The Psychological Effects of Continuity Threatening Cyber Incidents

Toni Virtanen
Military Psychology, Human Performance Division, Finnish Defence Research Agency (FDRA), Finland

toni.virtanen@mil.fi

Abstract: Working in the field of cybersecurity has been compared to working in a warlike environment. Understanding what types of psychological strain cyber attacks cause to the defending organisations' workforce can aid in developing methods and processes for mitigating those stressors. This paper discusses the first-hand psychological effects of experiencing an operational continuity threatening cyber incident caused by a real threat actor. The results are based on 19 interviews from IR professionals and IT security practitioners to decision makers, CISO's and other top executives. These individuals were working in multi-national corporations, hospitals, central government, financial sector, local government or educational institutions at the time of the incident. The interviews followed critical incident paradigm to focus on significant events during the cyber incidents, while also being semi-structured to compensate for the diversity of the incidents. Most of the interviewees raise up feelings of disbelief and despair as their first emotional response to the realization of being hit by ransomware, data theft or another severe cyber incident that could threaten operational or business continuity. Feelings of guilt and self-doubt were present, especially in those considered to be responsible for securing the network. However, at the same time, feelings of purpose and self-efficacy were also reported by some. Having scalable resources available in the time of need, with well-defined roles and responsibilities for the core incident response teams and protecting them from unnecessary inquiries seemed to alleviate the stressors and anxiety of the Incident Response (IR) team during the event. Good leadership and internal communication were seen as important to maintain the necessary situational awareness and focus during the active incident mitigation and resolve phase. Long-term negative effects of the cyber incident were increased cynicism, fear of the situation recurring, and thoughts of changing career. These negative outcomes were mitigated by increased trust in colleagues, processes and systems with experience of self-efficacy. This paper discusses what types of mental strain cyber incidents introduce to cybersecurity professionals and top executives. It deepens understanding on what factors need to be considered in developing and enhancing the overall resilience of organisations against cyber attacks.

Keywords: Cyberpsychology, Cyber Defence, Resilience, Mental demand, Cyber incident, Psychological effects of cyber attacks

1. Introduction

Working in the field of cybersecurity has been compared to working in a warlike environment (Brody, 2015; Singh, et al., 2023). Cyberspace does not follow geography and threat actors can project their attacks easily to anywhere on the globe making organisations defences endlessly contested. Cybersecurity professionals are providing critical service to ensure business continuity of organisations and government services in a constantly changing adversarial landscape (Paul & Dykstra, 2017). Recent studies have indicated that work-related stress is high in the cybersecurity profession (Nobles, 2022; Singh, et al., 2023). The VMware Global Incident Response Threat Report from 2022 demonstrates that 51% of cybersecurity professionals self-report having symptoms related to burnout and of that group, 65% have considered leaving the cybersecurity profession altogether (VMware, 2022). Understanding what types of psychological strain cyber attacks cause to the defending organisations' workforce can aid in developing methods and processes for mitigating those stressors.

2. Methods

Interviews were semi-structured and used an adapted version of Critical Incident Technique (CIT) (Flanagan, 1954). The semi-structured form went through certain set of questions with everybody, but included follow-up questions when applicable. The structured questions included but were not limited to, the following topics: what happened, how the cyber-attack was first noticed, how did collaboration with others work out, what actions were taken, what was surprising, were they able to mentally and physical recover during the incident, and what possible long-lasting effects did the event have. 18 out of 19 interviews were conducted in person. Each interview took approximately 1.5 hours. At the start of the interview, participants were asked to sketch emotional journey mapping and to a provided timeline and then pinpoint four critical events during the cyber incident (Figure 1). Various journey maps are commonly related to UX and service design methods (Nielsen Norman Group, 2018), but can also be applied to visualise the emotional change during the different phases of a cyber incident.

