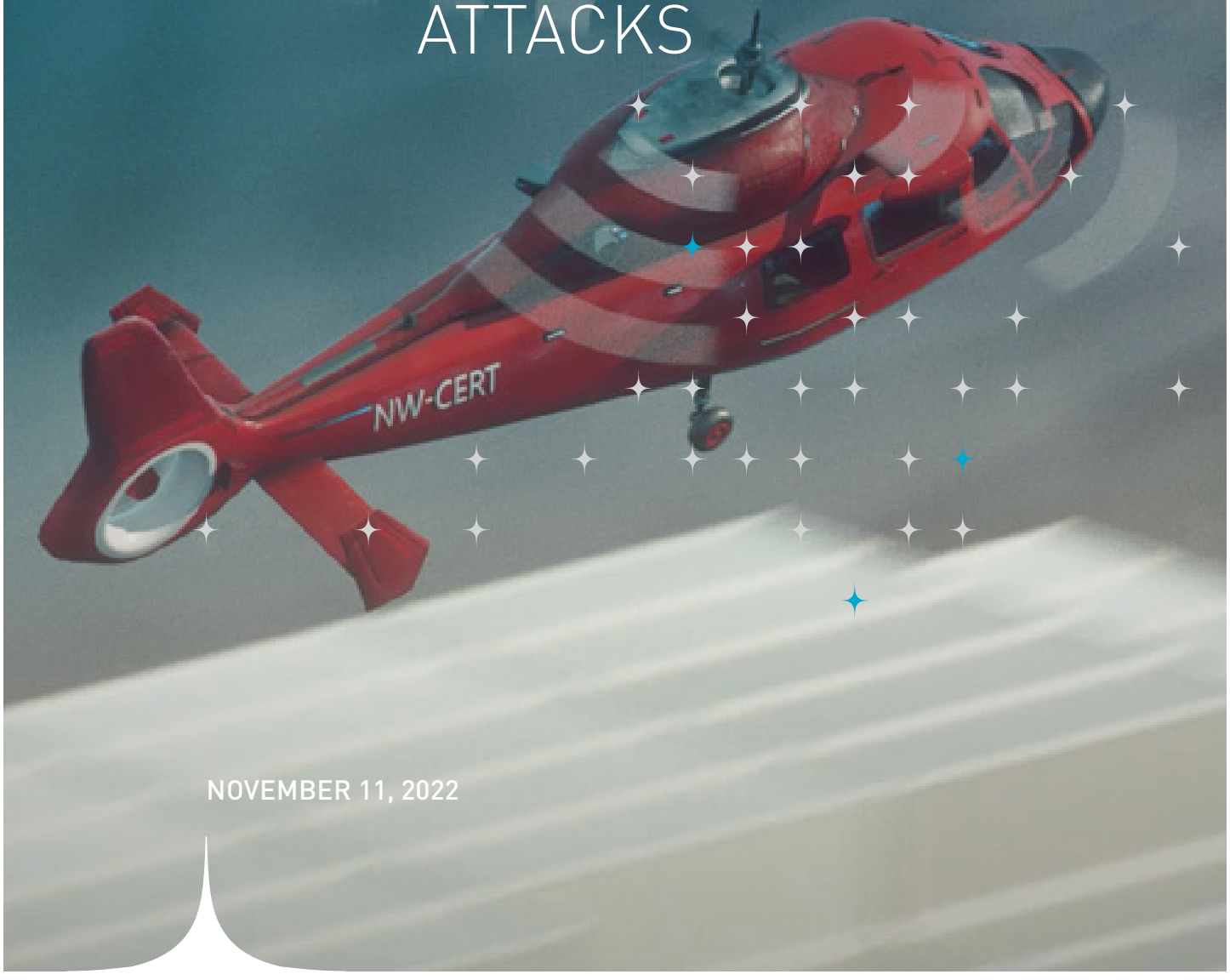
NORTHWAVE
Intelligent Security Operations

NORTHWAVE

AFTER THE CRISIS COMES THE BLOW – THE MENTAL IMPACT OF RANSOMWARE ATTACKS

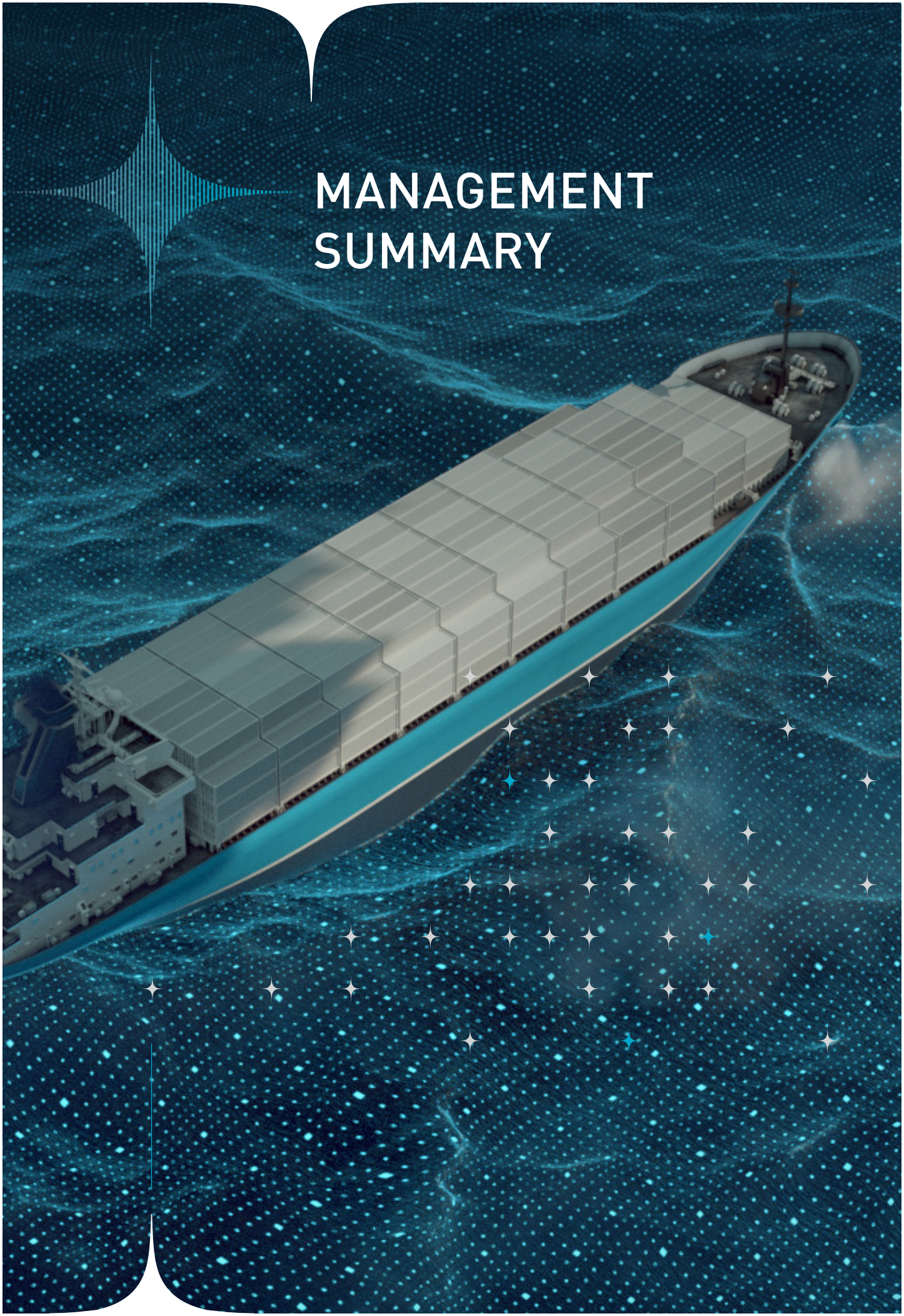


NOVEMBER 11, 2022

CONTENTS

NORTHWAVE BV
Visiting address: Van Deventerlaan 31-51, 3528 AG, Utrecht, the Netherlands
Postal address: P.O. Box 1305, 3430 BH Nieuwegein, the Netherlands
E-mail: info@northwave.nl
Head office phone number: +31 (0) 30 303 1204
NW-CERT (24*7) The Netherlands: 0800 – 1744
NW-CERT (24*7) International: +31 (0) 800 22 55 2747
Website: northwave-security.com

MANAGEMENT SUMMARY



MANAGEMENT SUMMARY

We examined the mental impact of ransomware incidents on CERT employees, managers, and employees. We did that using a combination of a survey in our own CERT (Computer Emergency Response Team), interviews with CEOs, IT managers and other managers of 11 affected companies, and a survey among 352 employees of affected companies.

These are the 10 most important findings:

1. **The impact of ransomware incidents on mental health is large**. In our Mental Impact of Ransomware Attacks (MIRA) phase model, we describe that these effects occur not only during the first, hectic phase of an incident, but persist across 3 phases: the first week of the attack, the first month after the attack, and the year after the attack.
2. **Sleeping problems** are among the most frequently reported symptoms in all phases. Sleeping problems are common among CERT members (81%), and employees report sleeping problems in phase 1 (60% of those directly involved), in phase 2 (42% of those directly involved) and in phase 3 (mentioned in 7 out of 11 interviews).
3. **Unhealthy coping mechanisms**, such as eating junk food, drinking alcohol or smoking, **are apparent during the first phase** of dealing with a ransomware attack, but have negative long-term consequences.
4. **Guilt is a common emotion during the first two phases of a ransomware attack**. This includes guilt towards the homebase (reported by 48% of CERT members). In the interviews, people also expressed guilt towards the organisation *"I should have seen this coming"*.
5. **About 2 in 3 of all employees**, including those not directly involved in the attack, **now believe that the world is a dangerous place**.
6. During the third phase of dealing with ransomware incidents, up to a year after the incident, **about 1 in 7** of those directly and indirectly involved in the recovery from the attack **have symptoms of trauma severe enough to require psychological help**.
7. **About 1 in 5** of those who were directly or indirectly involved in resolving the attack **considered or are still considering changing jobs**.
8. Across the board, impact on mental health appears to be similar for those directly involved in dealing with the ransomware attack (e.g., the IT team) and those indirectly involved (e.g., advising those directly involved). Therefore, **efforts to mitigate consequences for mental health should not be limited to the most visible groups**.
9. There were strong associations between physical and mental health symptoms across the phases of the MIRA phase model. This emphasises the **importance of early detection of mental health impact, as those who suffer from the start may continue to suffer in the future**.
10. Of those directly involved, 20% indicate that they would have liked more **professional help** to deal with the mental impact, 67% wants to **evaluate with team members** after the incident, 32% desires **concrete tools to deal with the impact of the attack** themselves, and 43% desires concrete advise on how to help others.

