Computer Security, Vol. 30 No. 1, 2022, pp. 137-150.
6. Wilson, M. & Hash, J. (2003). NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program. National Institute of Standards in Technology, (NIST), October 2003.
7. AMPG International. (2021). How to host a successful virtual, scenario-based cyber tabletop exercise. APMG International. Available at: https://apmg-international.com/article/how-host-successful-virtual-scenario-based-cyber-tabletop-exercise. (Accessed: 14 January 2022).
8. Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur J 35, 486–505 (2022). https://doi.org/10.1057/s41284-021-00286-2
9. Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, *11*(4), 1809.
10. Stewart, T. (n.d). Scenario-Based Learning. Available at: https://www.massey.ac.nz/massey/fms/AVC%20Academic/Teaching%20and%20Learning%20Cenrtres/Scenario-based-learning.pdf. (Accessed: 14 January 2022).
11. Brown, E. (2017) What Is Virtual Conference. Eztalks.com. Available at: https://www.eztalks.com/video-conference/what-is-virtual-conference.html. (Accessed: 18 January 2022)

12. Cyber Management Alliance (2020) Top 3 Benefits of Cyber Incident Response Training. Available at: https://www.cm-alliance.com/cybersecurity-blog/top-3-benefits-of-cyber-incidentresponse-training (Accessed: 07 June 2022).

13. Angafor, G. N., Yevseyeva, I. and He, Y. (2020). Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis. In Entertainment Computing and Serious Games, M. E. Ma et al. (Eds.): JCSG 2020, LNCS 12434, (pp. 1–15), 2020. https://doi.org/10.1007/978-3-030-61814-8_10.

14. Horne, B. On Computer Security IR Teams. In IEEE Security & Privacy, vol. 12, no. 05, pp. 13-15, 2014. Doi: 10.1109/MSP.2014.96.

15. Lyon, V. (2020). Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals. Walden University.

16. Tobarra, L.; Trapero, A. T.; Pastor, R.; Robes-Gomez, A.; Hernandez, R.; Duque, A. and Cano, J. Game-based Learning Approach to Cybersecurity. In 2020 IEEE Global Engineering Education Conference (EDUCON). pp. 1125–1132 2020.

17. Fordoński, R., & Kasprzak, W. A. (2019). WannaCry ransomware cyberattack as violation of international law: brak. Studia Prawnoustrojowe, (44), 47-73.

18. ENISA, E. (2020). [ENISA] threat landscape 2020: Cyber attacks becoming more sophisticated, targeted, widespread and undetected.

19. Vogel, R. (2016). Closing the Cybersecurity Skills Gap. Salus Journal Volume 4, Number 2, pp 32-46, 2016.

20. Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Crozier, D., & Furnell, S. (2021). Cyber Security Skills in the UK Labour Market: 2021 Findings Report. Ipsos MORI. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1042429/Cyber_skills_in_the_labour_market_report_v6_.pdf (Accessed: 07 June 2022).

21. Angafor, G. N., Yevseyeva, I. and He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy. DOI:10.1002 / spy2.126.

22. Hadley, J. (2019). Why the Cybersecurity Skills Gap Won't Be Solved in the classroom, Forbes. Available at: https://www.forbes.com/sites/jameshadley/2019/09/12/why-the-cybersecurity-skills-gap-wont-be-solved-in-the-classroom (Accessed: 07 June 2022).

23. FitzGerald, N (2019) 'What the Cybersecurity Skills Gap Really Means', CSO Online, 15 June. Available at: https://www2.cso.com.au/article/657807/what-cybersecurity-skills-gap-really-means/. (Accessed: 04 June 2022).

24. Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is Only the First Step: A Framework for Progressive Engagement of Staff in Cybersecurity. Hewlett Packard Enterprise.

25. Business-Higher Education Forum. Invest to Improve: The Cybersecurity Talent Deficit, 2017. Washington DC: BHEF. Available at: https://www.bhef.com/sites/default/files/bhef_2017_invest_to_improve.pdf (Accessed: 18 June 2022).

26. US Department of Homeland Security, Federal Emergency Management Agency. Emergency Management Institute (EMI). Virtual Table Top Exercise (VTTX). Available at: https://training.fema.gov/ programs/emivttx.aspx. (Accessed: 09 January 2022).

27. Wendelboe, Aaron & CRM, Amanda & Drevets, Doug & Salinas, MD & Miller, E. & Jackson, Dalton & Chou, PhD & Raines, JD & Group, Public. (2020). Tabletop exercise to prepare institutions of higher education for an outbreak of COVID-19. Journal of Emergency Management. 18. S1-S20. 10.5055/jem.2020.0464.

28. Garzón, F. & Garzón, G. (2020). Cybersecurity Incident Response Tabletop Exercises Using the Lego Serious Play Method. ISACA Journal, volume 4, 2020.

29. Madani, K.; Pierce, T.W. and Mirchi, A. Serious games on environmental management. Sustain. Cities Soc. 2017, 29, 1–11.

30. Marome, W.; Natakun, B.; Archer, D. Examining the Use of Serious Games for Enhancing Community Resilience to Climate Risks in Thailand. Sustainability 2021, 13, 4420. https://doi.org/10.3390/ su13084420.

31. Chang, C. Y. and Hwang, G.J. Trends in digital game-based learning in the mobile era: a systematic review of journal publications from 2007 to 2016". International Journal of Mobile Learning and Organization, 13(1), 68-90, 2019.