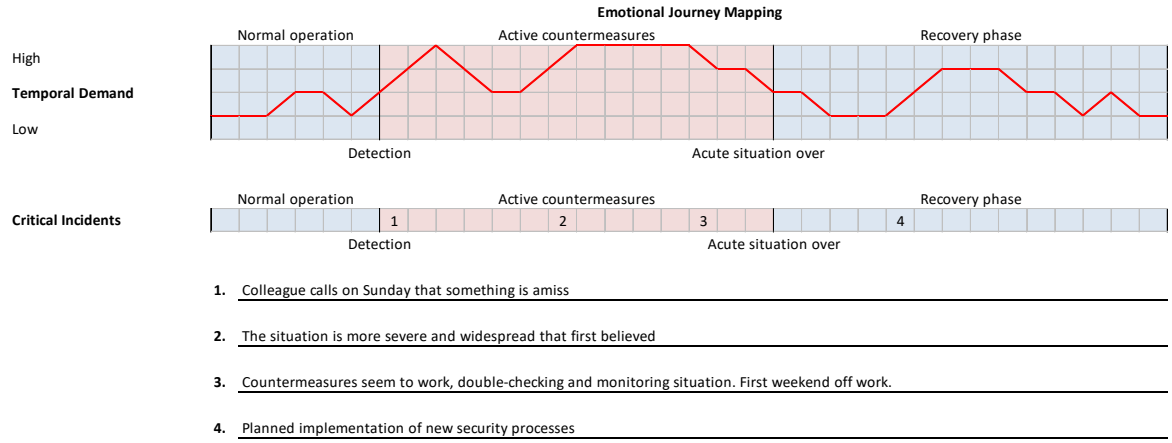

Figure 1: Example of the Emotional Journey Mapping and Critical Incidents

Participants sketched their emotional journey mappings using six categories: Stress, Mental Demand, Physical Demand, Temporal Demand, Effort, Performance and Frustration. Excluding Stress, the categories were based on the NASA Task Load Index (NASA-TLX) (Hart, 1986). Descriptions for each scale category were provided (Table 1)

Table 1: Descriptions of emotional journey mapping categories adapted from NASA-TLX (Hart, 1986).

Category	Description
Stress	Stress refers to a situation in which a person feels tense, restless, nervous, anxious or has difficulty sleeping when things are constantly bothering his mind. Try to recall and evaluate when you felt the most stress and when the least.
Mental Demand	How much mental demand and perceptual activity was required to do the job (e.g. thinking, deciding, calculating, remembering, looking, searching etc)? Was the task easy or demanding, simple or complex, exacting or forgiving?
Physical Demand	How much physical activity was required (e.g. pushing, pulling, turning, controlling, activating etc). Was the task easy or demanding, slow or brisk, slack or strenuous, restful or laborious? Did the task require physical stamina? Did it require long hours of continuous working?
Temporal Demand	How much time pressure did you feel, due to the rate or pace at which the task was required to be done? Was the pace slow and leisurely or rapid and frantic?
Effort	How hard did you have to work (mentally and physically) to accomplish your level of performance?
Performance	How successful do you think you were in accomplishing the task? How satisfied were you with your performance in accomplishing these goals?
Frustration	Were you left feeling discouraged, irritated, stressed and annoyed during the task (high frustration)? Or did you feel gratified, content and relaxed during the task (low frustration)?

The emotional journey mapping with the critical incidents acted as an orientation and memory aid that guided the semi-structured interview process afterwards. As an example, the emotional journey mapping provided a starting point for follow-up questions: "Your frustration level soared at this moment. What happened and why

were you frustrated about it?" As every cyber incident was unique, the timeline for the emotional journey mapping was deliberately very rough and no specific timeframe was given as some incidents only took days while others could even take months. Still, the aggregated timeline from these incidents can provide an overview of the general process victims go through.

2.1 Subjects

A total of 19 volunteer interviewees were recruited with the aid of the Finnish National Cyber Security Centre (NCSC-FI). A recent systematic review on qualitative sample sizes shows that 9–17 interviews or 4–8 focus group discussions generally reached saturation (Hennink & Kaiser, 2022). The NCSC-FI maintain Finnish national cyber situational awareness, develops forums for information sharing within industries and provides information and guidelines for improving cybersecurity. The NCSC-FI also receives voluntary reports from private persons, businesses and organisations when they suspect that they have fallen victim to an actual or attempted information security incident, such as malware infection, phishing or DDoS attacks. Interviewees were selected to represent a wide variety of organisations and government service providers such as manufacturing, Information Technology (IT) security providers, logistics, health care, central government, financial sector, local government or educational institutions and others. Organisations differed widely in size and internationality. Some organisations had more experience in cyber incidents and Incident Response (IR) management, while others had only small teams handling everything related to IT, from security to infrastructure and quality of service. None of the interviewees were personally the target or victim of a cyber-attack, and the results are based on interviews from IR professionals (six interviews) and IT security practitioners (eight interviews) to decision makers, CISO's and other top executives (five interviews) that were working at the organization or as an external IR professional brought to aid organisations that have fallen victim to a cyber-attack.