To mitigate the negative effects of ransomware attacks, companies can start with preparing for the mental impact of such attacks in a ransomware response plan. Additionally, in the distinct phases of the MIRA phase model, different measures can be taken.

ADVICE PER PHASE

PHASE 1	PHASE 2	PHASE 3
Make sure there is sufficient rest	Manage the workload of the incident team wisely	Monitor mental health
Have regular check-ins	Create a safe working environment	Plan evaluation sessions
Monitor coping mechanisms	Set realistic expectations	Offer tools to deal with the mental impact

INTRODUCTION: WHY WE CONDUCTED THIS RESEARCH

INTRODUCTION: WHY WE CONDUCTED THIS RESEARCH

Ransomware attack volumes increased with 105% year after year and is up 232% since 2019[1]. Thus, one would expect that by now we know everything there is to know about the phenomenon ransomware. Indeed, knowledge has increased tremendously on subjects such as who commits ransomware attacks, which methods of attack are used and how we can set up our systems to prevent ransomware attacks. Knowledge on the visible, tangible impact of attacks has grown rapidly in the past few years, such as the operational impact and the monetary impact. But we noticed more impact...

At our Northwave Computer Emergency Response Team (CERT), we daily help customers to recover from ransomware attacks. One thing we noticed in every single case is the enormous impact these incidents have on employees of the victim company. Months, or even years after we have helped companies to resolve the effects of an attack on their systems, we notice that people still struggle with what happened to them. Therefore, we asked ourselves the question: what about the human side of all of this? Does ransomware have an invisible – maybe long lasting – impact on the people involved? We could not find any research on this specific subject, so we started our own research.

Our main goal with this research was to examine what the impact of ransomware attacks on mental health is. We conducted 3 studies to examine this mental impact. First, we studied the mental impact of ransomware attacks in our own CERT. How do they deal with the stress, long days, and emotions from the customer? We administered questionnaires among CERT members and had conversations with our crisis managers. This resulted in some adjustments in the way we work to keep the stress level within the team as low as possible during deployment and to ensure enough time for recovery. Then we approached several victim companies that we have helped to recover from a ransomware incident. Second, we conducted in-depth semi structured interviews with board members and IT managers. Third, we conducted questionnaires across the organisation, with employees directly involved in resolving the attack, employees indirectly involved and employees not involved. These questionnaires were based on scientifically validated scales (for details, see Appendix 3).

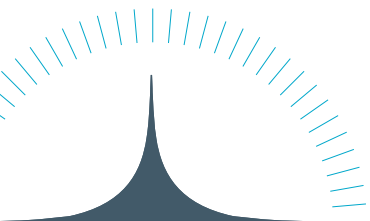
Study	Target	Method
Study 1	Northwave CERT	Questionnaires
Study 2	Victim companies (C-level, it-managers)	Semi-structured interviews
Study 3	Victim companies, all employees (directly involved, indirectly involved, not involved)	Questionnaires

In this report, we outline the results of these studies. To understand why ransomware attacks can have such a high impact on mental health, it is important to first understand what ransomware attacks entail. In the chapter Background: Why can ransomware have such a big effect?, we describe what a ransomware attack looks like and present our Mental Impact of Ransomware Attacks (MIRA) phase model, in which we describe the various phases that companies facing a ransomware attack go through. In the chapter People involved in solving the attack, we describe the key players who are involved in resolving the ransomware attack, and who were included in our research. In the chapter Study 1: mental impact of ransomware attacks for CERT members, we describe the results of our first study, which examined the mental impact of ransomware attacks among CERT members. In the chapter Study 2 and 3: mental impact of ransomware attacks in companies, we describe the results of our second and

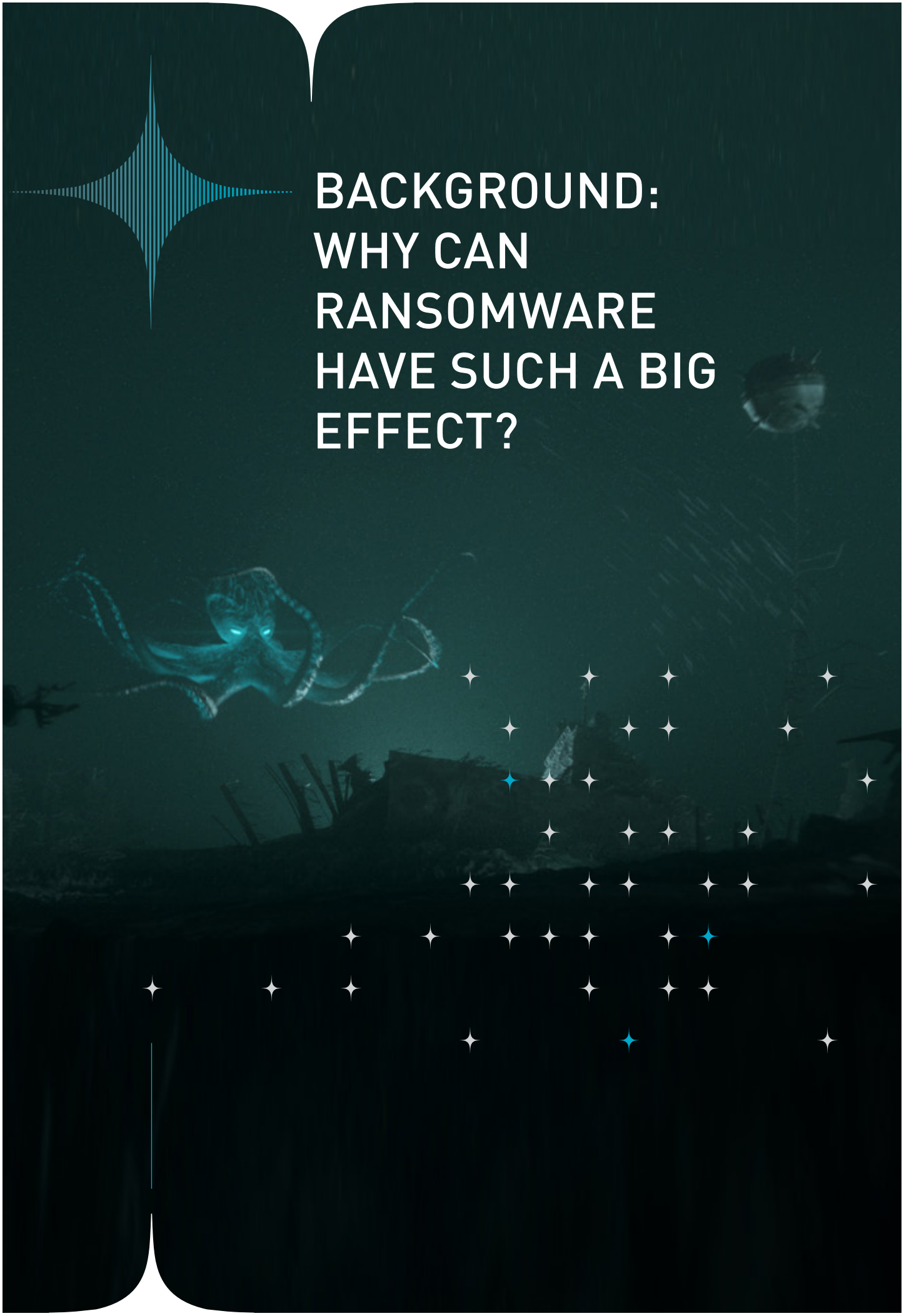
1. SonicWall (2022). SonicWall Cyber threat report.

third study, in which we examined the effects of ransomware attacks in companies. In chapter Mitigating the mental impact of ransomware attacks, we describe what those involved in resolving ransomware attacks indicate they need to mitigate the effects of ransomware attacks.

Based on our research, we also describe what managers can do to mitigate the effects of ransomware attacks and what Northwave can do to help with this. In the Conclusion chapter, we reflect on the main conclusions that can be drawn from the study. Finally, in appendices 1, 2 and 3, we provide a complete overview of the methods and results of all three studies.



BACKGROUND: WHY CAN RANSOMWARE HAVE SUCH A BIG EFFECT?



BACKGROUND: WHY CAN RANSOMWARE HAVE SUCH A BIG EFFECT?

Some people may be surprised to learn that ransomware attacks can have a huge impact on mental health. To understand why the mental impact can be so big, it is first necessary to understand what a ransomware attack looks like. In this chapter, we describe what ransomware is and who the threat actors are that perform a ransomware attack. Finally, we present our MIRA phase model, which describes the phases a typical company goes through when dealing with a ransomware attack

WHAT IS RANSOMWARE?

Ransomware is a form of malicious software that threat actors use to encrypt their victims' computer systems or files. This encryption makes it impossible to access any file on the affected servers and computers. For companies, this usually means that they cannot perform key business processes, because important (communication) systems and files are inaccessible. Before starting the encryption, a threat actor attempts to tamper with or destroy the backups and looks for sensitive data to steal. Then, their ransomware is deployed on a large scale within the victim's IT environment, making sure that as much as possible is encrypted.

