Finnish Defence Research Agency
Research Bulletin 03–2025

19.02.2025

Psychological effects of cyberattacks

Toni Virtanen, PhD
Human Performance Division

Working in cybersecurity is often compared to being in a war-like environment. Understanding the psychological strain caused by cyberattacks on the cybersecurity workforce can help develop methods to mitigate these stressors. This paper explores the first-hand psychological effects of experiencing a cyber incident that threatens operational continuity, based on 19 interviews with Incident Response (IR) professionals, IT security practitioners, and top executives. These individuals were employed in multinational corporations, hospitals, central government, financial sector, local government, or educational institutions at the time of the cyber incident. The interviews, which followed a critical incident paradigm, revealed feelings of disbelief and despair as initial emotional responses to ransomware, data theft, or other severe cyber incidents. Feelings of guilt and self-doubt were common, especially among those responsible for network security. However, some also reported feelings of purpose and self-efficacy. Having scalable resources, well-defined roles, and protecting core incident response teams from unnecessary inquiries helped alleviate stress and anxiety. Good leadership and internal communication were crucial for maintaining situational awareness and focus during incident mitigation. Long-term negative effects included increased cynicism, fear of recurrence, and contemplations for a career change, which were mitigated by increased trust in colleagues, processes, and systems.

Introduction

The field of cybersecurity is often likened to a warlike environment[1, 2]. Cyberspace transcends geography, allowing threat actors to project attacks globally, making organisational defences perpetually contested. Cybersecurity professionals provide critical services to ensure business continuity in a constantly changing adversarial landscape[3]. Recent studies indicate high work-related stress in the cybersecurity profession[4, 2]. The VMware Global Incident Response Threat Report (2022) shows that 51% of cybersecurity professionals report burnout symptoms, with 65% considering leaving the profession. Understanding the psychological strain caused by cyber-attacks can help develop methods to mitigate these stressors.

Methods

Nineteen semi-structured interviews were conducted using an adapted version of the Critical Incident Technique (CIT)[5]. The interviews included structured questions on topics such as incident detection, thoughs and feelings during the incident, collaboration, actions taken, surprises, recovery, and long-term effects. The stuctured questions were elaborated when applicable. Each interview took approximately 1.5 hours. Prior to the interviews, participants sketched emotional journey maps to visualise their experiences during cyber incidents and pinpointed four critical events during the cyber incident (Figure 1).

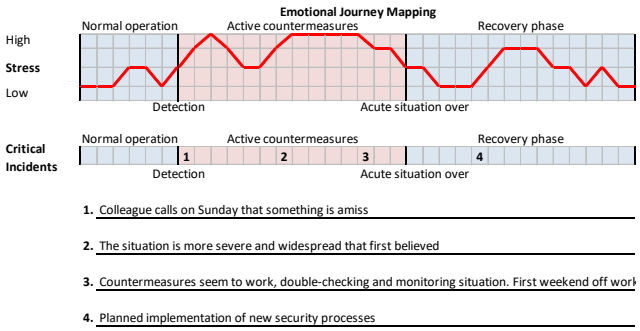

Figure 1. Example of the Emotional Journey Mapping and Critical Incidents.

These maps, commonly used in UX and service design[6], helped to guide the interview process and acted as a recall and visualisation aid for the interviewees. 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?"* Participants sketched their emotional journey mappings using seven categories: Stress, Mental Demand, Physical Demand, Temporal Demand, Effort, Performance and Frustration. Excluding Stress, the descriptions of the categories were based on the NASA Task Load Index (NASA-TLX)[7]. Descriptions for each scale category were provided (Table 1).

[1] B. A. Brody, "Cybersecurity akin to being in a war zone—you have to be "left of boom" to survive," 28 6 2015. [Online]. Available: 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].

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

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

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

[5] J. C. Flanagan, "The critical incident technique.," Psychological bulletin, vol. 51, p. 327, 1954.

[6] Nielsen Norman Group, "Journey mapping 101," 9 12 2018. [Online]. Available: https://www.nngroup.com/articles/journey-mapping-101/. [Accessed 23 JAN 2024].

[7] S. G. Hart, "NASA task load index (TLX)," 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)?

Table 1. Descriptions of emotional journey mapping categories.

Subjects

The 19 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[8]. They represented a variety of organisations and government service providers, including manufacturing, IT security providers, logistics, healthcare, central government, financial sector, local government, and educational institutions. Organisations varied in size and international presence. Interviewees included IR professionals (six interviews), IT security practitioners (eight interviews), and top executives (five interviews). The cyber incidents discussed were severe enough to risk operational continuity, cause major reputational damage, or involve the loss of sensitive information. Attacks included DDoS attacks, ransomware, and data exfiltration, with threat actors ranging from suspected state-sponsored APTs[9] to 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. All interviews were confidential, and results were aggregated to ensure anonymity.