The cyber incidents were required to be severe enough to either risk operational continuity, cause major damage to reputation, or include loss of IP or other sensitive information. Attacks included severe and long-lasting DDoS attacks on key services, ransomware attacks that encrypt key resources, and successful penetration and exfiltration of sensitive information. Attack vectors varied from zero-day vulnerability, to phishing emails, while the threat actors could be attributed to represent suspected state-sponsored Advanced Persistent Threat (APT) actors or cybercriminals. No requirement was made on how recent the incident needed to be. In addition, no exercises or penetration test experiments were included and all the cases were required to be authentic with genuine threat actors and contain real risks to the organisations. As the topic can be sensitive to the individuals and organisations involved, all interviews are strictly confidential and the results were aggregated in such a way that anonymity is ensured for the participants.

3. Results

3.1 Emotional Journeys

The grid on the emotional journey mappings (see Figure 1) was used as scale from 1 to 5, where 1 is the lowest point and 5 is the highest point on the scale. From this scale, average emotional mappings were calculated (see Figure 2), which provide an estimate of the general direction on how cyber incidents impacted the individuals. The thick central line represents the average value, while the upper and lower lines represent the high and low limit of the 5% confidence interval, meaning that 95% of all responses fit in between those lines.

The highest impact from detecting a severe cyber incident is shown as increased stress, mental demand and temporal demand. The temporal demand rises almost instantly after detection, while stress and mental demand accumulate and peak a bit later after detection. There also seems to be a second peak for mental demand later on during the active countermeasures phase. Unsurprisingly, physical demand remained generally low, even during the active countermeasures. Increased effort is observed to follow a similar pattern to the stress and temporal demand categories. Participants who self-reported estimates on their own performance level seemed to be unaffected and remained quite high at all times. Frustration level had the largest variation between requirement was made on how recent the incident needed to be. In addition, no exercises or penetration