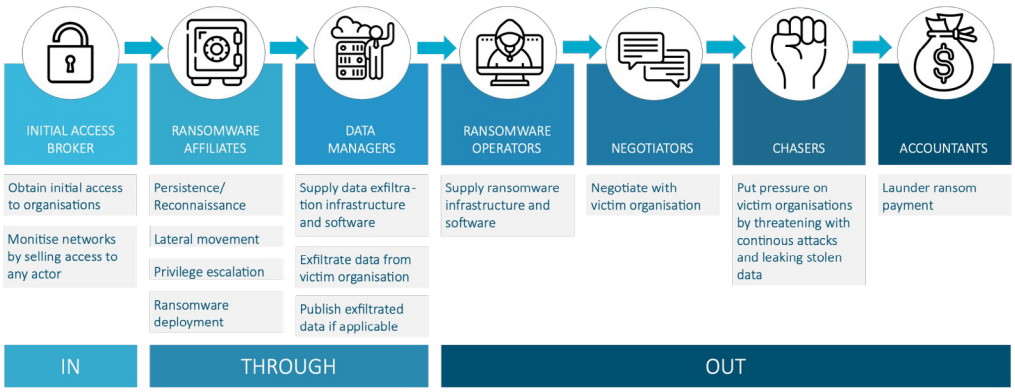
After the encryption is deployed, the threat actor demands a significant sum of money, called the ransom, to provide the keys needed to regain access to your data. Nowadays, criminals use several other methods to put additional pressure on companies to pay the ransom, this is called 'double extortion'. As the criminal tampers with the back-ups, they are now unavailable, putting extra pressure on the victim company. Next to this, the threat actors steal large amounts of sensitive data which is threatened to be leaked on so-called "leak sites" that reside on the Dark web. Sometimes criminals even call employees of the company to apply even more pressure or combine ransomware with other forms of attacks such as DDoS, resulting in a triple extortion scheme. Because of these threats, organisations that fall victim by ransomware often experience significant, immediate impacts on their day-to-day business.

WHO ARE WE BATTLING?

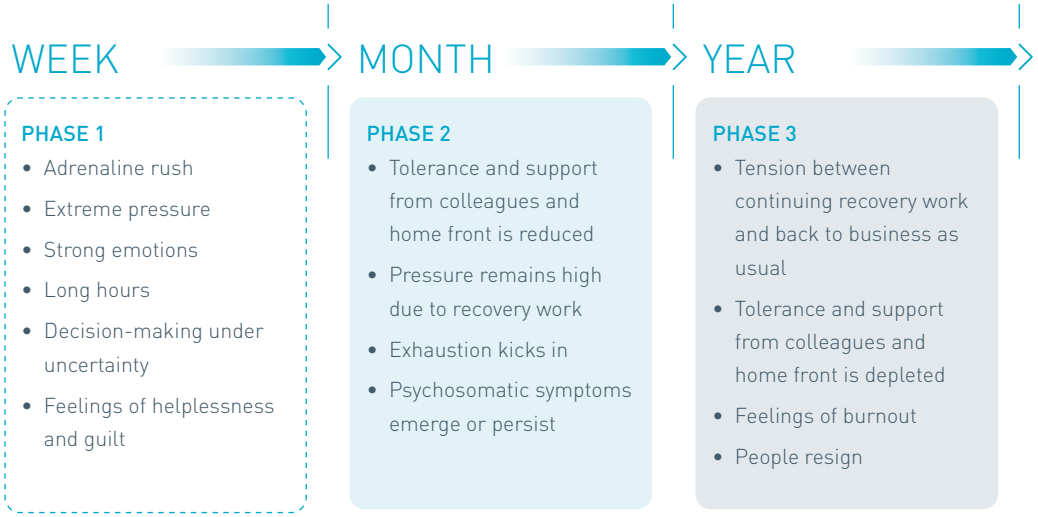
When people think of the threat actors responsible for ransomware attacks, they often picture 'the lone boy in the attic'. However, this is no longer a realistic image. We see that ransomware groups are highly professional operating organisations with a lot of expertise. It is thus important to keep in mind that when you protect your company from ransomware attacks, you are up against organized crime.

Ransomware organizations use different actors for each phase of the ransomware attack. All these actors have high expertise to carry out the actions. For an overview, see the figure below.

RANSOMWARE THREAT ACTORS



PHASES IN THE MIRA PHASE MODEL.



THE MIRA PHASE MODEL

When dealing with professional threat actors, recovery after an attack is difficult and time-consuming. In fact, on average it takes about 23 days to get most of the systems up and running again. When looking at the visible, tangible impact of ransomware attacks, that there are roughly three phases that companies go through to recover from the attack. During those three phases, the mental effects also differ. We describe those phases in our Mental Impact of Ransomware Attacks (MIRA) phase model. The figure below describes what happens in a company in each phase of responding to a ransomware attack, where we roughly distinguish between the first week, the first month, and the first year after the attack. In the remainder of this report, we describe the mental impact in those phases.

PHASE 1
• Adrenaline rush
• Extreme pressure
• Strong emotions
• Long hours
• Decision-making under uncertainty
• Feelings of helplessness and guilt

PHASE 1 - WEEK

During the first week of the attack, the goal is to quickly mitigate the damage of an attack, remove any remaining threats or attackers from the systems, and get back to business as usual as quickly and safely as possible. As the whole business has come to a standstill there is a lot of pressure on those tasked to fix the problems. Eradicating the threats from the system is time-consuming and involves several manual steps or decisions with wide-ranging consequences, such as changing all passwords. It is often assumed that restoring backups is enough to continue business as usual. In reality, ransomware attackers have often infiltrated deep into the network, meaning that the backups are often already destroyed or infected.

Due to the high pressure to get systems up and running again, people mostly work on adrenaline. Those involved make 12 to 16-hour working days, with high pressure, focus and extremely tough workloads, even on weekends. As there is little time left for anything other than work, unhealthy food is ordered, and exercise is skipped. These are easy ways to gain extra working hours. Family and other important social relationships are often ignored, or do not get the attention they usually get, which may result in a lack of understanding at home.

PHASE 2 - MONTH

PHASE 2
- Tolerance and support from colleagues and home front is reduced
- Pressure remains high due to recovery work
- Exhaustion kicks in
- Psychosomatic symptoms emerge or persist

After the first week, the first basic functionalities are getting back online, but most key processes are still down or running manually. The IT team is still removing the ransomware from the IT environment and taking measures to prevent an attack from happening again, such as network segmentation, updating all systems, security monitoring, and enabling Multi-Factor Authentication (MFA). But during this period, the IT team is not only responsible for recovering all systems from the attack, but also for providing support to the IT systems that are already up and running.

At this point, adrenaline is running out and people are getting exhausted, but the pressure is still high. The pressure is now coming from personal life, as families do not understand why work is suddenly so important and demanding. Colleagues are also starting to add pressure, as they complain about why everything is taking so long and why they must create new passwords. While the IT team is still up to their ears in the crisis, their colleagues often do not understand what the IT team is still dealing with. For them, time just goes on, and they are less aware of the work that still needs to be done to recover all the systems. Thus, colleagues start asking questions about regular projects, increasing the workload.

PHASE 3 – YEAR

PHASE 3
- Tension between continuing recovery work and back to business as usual
- Tolerance and support from colleagues and home front is depleted
- Feelings of burnout
- People resign

More than one month after the attack, business as usual is resuming. The IT team is still working on the long tail of the recovery. It has become a project – implementing security improvements, restoring the last systems, migrating others – it feels like it never ends. Because for most employees it's business as usual again, they start to forget about the crisis. We can feel that the sympathy for the IT team is dripping away. At the same time, the IT team still feels exhausted after weeks of crisis and months of pressure.

CONCLUSION - WHY DO RANSOMWARE ATTACKS HAVE LASTING IMPACT?

During the long period of downtime, there is uncertainty about the future, and no one knows whether the company will be able to survive. C-level executives are often used to working under such high pressure, being away from home a lot, and making complicated decisions under unclear circumstances. But others involved in the process, such as members of the IT team or people responsible for crisis communication, are usually not used to the enormous pressure, responsibility, and immense workload. In the first phase, those involved in dealing with the attack have a high workload. In the second phase, pressure from home and colleagues increases. In the third phase, when understanding diminishes, those involved in directly dealing with the attack still experienced increased work pressure, and the months of pressure start to weigh more heavily. It is thus not hard to imagine that ransomware attacks can have lasting impact on people's mental health.

PEOPLE INVOLVED IN SOLVING THE ATTACK

ROLES IN A RANSOMWARE ATTACK

A ransomware attack is handled by multiple groups of people, which are all included in this research. In this chapter, we briefly describe who those people are.

CERT

CERT stands for Computer Emergency Response Team. Northwave is one of the few Dutch organisations with its own publicly available CERT (NW-CERT). The NW-CERT coordinates incident response activities during a security incident, performs forensic investigations, helps organisations mitigate the attack, recover the operation, and provides advise on the next steps to prevent a future occurrence.

Northwave is licensed by the Ministry of Justice and Security to conduct private investigations to (security) incidents. The members of the CERT of Northwave are certified as private investigators, possess extensive experience in digital forensics and security and hold certifications such as FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA), FOR500: Windows Forensic Analysis (GCFE) and MS500 & AZ500.

The team currently has over 40 members, including former police officers and former employees of intelligence and security services. Their skills and expertise include crisis management, incident management, incident response, malware analysis, network & system forensics, and attacker communication. The exact incident response team differs per situation, depending on the desired skills and expertise for the incident. The team will always contain an Incident Response Coordinator and can be extended with NW-CERT employees and other Northwave employees with specific expertise, such as a Network Architect, Microsoft Expert and Offensive Specialist. Besides expertise within Northwave, we have connections with security organisations and communities and the police. We conducted a first study among 21 of our own CERT members, using a questionnaire.

MANAGEMENT OF VICTIM ORGANISATIONS

C-level managers, IT managers and other higher-level management are often involved in the crisis response team, which is responsible for the daily coordination of the response to the ransomware attack. To assess their experiences, we conducted a second study, with interviews with representatives of those groups of 11 companies. These interviews were conducted approximately 1 year after the ransomware attack. In the interviews, we focused on personal experiences with physical and mental symptoms during the ransomware attack and the time thereafter, and experiences of employees during the attack.