Results

Emotional journeys

Average emotional mappings were calculated across all particiapnts (see Figure 2), which provide an estimate of the general direction on how cyber incidents impacted the individuals. Although the timeline of the emotional journeys does not have an exact schedule due to the variation in the duration of individual cyber incidents, it still contains two fixed points in time: the detection and and the acute situation being over, which were tied to a specific event for all respondents. Therefore, the interpretation of Figure 2 focuses on these events.

When a severe cyber incident is detected, it has the most significant impact on stress levels, mental demand, and temporal demand. Temporal demand rises almost immediately after the incident is detected, meaning that the urgency and the amount of time required to address the incident increase sharply right from the start. Stress and mental demand, on the other hand, build up more gradually. Initially, there is a rise in stress and mental effort as the situation is assessed and initial actions are taken. These demands peak a bit later, reflecting the ongoing pressure and cognitive load required to manage the incident. Interestingly, there is often a second peak in mental demand during the active countermeasures phase.

Physical demand remains generally low throughout the incident, even during the active countermeasures. This suggests that the physical effort required to manage a cyber incident is minimal compared to the mental and temporal demands. Estimates on the the required effort follows a pattern similar to stress and temporal demand. Quite surprisingly participants' own estimate on performance levels remained consistently high, despite the increased demands of the situation. Frustration levels varied widely among participants, meaning that the level of frustration experienced depended greatly on the specific incident and the individual's personal response to the situation.

[8] M. Hennink and B. N. Kaiser, "Sample sizes for saturation in qualitative research: A systematic review of empirical tests," Social Science & Medicine, vol. 292, 2022.

[9] Advanced Persistent Threat

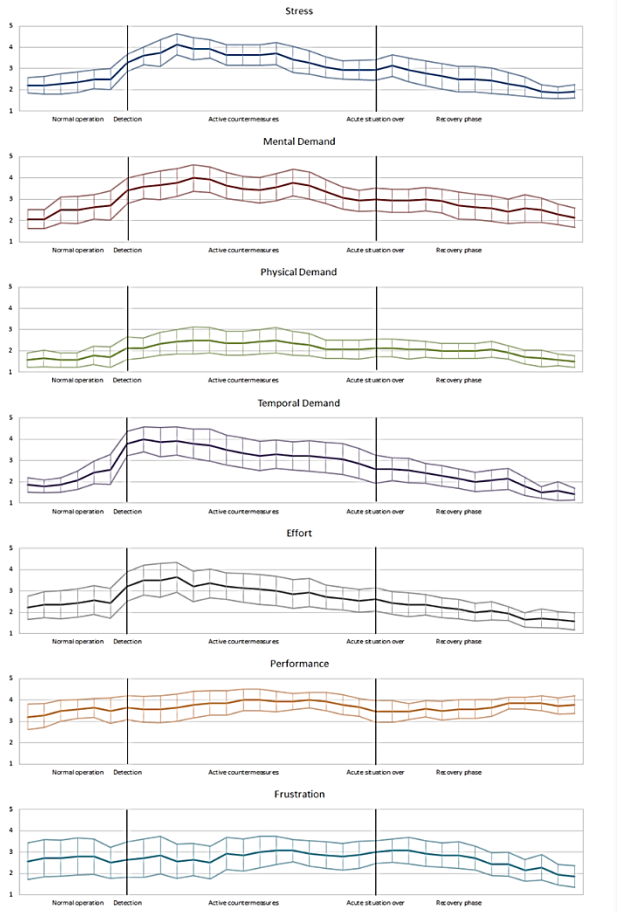

Figure 2: Average emotional journey mappings for each category. Thick central line represents average values, while the upper and lower line represents the high and low limit of the 5 % confidence interval.

Interviews

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

Interviews: IR professionals

IR professionals experienced less anxiety and stress due to their extenal role and were therefore able to distance themselves from the situation. They also had greater experience on various cyber incidents giving perspective to the situation. Many revealed that they continued to study and explore cybersecurity issues at home in their free time, driven by their strong interest in the field. Each new case was seen as an opportunity to learn and test their skills.

While their external role might shield them from the psychological effects experienced by the direct victims of a cyberattack, it introduced other types of stress. One of the most straightforward challenges was the need to set up and work at the customers' premises, often with less-than-optimal tools and ergonomics. Interestingly, unexpected stress arose from tense interactions with local IT support. This tension could be due to various reasons, such as the natural stress response of individuals in high-pressure situations. Another reason could be that local IT security practitioners felt their expertise was being challenged. There was also resistance from local IT support to making significant changes to systems within tight timeframes, changes that would typically be planned well ahead.