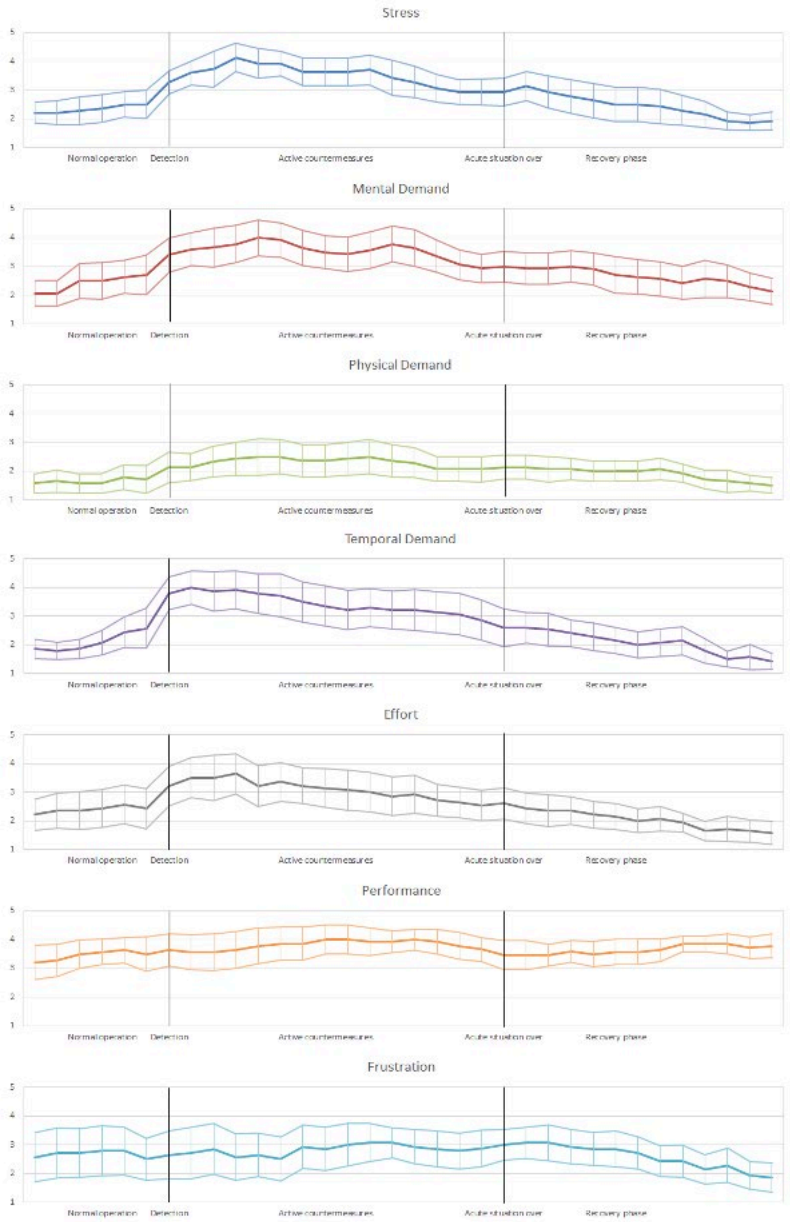

Figure 2: Average emotional journey mappings for each category. Thick central line represents average values, while the upper and lower line represents the high and low limit of the 5 % confidence interval

participants, meaning that feelings of frustration depended highly on the incident and the individual. Interviews

The 19 interviews revealed three distinct groups: 1. Incident Response (IR) processionals hired to aid an organization during the attack (six interviewees), 2. IT security practitioners at the organization under attack (eight interviewees) and 3. Top executives and decision makers at the organisations (five interviewees).

3.1.1 IR Professionals

IR professionals were better able to distance themselves from the situation as it was not them nor their organization that was under attack. They also had more experience on different types of cyber incidents giving better perspective to the situation. Overall, IR professionals experienced less anxiety and stress from these incidents, even if the temporal demand remained high. Some even reported being enthusiastic and excited as a new case meant a deviation from day-to-day activities. Many interviewees also commented that they continued to study and investigate cybersecurity-related issues at home in their free time, as it was something they were so interested about. A new case also presented a learning opportunity and a challenge to test one's skills. After

more severe and demanding cases, they did still report the need to recover for a few ordinary workdays before they felt ready for another case.

Working as an external IR professional might spare them from the psychological effects suffered by the targeted victims of a cyber-attack, but introduced other types of strain factors. The most straightforward inconveniences for IR professionals emerged when they needed to set up and work at the customers' premises with sometimes less-than-optimal tools and ergonomics. An unexpected source of stress came from tense social interactions with the local IT support in some cases. This tension was thought to stem from various reasons, such as simply being the result of how some people might act under highly stressful situations. One hypothesized reason was also that the local IT security practitioners could feel their position threatened, as they were no longer the definite expert on cybersecurity issues for their organization. Another reason for local IT support opposition might originate from the reluctance of doing any major changes to the systems in such tight timeframes, which during normal operation would be planned for weeks if not months. Thus, the external IR professionals feel pressure that they must be absolutely certain about their analyses and suggestions before they present them to the customers. This pressure, along with the increasing discovery of new vulnerabilities, contains a risk of burnout as IR professionals constantly try to keep up with the latest trends on threat actors' tactics, techniques and procedures. Building trust and being able to communicate what needs to be done with the customers' representatives at all levels were seen important by the IR professionals. This however might create another dilemma as not all technically skilled people are good at communicating with the customer, while those that are might not have the necessary understanding of the technical aspects needed to be discussed.

3.1.2 IT Security Practitioners

Local IT security practitioners had more variation in how much experience they had with Incident Response Management, depending on the size and type of the organisations. The smaller the organization, the more stretched out the individuals' role was. Larger or security-critical organisations had their own information and cybersecurity teams, while in smaller organisations only a few IT professionals handle everything from cybersecurity to local IT support for end-users. The less experience the individual had, the more stressful they felt the situation to be. There was also an element of frustration, as in many cases, the event could have been prevented if higher-ups would have listened to their recommendations earlier or that end-users would have followed the information security guidelines properly. All of them, however, understood that as their organisation's core business was not in cybersecurity they needed to make do with the resources they were given. Although all IT security practitioners reported that the situation was stressful, younger interviewees especially experienced the stress to be a mix of excitement and anxiety. They were excited that something is actually happening, but anxious about the workload and whether they are up to the challenge.