32. Sena A, Forde F, Yu C, Sule H, Masters MM. Disaster Preparedness Training for Emergency Medicine Residents Using a Tabletop Exercise. MedEdPORTAL. 2021;17:11119. https://doi.org/10.15766/mep_2374-8265.11119

33. Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems, 2015, 37. hal-01574600.

34. Abbott, D. Modding Tabletop Games for Education. In Gentile M., Allegra. M., Söbke H. (Eds), Games and Learning Alliance, GALA 2018, Lecture Notes in Computer Science, vol 11385. Springer, Cham, 2019.

35. Khurshid Z., Tariq R., Asiri F.Y., Abid K., Zafar M.S. (2021). Literature search strategies in dental education and research. Journal of Taibah University Medical Sciences, 16 (6), pp. 799-806.

36. Murray, R. (2018). An Overview of Experiential Learning in Nursing Education. Advances in Social Sciences Research Journal, 5(1) 1-6.

37. Dewey, J. (1938) Experience and education (New York: MacMillan).

38. Kolb, D. (1984) Experiential learning. Experience as the source of learning and Development (Englewood CliÚs, NJ: Prentice Hall).

39. Wingfield, S., & Black, G. (2005). Active versus passive course designs: The impact on student outcomes. Journal of Education for Business, 81(2), 119–125.

40. Department for Homeland Security. (2011). Communications-Specific Tabletop Exercise Methodology. SAFECOM, Washington, DC.

41. Theodoridis, G., Georgescu, A., & Gârban, H. N. (2021). Lessons from a Didactic Table Top Exercise During a European Training Course. International Journal of Cyber Diplomacy, 2, 79-105.

42. Furnell, S, and Shah, J. N. (2020). Computer Fraud & Security 2020(8):6-12. DOI: 10.1016/S1361-3723(20)30084-1

43. Ferreira, A, and Cruz-Correia, R. (2021). COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt? JMIRx Med 2021 | vol. 2 | iss. 2 | e21069.

44. Sadek G. S, Kora M. A. (2020). Transformation to virtual training during COVID-19 pandemic: Case report from a low resources' country. Journal of Microscopy and Ultrastructure. Volume 8, Issue 4.

45. Khan N. A, Brohi S. N, Zaman N. Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv. Preprint posted online on 11 May 2020. Doi: https://doi.org/10.36227/techrxiv.12278792.v1

46. Ahmad T. Coronavirus (COVID-19) pandemic and work from home: challenges of cybercrimes and cybersecurity. SSRN Journal. Preprint posted online on 05 April 2020. [FREE Full text] [doi: 10.2139/ssrn.3568830]

47. Bayl-Smith, P. Taib, R. Yu, K and Wiggins, M. (2021). Response to a phishing attack: persuasion and protection motivation in an organisational context. Information & Computer Security. Vol. 30 No. 1, 2022, pp. 63-78.

48. Chen L, Utkucan B, Jeremy B, Gianluca S. (2020), A first look at Zoombombing. ArXiv. Preprint posted online on 08 September 2020.

49. Pranggongo, B, and Arabo, A. (2020). COVID 19 Pandemic - Cybersecurity Issues. Internet Technology Letters. DOI: 10.1002/itl2.247.

50. Hakak S, Khan WZ, Imran M, Choo KKR, Shoaib M. Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access. 2020;8:124134-124144.

51. Fleming, S. (2020), "Surge in security concerns due to remote working during COVID-19 crisis", Journey Notes, Barracuda.com. Available at: https://blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-toremote-working-during-covid-19-crisis/ (Accessed: 18 April 2022).

52. Raywood, D. (2020). Redcar and Cleveland Attack Recovery Cost Over £10m. Accessed from https://www.infosecurity-magazine.com/news/redcard-attack-recovery/. 12 June 2022.

53. Pranggono, B. & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. John Wiley & Sons. https://doi.org/10.1002/itl2.247.

54. National Cyber Security Centre (NCSC). Advisory: COVID-19 exploited by malicious cyber actors (2021) Gov. UK. Available at: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory (Accessed: 04 June 2022).

55. Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Article in SSRN Electronic Journal. April 2020. DOI: 10.2139/ssrn.356883

56. The New Zeeland National Cyber Security Centre, (2013). Cyber Security and Risk Management: An Executive level responsibility, Govt. NZ. Available at:

https://www.ncsc.govt.nz/assets/NCSC-Documents/cyber-security-risk-management-Executive.pdf (Accessed: 05 May 2022).

57. National Cyber Security Centre. (2016). Common Cyber Attacks: Reducing the impact. Cyber Attacks White Paper, January 2016.

58. Thomas, J & Galligher, G. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. Computer and Information Science. 11. 10.5539/cis.v11n1p14.

59. Lošonczi, P. (2018). Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population. Security Dimensions. 26. 173-186. 10.5604/01.3001.0012.7249.

60. Goings, E., Plesco, R., Nides, D., and Kilman, D. (2016). 10 Common Cyber Incident Response Mistakes – Cyber Insights for the Federal Government. KPMG LLP.

61. Ulmanová, M. (2020). How to Develop a Cyber Security Table-top Exercise – A Practical Guide. National Cyber and Information Security Agency of the Czech Republic, Cybilportal.org. Available at: https://cybilportal.org/wp-content/uploads/2020/07/N%C3%9AKIB-How-to-Develop-a-Cyber-Security-Table-Top-Exercise-a-Practical-Guide.pdf (Accessed: 10 June 2022).