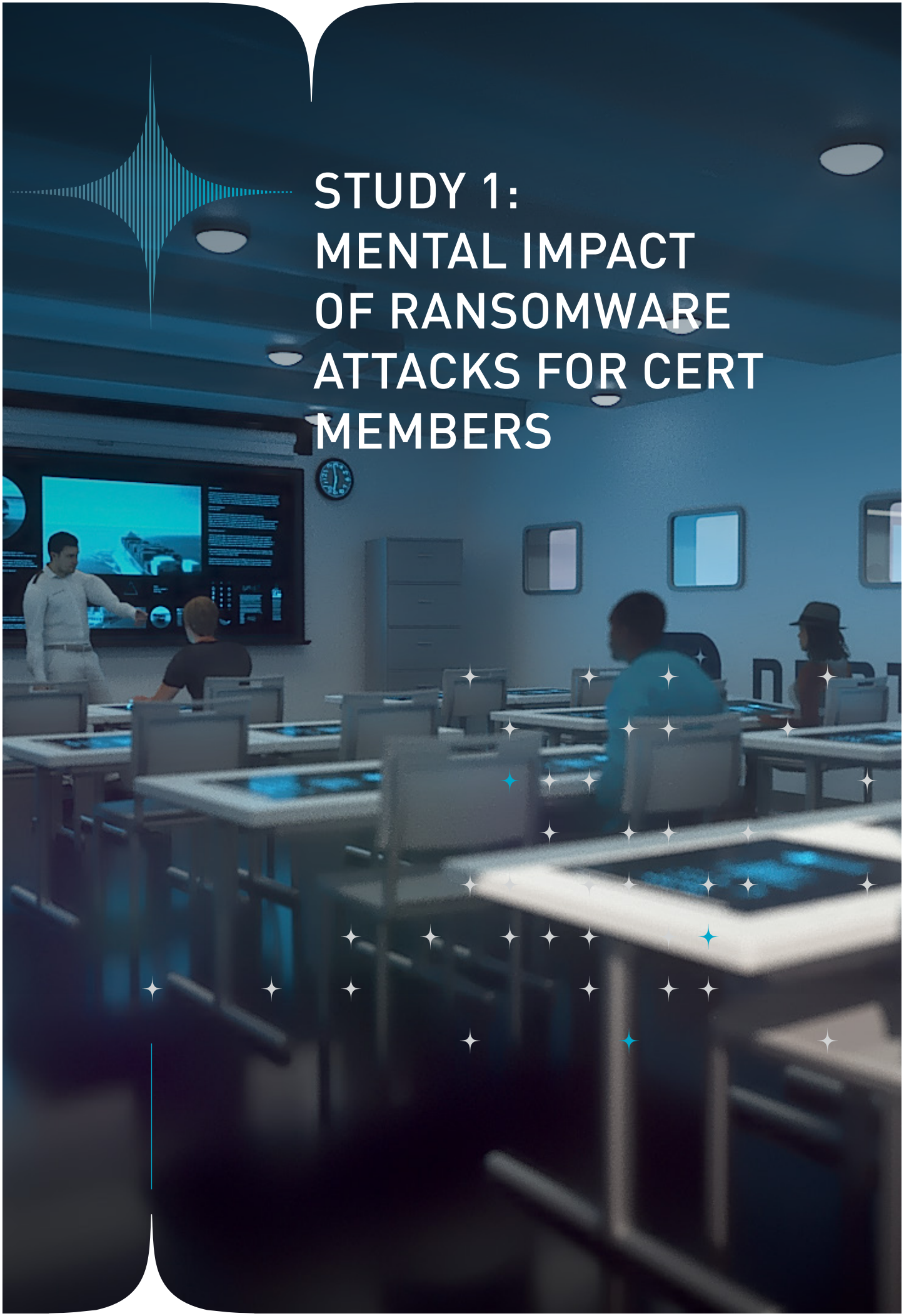
EMPLOYEES

Other employees also FEEL te consequences of a ransomware attack, but their level of involvement in dealing with the attack varies. In a third study, we conducted a survey among 352 employees of companies that had been hit by a ransomware attack. We distinguished between 3 types of employees:

1. Employees who were **directly involved** (38.1%) in responding to the ransomware attack. For instance, people in the IT team or people who were involved in crisis communication.

2. Employees who were **indirectly involved** (32.1%) in responding to the ransomware attack. For instance, people who had to take over tasks from those directly involved or who gave advise to those directly involved.

3. Employees who were **not actively involved** (29.8%) in responding to the attack. For instance, those employees who were largely able to continue their daily work.



STUDY 1: MENTAL IMPACT OF RANSOMWARE ATTACKS FOR CERT MEMBERS

STUDY 1: MENTAL IMPACT OF RANSOMWARE ATTACKS FOR CERT MEMBERS

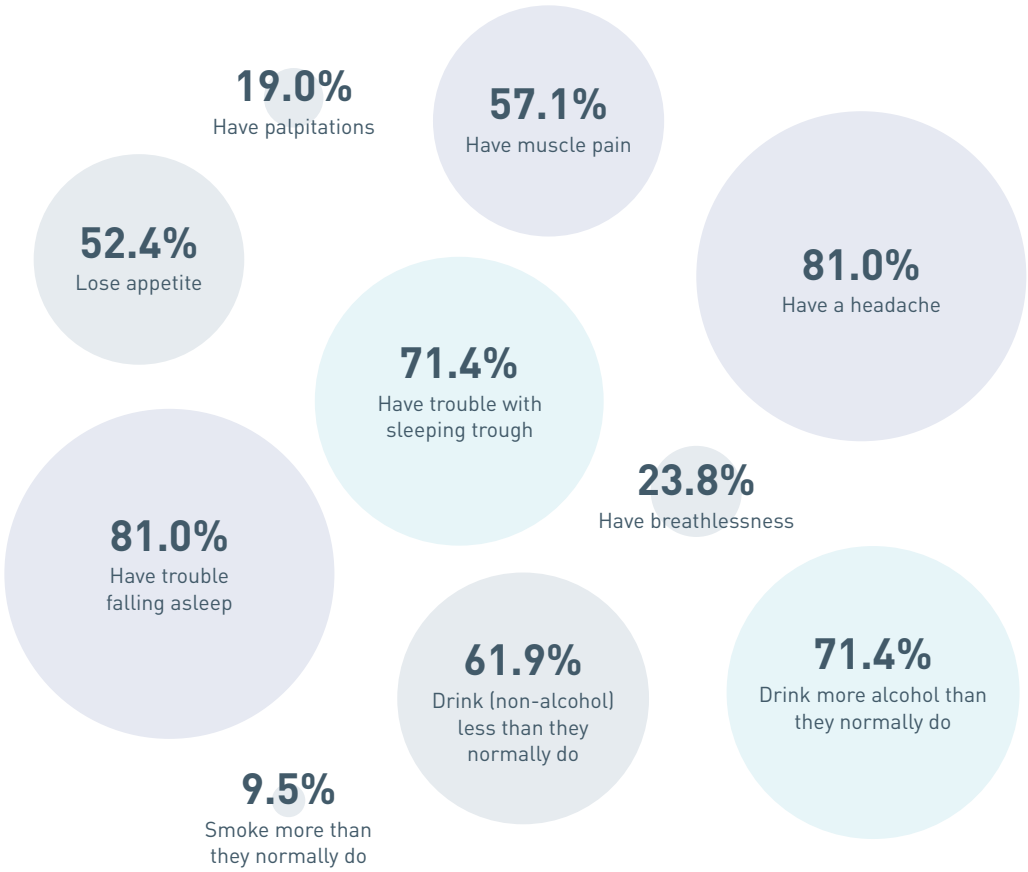
Our first study focused on the mental impact of ransomware attack for CERT members. An earlier report indicated that 65% of cybersecurity incident responders have sought mental health assistance in relation to responding to cybersecurity incidents[2]. We examined the mental impact of ransomware attacks among 21 of our own CERT members, and found the following results.

STRESS

First, we focused on stress experienced during the different phases of incidents, namely during the intake with a client, during deployment, during the incident and after the incident. While some CERT members do not experience high stress at all, 38.1% of them experienced a stress level of 5 or higher on a scale of 1 to 10 during intake, compared to 61.9% of CERT members during deployment, 52.4% during the incident, and 9.5% after the incident.

Interestingly, experience with incidents is not a strong predictor of perceived stress; only during intake does stress seem to be higher for those with less experience. At other times, the correlations are small and not significant. CERT members also indicated how high their stress tolerance was, for instance by indicating whether they enjoy working under pressure, whether they get stressed easily, and whether they get physical or mental symptoms when they are stressed. Stress tolerance predicted perceived stress during the incident, but this relationship was not significant for the other phases of an incident.

Thus, it seems like incidents are stressful for CERT members, irrespective of how well they can usually cope with stress, and irrespective of how much experience they have with ransomware incidents.



2. IBM (2022). Security Incident Responder Study.

GUILT AND RESPONSIBILITY

Besides stress, we also examined other feelings experienced during different phases of the incidents (for details, see Attachment 1). For each phase of an incident, CERT members reported on 11 feelings on a scale of 1 to 5.
During the incident, feelings of guilt towards work (23.8%) and feelings of guilt towards private life (47.6%) are common, and these feelings persist after the incident for both work (23.8%) and private life (42.3%). This number is comparable to that reported in an earlier study, in which 44% of incident responders reported an impact of cybersecurity incidents on their social life or relationships[2]. In line with this, 81.0% of CERT members rate the impact of an on-site incident on their private life with a 5 or higher, with an average impact of 7.3 on a scale of 1 to 10 across all CERT members.

We also see that the levels of compassion for the customer are high, especially during the incident (76.2%). This is consistent with findings from an earlier report, which noted that the sense of duty among cybersecurity incident responders is very high, but that this sense of responsibility is also among the most stressful factors during an incident[1]. This may explain why CERT members have such a high sense of responsibility. Even though many CERT members have a need for rest and lack sleep, 61.9% of CERT members indicate that they do not feel comfortable starting later in the morning if colleagues start earlier, and 57.1% do not feel comfortable leaving early in the evening when colleagues continue to work.

PHYSICAL SYMPTOMS

Physical symptoms are quite common among CERT members. For instance, many CERT members (52.1%) experience loss of appetite at least sometimes. In addition, CERT members often have trouble falling asleep (81%) and have trouble sleeping through (71.4%). As one team member said:

"During an incident I had trouble sleeping. I was even sleepwalking: I dressed myself in my sleep and got back to bed, but I have no clear memory of doing that."