As a result, external IR professionals felt a significant amount of pressure to ensure their analyses and recommendations were absolutely accurate before presenting them to customers. This pressure, combined with the strong interest in the field posed a risk of burnout. Building trust and effectively communicating what needed to be done with customer representatives at all levels was seen as crucial by IR professionals. However, this created another challenge, as not all technically skilled individuals were adept at communicating with customers, and those who were good communicators might not always have the necessary technical understanding required for the discussions.

Interviews: IT Security practitioners

Local IT security practitioners had varying levels of experience with Incident Response Management, largely influenced by the size and type of their organisations. In smaller organisations, individuals often had more stretched roles, handling everything from cybersecurity to local IT support for end-users. In contrast, larger organisations typically had dedicated teams for cybersecurity. The less experience an individual had, the more stressful they found the situation. There was also a notable element of frustration, as many incidents could have been prevented if higher-ups had heeded their recommendations earlier or if end-users had followed information security guidelines properly. Despite this, all practitioners understood that their organisation's core business was not cybersecurity, and they had to make do with the resources available.

Upon discovering a severe cyber incident, IT security practitioners initially reacted with disbelief and hope that the situation was not as dire as it seemed. This was followed by a brief period of numbness as the reality of the consequences set in, with some individuals also experiencing despair and a sensation of being alone in the situation, even admitting to a brief urge to give up. Once they moved past the initial shock, many felt indecisive about what to prioritise, as everything seemed equally important and urgent. After the initial restriction and mitigation actions were completed, there was usually a moment of respite. However, this was often followed by additional efforts to ensure that unaffected systems were truly clean. It was critical for their well being to not overexert themselves during the acute mitigation phase, only to find that much work remained.

During the acute response and mitigation phase, some practitioners reported frustration due to micromanagement by middle managers, not fully understanding the situation and requiring documentation and approval for even smallest actions. On the other hand, end-users were eager to get their tools and software back, but their questions took time away from actual recovery efforts. Disagreements and frustration also arose from IT service employees at other locations, who might argue against the instructions given by the IT security practitioners. In hindsight, they recognized that as they and others were under high mental load and preoccupied with their thoughts, people might not acknowledge each others as well, sometimes forgetting simple courtesies like greeting colleagues in the morning. These behaviors could be misinterpreted as rude or hostile to others, potentially causing conflicts within the wider work community.

Existing incident management and recovery plans were considered valuable checklists, although these were not always applicable. In larger corporations, it was 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 assist with mitigation and recovery and their experience and expertise were deemend critical. In many organisations, there was no justification for having an internal IR team, as cybersecurity

was viewed as only an unavoidable expense for doing business. During the recovery phase and even long after, some IT security practitioners reported experiencing impostor syndrome. With better resources and improved visibility and controls in the networks, they felt anxious about the possibility of failing again. Additionally, a new and improved Security Information and Event Management (SIEM) system was often adopted after the incident. As with any new system, there is a learning curve before getting the full benefit from it.

Interviews: Top executives

Top executives primarily faced stressors related to leadership, resource management, communication, and overall responsibility. In the initial moments following the detection of such an incident, they had to engage in extensive communication with stakeholders, gather resources, personnel, and expertise to manage the situation. They often felt a deep sense of responsibility for the incident, accompanied by feelings of shame and remorse, even if there was nothing more they could have done with the resources available to them. Some executives also expressed concerns upon their reputation. This sense of a tarnished reputation could persist long after the incident was resolved, causing ongoing stress from even minor network issues.

A significant source of stress for top executives was the publicity surrounding the incident. Stress levels were particularly high when they had no control over when or how the incident would become public. For instance, if threat actors leaked sensitive information or if the media took an interest because the organisation provided a popular service that was disrupted by the attack. Additionally, public awareness of a cyber incident often led to further attempts against the organisation's systems, creating extra work for the IT security practitioners who were already busy mitigating and resolving the ongoing incident.

In many cases, top executives saw themselves as gatekeepers for the Incident Response (IR) teams, ensuring that these teams could focus on resolving the issue without being distracted by irrelevant inquiries. They felt responsible for their teams well-being. However, managing highly motivated and enthusiastic experts, who often strive for perfection, presented unique challenges. Executives needed to balance maintaining high motivation without allowing their teams to burn out. For example some experts reacted to crises by believing they were irreplaceable and took on tasks outside their responsibilities on their own initiative, leading to exhaustion and an inability to focus on the tasks in which they were the best authority available. Such unprompted actions could lead to faster burnout and increase the likelihood of fatigue-related errors. Therefore, it was important to clearly define roles for the IR team and IT security practitioners so that everyone knew their responsibilities and those of their colleagues.