IT security practitioners' first reactions on the revelation of a severe cyber incident were disbelief and hope that things are not as bad as they seem. This was followed by a brief moment of numbness as the consequences of the situation started to sink in. Feelings of failure and shame were also frequently reported during the first moments after the discovery. Some individuals also reported feelings of despair with a sensation that they are alone in this situation and admitted that they experienced a brief urge of just giving up and quitting then and there. Once they had gotten over the shock, many felt indecisive on what should they do first as all things seemed equally important and urgent. Once the initial restriction and mitigation actions were done, a moment of respite followed. However, in most cases there were always some repercussions that required extended effort, such as checking that unaffected systems were really clean. This moment is critical for the well-being of IT security practitioners, and they shouldn't overexert themselves at the acute mitigation phase just to realize that a lot of work is still required to be done.

During the acute response and mitigation phase, some reported feeling frustration because of the micromanagement of higher-ups and constant questions from end-users or other departments. IT practitioners felt that when the middle-managers didn't understand the situation, they seemed to panic and required even small decisions to be approved by them hindering the recovery activities. End-users on the other hand, were keen to get their tools and software back, but all of these questions took time away from the actual recovery actions. Disagreement and frustration were also caused by IT service employees from other locations, as they might argue against the instructions given by the IT security practitioners. In hindsight, the interviewees reported that during the stressful and time-demanding situation, their delivery could have become quite narrow, leaving pleasantries and explanations at a minimum in e-mails and other communication channels. In addition, they recognized that being under a high mental load and so preoccupied in their thoughts, they might have not acknowledged others around them very well and, for example, forgotten to greet them in the morning. Both of

these behaviours might seem rude or even hostile from the perspective of other colleagues, which can cause conflicts within the wider work community.

Existing incident management and recovery plans were mentioned as valuable checklists, although in some cases the situation was assessed to be so unique that they weren't applicable. With larger corporations, it was also sometimes difficult to find the right contact person for inquiries and requests in other departments and locations. In almost every case, an external IR team was hired to help the local IT security practitioners with the mitigation and recovery. Their experience and know-how were seen as critical and many commented that they wouldn't have managed the situation without them. In many organisations, there just isn't any reason to have an internal IR team, as cybersecurity is only seen as an unavoidable expense for doing business. During the recovery phase and even long after few IT security practitioners reported having some kind of an impostor syndrome. They were now given better resources and had better visibility and controls in the networks, so they felt anxious on the prospect that they would fail again. In addition, quite often a new and improved Security Information and Event Management (SIEM) system was adopted after the incident by the recommendation of the external IR teams. As with any new system, there was always a learning curve for familiarizing themselves with the slightly different types of alerts the new SIEM system produces, and this new system had to be learned alongside the recovery and build up still underway.

3.1.3 Top Executives

Top executives mostly had stressors related to leadership, resources, communication and responsibility. The first moments after a severe cyber incident included a lot of communication to stakeholders, gathering resources, people and expertise to handle the situation. They felt responsible about the incident and also had feelings of shame and remorse that they had failed, even if there wasn't anything they could have done better with the resources at their disposal. Some also reported being worried about losing their job and reputation, thinking that they will never get a job in cybersecurity again. The feeling of a blemished reputation, could last even long after the actual cyber incident was over, making them stressed out from even the slightest rustles in the network. As cybersecurity can be so abstract, one could even feel guilty in situations that weren't even part of their responsibility.

A major source of stress came from publicity of the incident. Stress was higher when the top executives didn't have control of when or how it would become public. For example, in a situation where the threat actors themselves went public by leaking sensitive information, or when the public media takes interest as the organization is providing a popular service that becomes unavailable due to the attack. Publicity can affect the organization's reputation, which can have an impact on the valuation of a publicly traded company. In addition, very often when a cyber incident becomes public it also generates other attempts against the organisation's systems, resulting in extra work for the SOC and other IT security practitioners who already have their hands full mitigating and resolving the ongoing incident.