Headaches (81.0%) and muscle pain (57.1%) are also common. Part of these physical symptoms may be the result of changes from peoples regular lives. A CERT member indicates: *"I often feel weak because I cannot work out. On many incidents, we are only offered a lot of unhealthy food, and that for days in a row. This makes me feel unwell".* Unhealthy food is also mentioned as a problem by others. One of the CERT team members indicates: *"I even get skin rashes from the lack of sleep and the unhealthy and untimely food".*

CONCLUSION

Our first study confirms findings of earlier studies indicating that the mental impact of ransomware incidents can be high for incident responders. CERT members experience amongst others high stress levels, sleeping problems, guilt towards home, and physical symptoms such as headaches. The mental impact does not seem to be related to the level of experience or people's preference for stress, indicating that we should be aware of signs of impact on mental health for all CERT members. Based on the findings in this study, we have implemented some changes in how we handle incidents for our own CERT members (see Mitigating the mental impact of ransomware attacks).

STUDY 2 AND 3: MENTAL IMPACT OF RANSOMWARE ATTACKS IN COMPANIES

STUDY 2 AND 3: MENTAL IMPACT OF RANSOMWARE ATTACKS IN COMPANIES

To examine the mental impact of ransomware attacks in companies, we used a combination of quantitative and qualitative research. For study 2, we interviewed of interviews with CEOs and IT managers. For study 3, we conducted quantitative research among employees of companies that were hit by ransomware attacks. In this chapter, we report the results of those studies, separately for each phase of the Mental Impact of Ransomware Attacks (MIRA) phase model: the first week after the attack, the first month after the attack, and a year after the attack.

PHASE 1
- Adrenaline rush
- Extreme pressure
- Strong emotions
- Long hours
- Decision-making under uncertainty
- Feelings of helplessness and guilt

MIRA PHASE 1

SYMPTOMATIC SYMPTOMS

In our quantitative study, we examined what somatic symptoms people experienced during the first week of a ransomware attack. Some of the most striking findings are that, among the 352 employees who filled out the questionnaire:

- In total, 47.8% of employees experienced trouble sleeping in the first week after the attack. This was most common in those directly involved (60.0%) and least common among those not involved (35.0%).
- 43.8% of those directly involved and 37.1% of those indirectly involved experienced headaches
- 30.4% of those directly involved and 31.9% of those indirectly involved experience backpain.
- 54.3% of those directly involved and 46.9% of those indirectly involved reported feeling tired or low energy.
- All symptoms taken together, 20.0% of those directly involved, 18.9% of those indirectly involved but only 10.4% of those not involved score medium to very high.

Tiredness and trouble sleeping thus seem to be among the most common problems during the first week of a ransomware attack. Indeed, as one interviewee indicated: *"Every day that our production was shut down, cost us a million euros. But we also lost money because of all the other departments that were shut down. So, I was very stressed, I couldn't sleep anymore."*

We examined whether there were significant differences between those directly involved, those indirectly involved, and those not involved in dealing with the ransomware attacks. We found significant differences between those groups for all symptoms mentioned above. Interestingly, both those directly involved and those indirectly involved differed significantly from those not involved, but those directly and indirectly involved did not differ significantly from each other. Thus, in terms of experienced symptoms, it does not seem to matter if employees are involved more directly or more indirectly.

"A member of the IT team suffered a heart attack."

Symptomatic symptoms also became clear in the interviews with victims of ransomware attacks. Even so, a member of the IT team suffered a heart attack because of the severe stress their team had been put under. Two of the interviewees mentioned explicitly having a way higher blood pressure than usual. A CTO states *"I was already taking medication for high blood pressure but during the incident my blood pressure became sky-high. So, I had to take a higher dose. My blood pressure returned to normal a bit three months after the incident."*

K. van der Plas, general practitioner, is not surprised by these effects. He explains: *"people that are exposed to acute or prolonged extreme stress have a higher risk of heart and vascular diseases, such as heart attacks. This is especially the case in persons who are closely involved in the event. Therefore, the impact of ransomware attacks on health should be taken very seriously."*

COPING MECHANISMS

Coping is the actions people take to deal with the stress of an unusual situation[3]. Some coping mechanisms seem to feel good in the moment because they offer some relief, but potentially have long-term negative effects. This is known as unhealthy coping, and includes tactics such as over- or undereating, sleeping too much or too little, or aggression. In contrast, healthy coping mechanisms, such as seeking social support, exercising, or eating healthy may not feel like immediate stress-relief, but they do lead to long-term positive outcomes[4].

UNHEALTHY COPING MECHANISMS

In 8 out of 11 interviews, interviewees mentioned unhealthy coping mechanisms among which eating junk food, no sleeping, or no sporting. Two interviewees also said that they gained weight because of the incident. The average amount of kilos gained was 8.5 kilos. Not taking rest at all was also prevalent. An IT representative of a victim said *"there were very long days, with continuously high stress. After a week I felt exhausted. And after two weeks we agreed to go home for a few hours and take a bit of rest."* This illustrates the lack of rest and sleep that the people directly involved get. Because of the stress, employees had to pick and choose which coping mechanisms to use. With very little time, that sometimes meant making hard choices, sacrificing some needs for others. An interviewee said: *"If I could sleep, I would fall asleep like a log and get up again to go to work. I didn't talk to my wife and children because I didn't see them anymore."*

"During the incident, you live on adrenaline. We worked for 20 hours a day. After the incident, I collapsed. I had a short fuse and I had problems concentrating."

HEALTHY COPING MECHANISMS

Fortunately, healthy coping mechanisms were also brought up during the interviews, although in minority in comparison to unhealthy coping mechanisms. Several companies applied different problem-solving techniques. For example, many of those closely involved to the ransomware attack, were unable to spend time with their loved ones for weeks. One director IT said he brought their sick son to the office, so he could still spend time with him. Many of the interviewees fortunately experienced social support in one way or another (from their management or direct colleagues); however, we can call it a way of healthy coping when they actively seek for social support. For instance, one interviewee said: *"I was very tired, but I chose not to go to sleep right away. Instead, I drove to my girlfriend's home, opened the window, and talked with her. I emptied my head to her, and it really gave me support to be able to tell my story."* Therefore, actively seeking out social support seems to make a difference in the stress levels that the incident responders experience.

3. https://dictionary.apa.org/coping
4. Therapist AID LLC, 2018.

"An IT director brought his sick son to the office, so he could still spend time with him."

PHASE 2
- Tolerance and support from colleagues and home front is reduced
- Pressure remains high due to recovery work
- Exhaustion kicks in
- Psychosomatic symptoms emerge or persist

MIRA PHASE 2

GUILT

Feelings of guilt and neglect of the home front is an issue that persisted during the first month of ransomware attacks. Five of the interviewees mentioned this as a problem during the incident. A director IT said: *"The network administrator collapsed after 3 days because he didn't get out of the blame reasoning circle and blamed himself. The question of guilt haunted him for a long time."* Others also state that they had barely been home for days to weeks. And when they were at home, they felt easily irritated with things that would usually not bother them, because of their exhaustion. A CTO states: *"I was fiery at home. I had to re-introduce myself at home because I had worked such long days. It could have led to a huge rift at home. A ransomware attack feels like a divorce."*

"You really feel you are overworked. After the incident I collapsed because of the fatigue and stress."

SYMPTOMS

We also examined other symptoms experienced in the first month after the attack. In line with the first week of the attack, many of those directly (42.3%) and indirectly involved (41.9%) still experienced trouble sleeping. Not surprisingly, this leads to high levels of fatigue for both those directly (57.0%) and indirectly (43.0% involved). A CTO says in one of the interviews: *"You really feel you are overworked. After the incident I collapsed because of the fatigue and stress."* An IT director of another company says: "I had sleep deprivation and the only thing I did, was working." The CIO of another company even states: *"After two weeks we agreed to go home for a few hours to get some rest. I felt completely exhausted."* Sleep deprivation can have severe consequences for functioning in daily life, not in the least because it can lead to concentration problems[5]. Indeed, difficulty with concentrating was common, especially among those indirectly involved in dealing with the attack (31.8%). An interviewee stated he really suffered from concentration problems, which even lasted up until a year after the incident. Also, worrying and negative thoughts were common among all employees, with about 61.9% reporting worrying or negative thoughts in the first month after the attack. For the full overview of symptoms experienced in the first month after the attack, see in document referral.

5. Lim, J. & Dinges, D.F. (2010). A meta-analysis of the impact of short-term sleep deprivation on cognitive variables. .

MIRA PHASE 3

CONTINUED SYMPTOMS

PHASE 3

- Tension between continuing recovery work and back to business as usual
- Tolerance and support from colleagues and home front is depleted
- Feelings of burnout
- People resign

In the long term, after the incident had turned into a project, the impact of the ransomware attack persists. Some of the symptoms that were experienced earlier still play a role after many months or even years. Seven out of eleven interviewees still suffer from sleeping problems months after the attack. *"Eventually I gained 6/7 kilos, stopped exercising, stopped hobbies. The only thing I do is work. Even during moments of relaxation, I do not have the energy to take up hobbies. If I do, I almost feel guilty for work. I Never had the idea that enough is enough,"* said the CIO of a victim company. In other interviews, guilt was also a common theme. An IT director said: *"I still [3 years after the incident occurred] have severe feelings of guilt. It is the worst thing that has ever happened to me. I have a coach who guides me in this."*

SYMPTOMS OF TRAUMA

Earlier research indicated that the psychological consequences of cyberattacks in general can be huge and can be comparable to those of terrorist attacks[6]. This suggests that people who experienced a ransomware attack may also experience symptoms of trauma. Indeed, in another study, IT experts indicated that traumatised employees are one of the main consequences of a ransomware outbreak in terms of the impact on business[7]. To examine whether employees were indeed experiencing symptoms of trauma, we used the Impact of Event scale, a measure that is often used in clinical practice to measure subjective distress. Symptoms of post-traumatic stress disorder are being assessed in this scale[8]. The scale is also used in clinical practice by psychologists, to determine the severity of stress symptoms, and to get an indication of whether psychological help to deal with the event is desired[9].

"1 out of 7 employees still have such high levels of distress that psychological help for trauma is needed."

This questionnaire was also administered to our sample of 352 employees of companies who fell victim to a ransomware attack. Strikingly, 12.3% of those directly involved and 15.5% of those indirectly involved fall into this category. That means that about 1 in 7 employees has such severe symptoms of distress that psychological help for trauma is needed.