Another source of irritation and frustration for top executives was dealing with managers and executives from other departments. Even if the organisation had an existing disaster recovery plan that outlined which systems were to be brought online first, there was always someone who tried to challenge it to prioritise their department's systems. Managers and executives from departments affected by the incident might try to deflect blame onto the Chief Information Security Officer (CISO) or other IT security managers, claiming they had not received recommendations to patch their systems or did not receive any help from the IT to address vulnerabilities. This behavior created a less than optimal working atmosphere and necessitated maintaining detailed records of agreements and timelines.

Interviews: General observations

Arranging a work-life balance during a cyber incident proved particularly challenging for individuals with small children. Interviewees noted that while their spouses and families were generally understanding and supportive, the incident often created tension at home. This tension arose because the bulk of household chores, childcare, and other responsibilities frequently fell on the spouse. Most interviewees also mentioned that they couldn't discuss the details of the situation at home due to confidentiality, adding another layer to the tension. It is quite common for threat actors to time their attacks during holiday seasons, further complicating the work-life balance. Only a few interviewees had previously discussed with their spouses that their cybersecurity roles might require them to be on call and work long hours. Another challenge to maintaining work-life balance came from significant personal events coinciding with the cyber incident, such as serious illness or the loss of a close relative, or major family gatherings like weddings.

Many interviewees found that engaging in activities requiring their full attention was the best way to take their minds off work. Physical exercise was frequently mentioned as an effective way to release stress and maintain general well-being. For those with families, playing and spending time with their children was also an effective way to unwind. Many interviewees reported that their work-life balance generally improved as they got older, settled down, and started families. Having some structure in life, such as a relationship, family, or even a pet, helped them avoid spending all their waking hours on computers. For many, cybersecurity was a topic of extreme interest and to maintain some level of work-life balance, many had developed strategies to limit their screentime. A common method was to avoid having computers or smart devices easily accessible at home. Another, less constructive method was using alcohol, as having a couple of drinks gave them the excuse to not work. Almost everyone mentioned that a good working atmosphere and humor were effective ways to relieve stress at the workplace.

Interviewees did not always emerge from severe cyber incidents unscathed and reported experiencing long-term symptoms similar to those associated with traumatic events. These symptoms included difficulty sleeping, hyper-alertness, cynicism, emotional numbness, and risk behaviors related to alcohol. According to the Diagnostic and Statistical Manual of Mental Disorders (DSM-5-TR), most cyber incidents do not meet the criteria for a traumatic event, as they generally lack the real or perceived danger of death or serious injury. However, it could be argued that severe cyber incidents can still be considered potentially traumatic. For some, the severe cyber incident acted as a catalyst for reflecting on their identity, what they wanted to do with their lives, and considerations of changing careers. Cybersecurity experts with small children seemed to seek a less demanding positions after the cyber incident. Severe cyber incidents also had a broader ripple effect within the organisation. End-users at all levels tended to lose trust in the system, which was often evident by the increased number of questions and tickets to IT security and the increased use of paper copies.

Discussion

This paper presented the psychological impact of severe cyber incidents based on 19 interviews. The study's limitations include the relatively small sample size and potential cultural dependencies, which might somewhat diminish the generalisability of the results. Although none of the interviewees were personally targeted by the cyberattack, those working in the affected organisations experienced the event as highly stressful. Coping with uncertainty, time pressure, and communication were

the prevailing stressors for cybersecurity professionals at all levels during a cyber incident. As a highly motivated group, cybersecurity professionals are at risk of burnout, especially during crisis situations.

Several best practices and recommendations to reduce the mental load of cyber incidents can be derived. Sharing information about the cyber incident with other industry members is highly recommended. 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 through periodic exercises. It is essential to ensure that all critical personnel get enough rest and nutrition during the incident. It is recommended that the core incident response team be protected from unnecessary inquiries so they can concentrate on the incident, while access to the war room should be limited to those actively participating in the incident response. Special attention should be given to communication, as misunderstandings can cause unnecessary conflicts within the organisation. In addition to general lessons learned events after the incident, arranging debriefing sessions focused on mental and physical well-being, led by a healthcare professional, could be beneficial.

Although this study focused on the negative impacts of cyber incidents, these events can also positively impact team cohesion, give a sense of purpose to one's work, and act as a baptism by fire for professionals. Very often, a cyber incident acted as a catalyst for eliminating insecure legacy systems and securing sufficient resources for maintaining and improving cybersecurity within the organisation. Further research is needed to verify these findings with a questionnaire study and explore potential cultural differences between countries and organisations.

Acknowledgements

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

For More Information

Dr Toni Virtanen (p. 0299 550 800) is a cyberpsychologist and a researcher at the Finnish Defence Research Agency (FDRA).