In many cases, top executives saw themselves as the gatekeepers for the IR teams and IT security practitioners working towards recovering from the incident so that they could concentrate on fixing the issue and not worry about irrelevant inquiries from media, other departments or end-users. They feel they need to ensure that the people working for them get enough rest and do not become exhausted during the incident. Managing experts, who are often very motivated, enthusiastic and strive for perfection also has its unique challenges. High motivation needs to be curated so that people do not burn themselves out, while still avoiding discouraging them. Some experts seem to react to a crisis by thinking they are irreplaceable and keep working even on areas that are not their responsibility. For example, a networks expert will begin to analyse databases for Indications of Compromise (IoC) on their own initiative, when the best thing he or she could actually do is to just get some rest and then continue to work on the things that are their expertise. These unprompted actions can just wear out people faster and increase fatigue related human errors. It is therefore important to allocate clear roles for the IR team and IT security practitioners so that people know what they and others are doing.

Interestingly, another source for irritation and frustration for top executives were the managers and executives from other departments. Even if the organization had an existing disaster recovery plan, dictating which systems are deemed as most important. There seems to be always someone who tries to challenge it trying to get the system most important for their department recovered first. Managers and executives from those departments that were spared by the effect of the cyber-attack might realize that they dodged a bullet by luck and are now demanding that all the recommendations and changes to be made as soon as possible, even if they had been opposing any changes to their legacy systems earlier. Others who have been affected by the incident, might also

try to hide behind red tape and blame to the CISO or other IT security managers for the incident. As an example, they might claim that the reason they hadn't patched their systems was because they hadn't got any recommendations to do so, or that they don't recall any requests for extra resources to patch the vulnerability. This results on less than optimal working atmosphere and insisting to have detailed records on what has been agreed upon and when at all times.

3.1.4 General Observations

Work-Life balance was difficult to arrange during the cyber incident especially for individuals with family and small children. Although interviewees reported that their spouses and family were understanding and supportive, the incident could generate some tension at home. Much of the household chores, childcare, and other responsibilities might fall on the spouse, which could seem unfair from their perspective. They also might appear distant and weary at home during the height of the incident. Most of the interviewees also reported that they couldn't discuss the situation at home as much of it was confidential. It is quite common for threat actors to schedule their attacks during holiday seasons. Only few of the interviewees had discussed with their spouses that their cybersecurity occupation could involve situations where they would need to be on call and spend long hours at work for extended periods. Another challenge for work-life balance came from significant event outside of work that could coincide with the cyber incident. These could be, for example, serious illness or loss of a close relative, or big family reunions and celebrations such as weddings.

Many interviewees also considered that any activity which required one's full attention worked best to take their mind off work. These types of activities varied widely depending on the person and could be anything from hunting to watching TV. Physical exercise was mentioned as another way to release stress and maintain general well-being. Playing and spending time with children were also mentioned as an effective way to unwind for those who had a family. Many interviewees mentioned that their work-life balance had improved as they got older, settled down, and started a family. Having some kind of structure in life, such as a relationship, family or even just a pet, helped them to not spend all their waking hours with computers. For many, cybersecurity were almost a vocation and a topic that they were extremely interested in. To maintain some level of work-live balance, many of the interviewees had developed ways to limit how much time they can spend on it in their free time. A common method was to not have any computers or smart devices easily available at home, deliberately preventing them from working at home. Another, regrettably less constructive method, was alcohol, as having a couple of drinks gave them the permission to relax. Almost everyone mentioned good working atmosphere and humour as an effective way to release stress at the workplace.

Interviewees didn't always emerge from the severe cyber incidents unscathed and reported experiencing similar long-term symptoms more often associated with people experiencing traumatic events. Such symptoms included difficulty sleeping, hyper-alertness, cynicism, awkward reactions to stressful situations, emotional numbness and risk behaviour related to alcohol. According to the definition of the Diagnostic And Statistical Manual Of Mental Disorders (DSM-5-TR) (American Psychiatric Association, 2022) most cyber incidents do not fulfil the criteria of a traumatic event as they generally lack the real or experienced danger of death or serious injury, or a threat to the physical integrity of self or others. Even though cyber incidents do not fulfil the diagnostic criteria, it could be argued that severe cyber incidents can still be considered as a traumatic event by some. For some, the severe cyber incident seemed to work as a catalyst on reflections of one's identity, what they want to do with their life and considerations of changing careers completely or finding a less stressful field in IT. A general observation by the interviewees was that many of their colleagues with small children, changed position or left the organization a couple of months after the cyber incident. Severe cyber incidents also had a wider ripple effect within the organization, and often resulted in an increased workload to other departments that could last long after the incident was already over. End-users in all levels also tended to have a general loss of trust in the system. This was often visible by the increased number of questions and tickets to IT security and the increased number of paper copies.