For example, both those directly involved (44.2%) and those indirectly involved (41.6%) report that they have trouble falling asleep or staying asleep because of pictures or thoughts about the attack that crossed their minds. Relatedly, 24.8% of those directly involved and 27.7% of those indirectly involved had dreams about the attack. Unwanted thoughts about the attack were common among all employees, even those not involved in the attack. Across the entire sample, 80.9% of employees indicate that they had to think about the attack when they didn't mean to, and 21.1% of employees indicate that this happens often.

We also asked employees to what degree they agreed with several statements since the attack took place. Strikingly, 62.5% of all employees, including those not directly involved in the attack, now believe that the world is a dangerous place.

6. Cheng, J. (2022). The huan consequences of ransomware attacks.
7. Henning, J. (2016). Crypto-Malware. Researchscape International.
8. Horowitz, M., Wilner, N., & Alvarez, W. (1979). Impact of Event Scale: A measure of subjective stress.
9. Sterling, M. (2008). The impact of event scale (IES).

CONSEQUENCES FOR PERSONNEL

Both job stress and high workload predict intentions to resign[10]. Given the high stress and workload associated with ransomware attacks, it is therefore not surprising that 21.0% of those directly involved and 17.9% of those indirectly involved changed jobs or considered changing jobs as a direct result of the attack. It is important to note here that we distributed the questionnaire in the companies that were hit by ransomware attacks, employees who already left the company are therefore likely underrepresented in our sample.

Resignation was also a topic that was mentioned in several five interviews. This concerned mainly thoughts about resigning, getting fired or firing people. Two of the interviewees had serious thoughts about having to quit their jobs.

"The pressure was so high that I was on the verge of resigning."

said an IT director of a company with more than 2500 employees. This was mainly because of the high pressure put on them by management, which caused high stress and sleeping problems. Also, one COO really lost trust in their Chief of IT. They stated: *"I was really angry with the head of IT, and I was planning to fire him. We discovered so many issues during the incident. I felt betrayed by him."*

When asked what they would do differently if they would get hit by ransomware again, two interviewees stated they would resign or get fired: *"I would resign. No, I think I would get fired. I'm serious about that."*

POSITIVE CONSEQUENCES OF A RANSOMWARE ATTACK

A highly stressful experience such as a ransomware attack can clearly have a lasting negative impact on mental health. But in addition to those negative effects, people can also experience positive changes at the same time, for instance because they were able to overcome the stressful period, the deepening of social connection with those who went to the same experience, or changes in realization about what is important in life[11]. This process is known as post-traumatic growth.

Indeed, we also observed such positive effects in people involved in ransomware incidents. For instance, both those directly (66.7%) and indirectly (62.0%) involved indicated that after the ransomware incident, they know better that they could handle difficulties. Many of those directly involved (46.7%) also indicated that they discovered they were stronger than they thought. An interviewee stated: *"Our mental strength has been tested; I now know that I can do this too."* Also, people stated that they had matured in their function: *"I have matured in my role as COO".* Many also experienced positive impact on social relationships. For instance, 61.8% of those indirectly involved indicate that, looking back on the first year after the incident, they learned a great deal about how wonderful people are.

We also assessed how close people felt to their colleagues in the first month after the attack. Those directly involved felt closer to their colleagues in the first month after the attack than those who were indirectly involved or not involved. In fact, 20.0% of those directly involved and 10.7% of those indirectly involved indicate that they feel closer than ever, against only 3% of those not involved. In contrast, 33.5% of those not involved indicate that they feel isolated from colleagues, only 10.5% of those directly involved. The interviewees also acknowledged that,

10. Qureshi, M. I. et al., (2013). Relationship between job stress, workload, environment and employees turnover intentions: What we know, what should we know.
11. Tedeschi, R. G., & Calhoun, L. G. (2004). Posttraumatic growth: conceptual foundations and empirical evidence.

even though they never want to experience it ever again in their lives, the ransomware attack brough them positive effects. An IT manager said, after being asked what consequences the incident had for the organization: *"yes, after the incident we felt way more connected to each other. We did a great job and I'm really proud of how we've handled the incident."* A CEO says: *"it was a good teamwork activity. Crisis always has a positive effect on bonding. It has also been found that IT employees have become more connected and that they have received a lot of compliments from the environment, they are very much appreciated."*

Also, because the incident had occurred awareness was raised both at C level and throughout the whole organisation and measures were implemented more quickly in a short period of time. In addition, the directly involved people also stated a few times that they really gained more respect for the field of cybersecurity. *"I gained more love for the cyber field. It gives a feeling of servitude. I would really like to work for the police."* For an IT director, the cyberattack was the reason to move from IT field to the field of cyber security, *"I have seen how important this field is."*

DIFFERENCES BETWEEN EMPLOYEES

People respond differently to stressful events. We examined several individual characteristics, to examine whether certain groups might need more attention than others.

DO MEN AND WOMEN EXPERIENCE SIMILAR MENTAL IMPACT?

First, we examined whether there were gender differences in the mental impact of ransomware attacks. In our study, women seemed to score higher on most scales, but most of these differences were not significant. However, women did experience significantly more symptoms in the first week of the attack, and experienced significantly higher levels of distress (i.e., more symptoms of trauma) in the year after the attack than men did. Possibly, the impact on women is larger because they also experience more daily stress, chronic problems, and frustrations than men[12]. Women in our sample may for instance have been more likely than men to still have obligations in the home situation, leading to higher daily stress, and thus larger impact.

IS AGE RELATED TO MENTAL IMPACT?

Second, we examined whether age was related to the mental impact of ransomware attacks. We found a significant relationship between age and responses to stress. Although there were no significant differences in the number of experienced symptoms in the first week or first month and age, we found that older employees experienced more distress several months to years after the attack and were more likely to experience such severe symptoms that they would need psychological help. Yet, they also experienced more positive experiences, such as more appreciation for life. This could have several explanations. It is possible that older employees are more vulnerable to the stress of ransomware attacks. However, as older employees on average also had more positive experiences, it is also possible that they are more reactive in general. Another possibility is that older employees, on average, have higher level jobs, which could lead to more responsibilities in dealing with the ransomware attack, and thus higher stress levels during the attack.

DO IT EMPLOYEES EXPERIENCE HIGHER IMPACT THAN OTHERS?

Among the 105 employees who indicated they were directly involved in responding to the attack, 42.9% were involved in IT. We examined whether being involved in IT was related to the mental impact of ransomware attacks. We found no evidence that mental issues were higher among those involved in IT. However, they did have significantly higher scores on post-traumatic growth. For instance, people in IT were more likely to agree with statements such as "I know now that I can deal with difficult circumstances".

12. Matud, M.P. (2004). Gender differences in stress and coping styles.

DO THE SAME PEOPLE EXPERIENCE SYMPTOMS ACROSS TIME?

There were clear and strong relationships between symptoms experienced in the first week and symptoms experienced after one month. Perhaps more importantly, symptoms experienced in the first week and month also predict later symptoms. Those who experienced more symptoms 1 week or 1 month after the attack were also more likely to have higher distress levels months or years later and were more likely to consider changing jobs. This emphasizes the importance of taking measures to reduce stress in the first week and month after the attack, as the effects may linger.

CONCLUSION

The mental impact of ransomware attacks on employees is very high, in all three phases of the MIRA phase model. In all phases, sleeping problems are common. In the first phase, unhealthy coping practices such as eating junk food or skipping exercise are common, and people experience a lot of physical symptoms. In the second phase, many of those physical symptoms persist, people start to feel exhausted. Moreover, feelings of guilt become common, both towards the home and the employer. In the final phase, up to a year after the attack, physical symptoms persist, and the long-term mental impact becomes more apparent. Symptoms of trauma and the need for psychological help is common, and many people start to consider changing their jobs. There are also positive consequences. People can feel more confident in their own abilities, and closeness between those who helped to resolve the attack is likely.

When looking at differences between different types of employees, it is notable that most effects are similar for those directly involved in resolving the attack and those indirectly involved. For those directly involved there are no significant differences between those in IT and others. Symptoms are more likely to occur in women, and some symptoms are more likely to occur in older employees. Those who experience symptoms in the first phase are also more likely to experience symptoms in the second and third phases. Thus, these groups may need more attention.


MITIGATING THE
MENTAL IMPACT
OF RANSOMWARE
ATTACKS

MITIGATING THE MENTAL IMPACT OF RANSOMWARE ATTACKS

In this chapter, we outline what can be done to mitigate the mental impact of ransomware attacks. We provide an overview of what CERT members (study 1), CEO's and IT-managers (study 2) and regular employees (study 3) indicate they would have needed during their experience with ransomware attacks. Next, based on what we learned from our research, we provide concrete advise to managers. Finally, we outline how Northwave can help to mitigate the mental impact of ransomware attacks.

WHAT DO PEOPLE SAY THEY NEED?

We inventoried the needs in ransomware attacks across all groups involved in the study. For CERT members, we asked about needs in different phases of the attack, during the intake phase, the deployment phase, the actual incident and after the incident. In our interviews, we asked questions like: what do you think your organization could have done better? And: in retrospect, what would you have liked to know, get, or hear from Northwave that would have helped you? These questions shine a light on what people or organization might have needed. Finally, we inventoried needs in the 352 employees who took part in the quantitative study. Taken together, there were a few clear themes.

"Planning is one of the most important subjects."

PLANNING AND TASK DIVISION

According to CERT members, during the intake phase, planning is one of the most important subjects, both people's planning (76.1%) and the team planning (81.0%). When asked what would be helpful, one CERT member indicated: *"I would like to have a coordinator to ask what appointments I have during the expected duration of the incident, so I feel like the coordinator finds it important to create time for personal life during the deployment"*, and another one said: *"Most important for me is if management is able to 'manage away' other parts of my planning for the duration of the incident"*. Thus, having attention for conflicting tasks and appointments, both in the private life and at work, can be very helpful to reduce stress. An interviewee of a victim said: *"introducing a rotation schedule was really helpful, because otherwise people will go under completely."* Thus, bringing structure through a planning is an important helping factor in handling ransomware incidents. Also, clarity in role division and incident handling structure is appreciated (85.7%).

REGULAR REST

A vast majority of CERT indicated that being able to relax alone during incidents is important (87.5%). *"Make room for off and on time during incidents. For instance, have some time off for things like sport, relaxing, or walking"*. Similarly, a cool-down period is mentioned as important by almost all CERT members (90.5%). As one CERT member mentioned, *"It is important to have planned time off to recover. You cannot start working normal hours straight after an incident week"*.

In response to the question *"What advice would you give to others if they were faced with a cyber crisis?"*, a CIO answered, *"Take sufficient holiday after such an incident. Employees also indicated that they would have preferred an extra two weeks off instead of a financial bonus."* Therefore, getting extra rest seems to be a more important factor than getting financial rewards.

EVALUATIONS

Across all sources, the need for evaluations both during and after the incident becomes clear. The need for regular evaluations is mentioned by a large majority of CERT members (61.9%). One CERT member indicated: *"I appreciate time or even organized occasions to vent about the state of affairs, to prevent the build-up of tension when you work hard as a team for a couple of days"*. Post-incident evaluation also seems important. Team evaluation after the incident is mentioned as an important topic by 71.4% of CERT members as an important issue. In addition, in our quantitative study all employees, including those not directly involved, indicate that they would have liked to discuss and reflect with colleagues about the attack, ranging from 50% of those not involved and 66.7% of those directly involved. An IT director of a victim states: *"A de-briefing would have been helpful, we never had that."* A manager cyber security of a victim also says: *"getting together intimately to evaluate the incident to check how everyone is doing and what could be done better next time. Simply asking: how are you doing? How are things going at home? What kind of help can we offer you?"*

STRUCTURAL ATTENTION FOR MENTAL HEALTH

When asked what they needed after the attack, a striking 20% of those, directly and indirectly, involved indicated that they would have liked (more) professional help afterwards to deal with the attack. Especially those directly involved also indicate that they would have liked more reflection on the mental impact of the attack (32.4%), which was also mentioned a few times during the interviews. A CTO says, being asked what they would do differently in the future: *"I think we could have lowered pressure for IT in the first two weeks. We could have used a mental coach. Are people still 'yellow' or even 'red'? Not in the first days, but after a week to months afterwards, this could have helped."* Besides this need to evaluate and reflect, it is also clear that there is a need for concrete tools to deal with the impact of the attack (32.0%), such as having some time off after the incident.

In addition, it seems to be the case that feelings of guilt play a great role in the aftermath of an incident. This was also expressed in reluctance to ask for help. Several managers pointed out that they had lost a lot of crucial time, because they postponed asking for help because they felt ashamed. Luckily, there is willingness of those directly and indirectly involved to help others, around 43% indicate that they would have liked to know how they can help others around them to cope with the attack. Concrete tools to create a safe, guilt-free culture need to be designed. Direct colleagues can play an important role in this. Working towards an open, guilt-free culture, can potentially decrease the mental impact greatly. A CIO stated during the interview: *"Emotional impact should be addressed during the incident. A place should be provided for people to go and talk somewhere. Especially in toxic cultures, the mental impact can be even greater. Simply naming it is crucial. After all, you're also talking about recovery, negotiation. Mental impact should be an issue too."*

HEATHY COPING

During ransomware incidents, important topics were mentioned in the interviews that relate to negative coping mechanisms that negatively impact physical health, such as eating unhealthily, smoking, or not exercising. Easy, fast and comfort food is easily served. An Enterprise Architect said: *"I gained 10 kilos, because we ordered Chinese food every day."* Serving healthy food may not feel satisfactory in the moment, but will help people recover in the long run, as it is a healthy form of coping with stress. An interviewee said, *"You get tired from the long days, difficulty concentrating and paying attention. I started smoking again."* Structural attention for physical health is important to reduce long-term effects of unhealthy behaviour. For example, make someone responsible for safeguarding healthy behaviour during the incident.

"Support from C-level in creating a safe culture for those who handle the incident is crucial."

SAFE CULTURE

Trust towards the crisis response team accelerates the speed with which the crisis can be resolved and decreases pressure on incident responders. An IT director said: *"The more time it took, the more desperate and stressed the management became. And the higher the pressure on us became. The pressure from management caused me to sleep badly and have a lot of stress. There was a manager who put a lot of pressure on me and asked me, "Why are you so indifferent? You just walk around all peaceful like nothing is wrong!" I asked him if he'd rather have me running around like a headless chicken. My people don't get support from that. And what I show on the outside says nothing about what I feel inside. The pressure was so high that I was on the verge of resigning."*
A negative culture seems to play an important role in the amount of stress people experience and way people look back at the incident. This was also shown in the interviews, where a CTO said: *"We got a lot of support and never felt like we were being 'blamed'. I was so impressed with the board, everyone was involved. Everyone took responsibility. Even the CEO came every day to ask how things were going and if there was anywhere to help. I was really impressed by the team spirit."* Thus, C-levels play a crucial role in safeguarding a safe and supportive culture.

ADVISE FOR MANAGERS

In line with our MIRA phase model, we argue that different actions are required in different phases of dealing with ransomware attacks.

BEFORE THE ATTACK

The mental impact of ransomware attack should be addressed even before such an attack occurs. Based on their report on the impact of ransomware attacks on IT professionals, IBM main advice is to have a detailed response plan ready and to practice incident response[2]. In addition to this, we argue that such a response plan should include a section on mental health. Such a plan should include concrete answers to questions such as:

- How will we ensure sufficient rest?
- How do we create redundancy?
- How do we support people in their private lives?
- How will we monitor mental health impact?
- Where can employees who need help to deal with mental health issues go?
- Who is responsible for and who will be involved in mental health support?

DURING PHASE 1 – THE FIRST WEEK OF THE RANSOMWARE ATTACK

In the first phase of the ransomware attack, when systems are down and people are working around the clock to mitigate the consequences of the attack, high stress levels are. Yet, there are still measures companies can take to minimise the negative effects of ransomware attacks.

1. **Make sure there is sufficient rest.** Based on research in our own CERT, we now aim to limit the working hours during ransomware incident to 12 hours. However, sometimes a peak over those 12 hours is unavoidable. In that case, ensuring a minimum of 8 hours of sleep is essential for everybody involved. In addition, we regularly change the composition of the team during the attack, so that our team members can pay attention to their private life and so they can rest.

2. IBM (2022). Security Incident Responder Study.

2. **Have regular check-ins.** During check-ins, tasks can clearly be divided, which reduces stress. Additionally, regular check-ins also allow regular attention for mental health in a structured way. In our own CERT, we have a daily check-in with the response coordinator, where we do not only monitor work progress and set clear goals and tasks, but also pay attention to how someone is feeling. Such meetings can allow employees to speak up if the impact is too high, so that timely interventions can take place.
3. **Monitor coping.** Unhealthy coping, such as smoking, drinking, eating junk food and ignoring social relationships, is common during the first phase. Creating an environment in which it is easier to make healthy decisions, for instance by not only providing snacks but also fruit, or by having meetings while taking a walk outside, can have a positive effect.

DURING PHASE 2 – THE FIRST MONTH AFTER A RANSOMWARE ATTACK

In the second phase of the ransomware attack, the company is starting to recover, but the consequences of the attack are still felt, especially for those involved in the crisis response team. In this phase, the following actions can be taken to minimise the negative consequences for mental health:

1. **Manage the workload of the incident team wisely.** Fatigue, sleep deprivation and persistent high stress levels are very common during this phase. The return of regular tasks means that the workload of IT and others involved in mitigating the consequences of the attack is still very high. This can be addressed by distinguishing between incident work and regular tasks. Whenever possible, find extra people for regular tasks. Create a rhythm with rest and recovery time for everyone.
2. **Create a safe working environment.** Guilt is one of the most expressed emotions in all elements of the study. Sometimes this guilt is amplified by management or by other employees. This is very counterproductive. Focus on the process of getting the business back on track, rather than finding someone to blame.
3. **Set realistic expectations.** As the business is getting back on its feet, we see a decline in understanding for the IT team and others involved in mitigating the consequences of the attack. Creating an understanding for those still involved in dealing with the consequences of the attack among other employees can help lower the stress they are experiencing.

DURING PHASE 3 – THE FIRST YEAR AFTER THE RANSOMWARE ATTACK

Although the company is back to normal in this phase, people are still feeling the consequences. In this phase, the following actions can be taken:

1. **Monitor mental health.** The results of this report make it clear that the long-term mental health impact of ransomware incidents is severe and that serious problems requiring professional help are common. Setting up a system to monitor mental health symptoms is therefore essential.
2. **Plan evaluation sessions.** People involved in ransomware attacks express a clear desire to have evaluation sessions to talk about the attack and its mental consequences. As closeness amongst colleagues increases, creating an open environment where such feelings can be discussed regularly can thus be powerful.
3. **Offer tools to deal with the mental impact.** People express a clear desire for help to deal with the mental impact of ransomware attacks, and for tools to deal with the mental impact for themselves and for colleagues.

MENTAL HEALTH SUPPORT FOR RANSOMWARE ATTACKS AT NORTHWAVE

The outcomes of the research described in this report show that ransomware attacks have a significant long-term mental impact on organizations.

"Measures to mitigate or prevent mental consequences in organisations are not a luxury but a necessity."

Unfortunately, attention for the mental impact ransomware attacks is still underdeveloped. We see it as our social responsibility to make organizations more resilient. We want to help organizations to be able to prevent negative consequences where possible and mitigate the consequences if they do occur. To achieve this, we have developed an incident support support service based on our results. This ransomware incident support service will be tailored to the needs of individual organizations.

During the first phase of the MIRA phase model, this service can include consultancy for incident communication. With this consultancy, the behavioural dynamics surrounding the incident can be addressed. Various groups, including managers, the crisis response team and the homebase of those directly involved in resolving the attack can be informed about what to expect in the upcoming weeks and months. In addition, on-site emotional support can be provided, including signalling, monitoring, and encouraging healthy coping.

In the second phase of the MIRA phase model, up to one month after the incident, services can include continued communication consultancy, for instance by helping board, IT and employees manage expectations. In addition, we can organize a mental health scan to assess current symptoms among employees. Finally, the emotional support in this phase can take the form of a debriefing and evaluation session with all of those directly and indirectly involved.