4. Discussion

This paper presented the psychological impact of severe cyber incidents based on 19 voluntary interviews from various organisations. The limitations of this study are the relatively small sample size and possible culture dependencies which might somewhat diminish the generalizability of the results. Although none of the interviewees were the target of the cyber-attack in person, those working in the organization under fire did experience the event as highly stressful. Coping with uncertainty, time pressure and communication were

prevailing stressors for cybersecurity professionals in all levels during a cyber incident. As a highly motivated group, cybersecurity professionals can be at risk of burning oneself out especially during crisis situations.

Several best practices and recommendations to reduce the mental and social load of the cyber incidents can be derived based on the interviews. Sharing information about the cyber incident with other industry members is highly recommended. In some cases, organisations were able to speed up their countermeasures as they had been recently informed of a similar incident. Organisations should define clear roles and responsibilities for incident response beforehand to avoid miscommunication and conflicts. These roles and practices also need to be practiced and trained with periodical exercises. It should also be ensured that all the critical personnel get enough rest and nutrition during the incident, by arranging work shift and food supply for the team. It is recommended that the core incident response team is protected from unnecessary questions and inquiries so that they can concentrate on the incident, while the access to the war room or operation centre needs to be limited to only those actively participating in the incident response. Having too large of a group, can decrease focus and efficiency. Special attention should be given for communication as misunderstandings can cause unnecessary conflicts within the organisation. In addition to the general lessons learned events after the incident. Arranging debriefing sessions with a focus on mental and physical well-being led by a social scientist or a similar professional could be beneficial after especially demanding cases.

Although this study focused on the negative impacts on cyber incidents, these events can also have a positive impact on the team cohesion within the organization, giving purpose to one's work and acting as a baptism by fire for the professionals, making them more prepared in the future. Very often, a cyber incident acted as a catalyst for getting rid of unsecure legacy systems and receiving sufficient resources for maintaining and improving cyber security within the organization. Further research is needed on the psychological effects during and after cyber incidents. Future research will look into verifying these findings with a questionnaire study and test if there are any cultural differences between countries and organizations.

Acknowledgements

The author would like to thank Finnish National Cyber Security Centre (NCSC-FI) and all the interviewees for participating in this study.

References

American Psychiatric Association, 2022. Diagnostic And Statistical Manual Of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR).

Brody, B. A., 2015. Cybersecurity akin to being in a war zone—you have to be "left of boom" to survive. [Online] Available at: https://philipcao.com/2015/06/28/cybersecurity-akin-to-being-in-a-war-zone-you-have-to-be-left-of-boom-to-survive/ [Accessed 22 JAN 2024].

Flanagan, J. C., 1954. The critical incident technique.. Psychological bulletin, Volume 51, p. 327.

Hart, S. G., 1986. NASA task load index (TLX).

Hennink, M. & Kaiser, B. N., 2022. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine, Volume 292.

Nielsen Norman Group, 2018. Journey mapping 101. [Online] Available at: https://www.nngroup.com/articles/journey-mapping-101/ [Accessed 23 JAN 2024].

Nobles, C., 2022. Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA–Journal of Business and Public Administration, Volume 13, p. 49–72.

Paul, C. L. & Dykstra, J., 2017. Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. Journal of Information Warfare, Volume 16, p. 1–11.

Singh, T., Johnston, A. C., D'Arcy, J. & Harms, P. D., 2023. Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research. Organizational Cybersecurity Journal: Practice, Process and People.

VMware, I., 2022. Global Incident Response Threat Report: Weathering the Storm. [Online] Available at: https://www.vmware.com/content/microsites/learn/en/1553238_REG.html [Accessed 22 JAN 2024].