In the third phase of the MIRA phase model, 6 months to a year after the incident, we can offer a check-up for emotional support. This can include evaluation sessions with those directly and indirectly involved, a continued mental health scan, and a set of micro-interventions designed to mitigate the negative consequences of the ransomware attack.

For more information, please contact us at mentalimpact@northwave.nl.

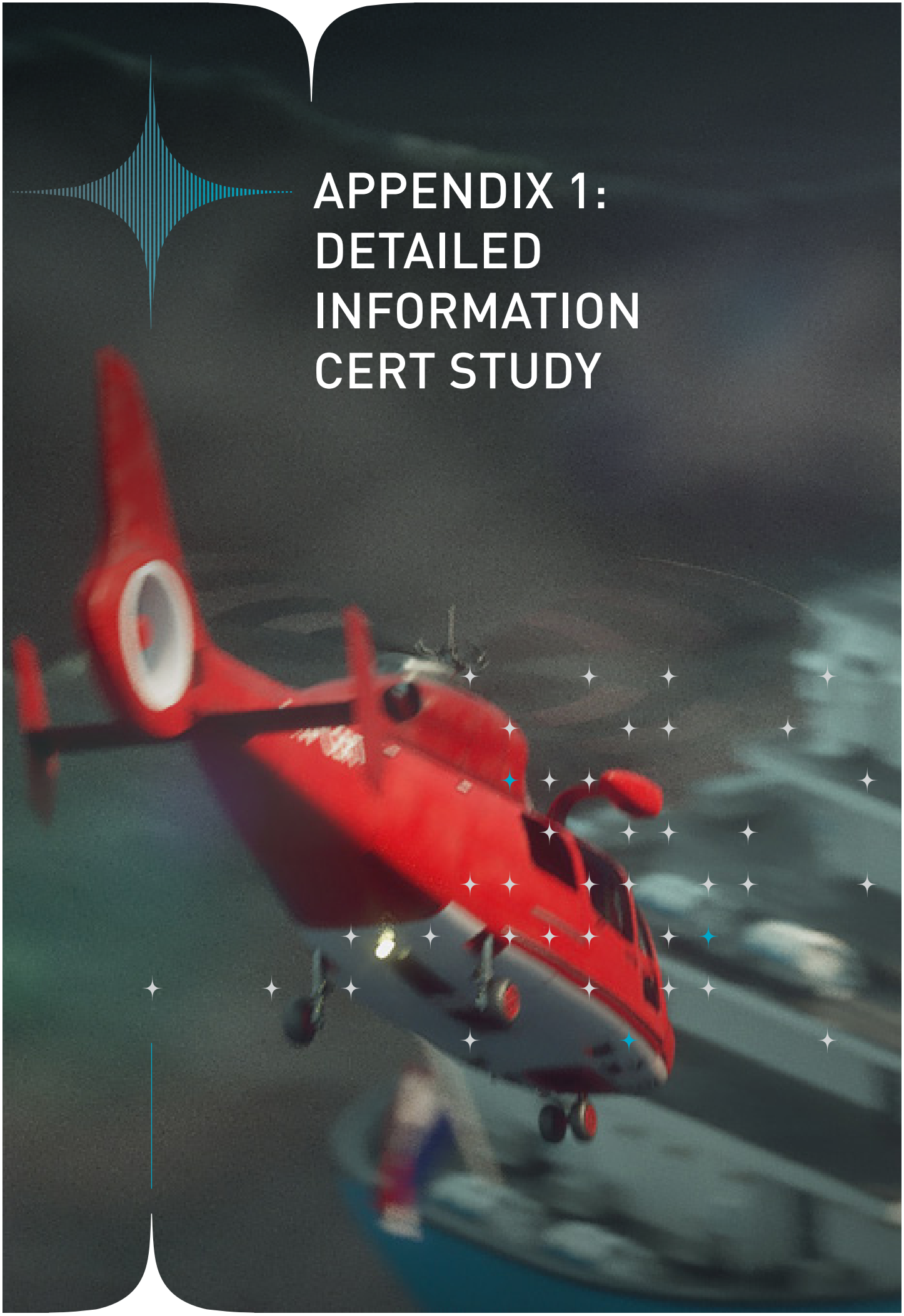
CONCLUSION

CONCLUSION

We set up this research to examine what the mental impact of ransomware attacks is. Although, based on our experience, we expected there to be an effect of ransomware attacks, the results of this research show that the effects are even bigger than we expected.

People who experience ransomware attacks go from high stress, physical symptoms, and unhealthy coping in the first week after an attack, to exhaustion and guilt in the first month after an attack, to severe impact on how they view the world and symptoms of trauma in the year after the attack. These effects are not only limited to those directly involved in resolving the ransomware attack, such as CERT members and IT staff, but also in those indirectly involved, such as people taking over tasks from others in companies. People who are involved in resolving the attack also express a clear need for more tools and guidance in dealing with the mental consequences of ransomware attacks.

Resolving a ransomware attack is not just a matter of resolving the first crisis and getting systems up and running again. After the crisis comes the blow – the blow to mental health. It is thus evident that we need to pay more attention for the mental impact of ransomware attacks. Security companies that help companies resolve ransomware attacks should look beyond their technical duties and offer help in dealing with this blow to mental health. Companies that want to prepare for future security incidents should not only prepare for technical and business measures, but also for the impact an attack can have on the mental health of employees. By paying structural attention to the impact such attacks can have on mental health, we can work together to soften the blow to mental health.



APPENDIX 1: DETAILED INFORMATION CERT STUDY

APPENDIX 1: DETAILED INFORMATION CERT STUDY

PROCEDURE

The study was set up to learn more about the experiences of our own CERT, to learn from the results, share experiences and adjust practices where possible. To achieve this, we created a survey, which was distributed to all the members of the NW CERT (27 at the time) through email. Both members of the regular CERT and members of the virtual CERT who had been on incident at least once were invited to participate. In the e-mail, we indicated the importance of gaining insight into the experiences, needs and mental impact of incidents on the CERT. Participation In the survey was voluntary and answers were anonymously processed.

PARTICIPANTS

The table below describes the sample. A total of 21 CERT team members participated in the survey, 20 of whom were male and 1 female. Most team members were between 25 and 34 years old. The group was divided in terms of experience, ranging from 1-5 incidents to more than 15 incidents. Various roles within the CERT team were also represented.

Question	%	N
Gender		
Female	4.8%	1
Male	95.2%	20
Age		
18-24	4.8%	1
25-34		14
35-44	19.0%	4
45-54	9.5%	2
Number of ransomware incidents		
1-5	33.3%	7
6-10	28.6%	6
10-15	14.3%	3
>15	23.8%	5
Role at incidents		
Crisis manager	14.3%	3
Forensic Investigator	33.3%	7
Incident response coordinator	19.0%	4
Recovery expert	33.3%	7

MEASUREMENTS

Stress tolerance. Stress tolerance was measured with 5 items measuring how people usually deal with stress on a 5-point Likert scale ranging from 1 = "Strongly disagree" to 5 = "Strongly agree". The scale included items such as "I prefer to work under pressure", of which item was reverse coded. We computed a scale score by taking the average across items. The reliability of this scale was moderate with α = .62.

Comfort level. We asked about the level of comfort CERT members have with several elements of being part of a ransomware attack incident response, such as "I feel comfortable in the roles I have during incidents" and "I feel comfortable with leaving early in the evening while my colleagues continue to work". Participants indicated to what extent they agreed with each statement on a 5-point Likert scale ranging from 1 = "Strongly disagree" to 5 = "Strongly agree". Each item was analysed separately, no scale scores were computed. For reported percentages, we counted the percentage of incident responders who responded with "Agree" or "Strongly Agree" for each statement.

Importance. For each phase of a ransomware incident (intake, deployment, during the incident and after the incident), we asked several questions about what CERT team members find important. For each phase, we asked "How important are the following aspects for you during the [intake] phase". These questions were based on conversations with CERT team members. The scale included items such as "your planning" in the intake phase, "being able to go home before deployment" during the deployment phase, "Quality of the food" during the incident phase, and "team evaluation" in the phase after an incident. Participants indicated for each item how important this was to them, on a 5-point Likert scale ranging from 0 = "not important" to 5 = "very important". Each item was analysed separately, no scale score was computed. We computed the percentage of participants who indicated that an item is "important" or "very important" to them. For each phase, we also included an open question where participants could indicate what else they found important during this phase (e.g., "Are there any other aspects important to you [after the incident]?").

Feelings. For each phase of a ransomware incident (intake, deployment, during the incident and after the incident), we asked about feelings, by asking "When I [do the intake with the costumer] I am feeling...". Participants indicated on a 5-point Likert scale ranging from 1 = "Strongly disagree" to 5 = "Strongly agree" to what extent the felt things such as "excitement" or "insecurity". Each item was analysed separately, no scale scores were computed. We counted the percentage of participants who indicated that they "agree" or "strongly agree" with each item.

Physical symptoms. We asked which symptoms occur during incidents using 10 items on a 5-point Likert scale ranging from 0 = "never" to 5 = "always". We asked the question "During incidents I..." followed by 10 items, including "Lose my appetite". We counted the percentage of participants who indicates that this occurs (i.e., excluding those who say it never occurs), and the percentage of participants who indicate it happens "often" or "always". We analysed each item separately and did not compute a scale-score.

Stress. For each phase of a ransomware incident (intake, deployment, during the incident and after the incident), we asked how people would rate their stress level on a scale of 1 = lowest to 10 = highest. For each phase, we calculated the average score across participants, and the percentage of participants who scored 5 or higher on that scale.

Impact. We asked participants to indicate what the impact of incidents on their private life was using 4 questions, asking about both on-site and remote incidents, and incidents with a duration of 3 and 10 days (e.g.: "I would rate the impact of an on-site incident of 10 days on my private life as..."). Participants responded to these items on a 10-point scale ranging from 1 = "lowest" to 10 = "highest". For each item, we calculated the average score across participants, and the percentage of participants who scored 5 or higher on that scale. We also asked an open question, "Which measures can Northwave take to minimize the impact on your private life in case of an on-site incident?".

DATA-ANALYSES

Given the limited sample size, we focused mainly on descriptive statistics in this study. To explore whether the experience of stress was related to either experience or stress tolerance, we used Spearman correlations combined with a visual inspection of scatterplots.

RESULTS

RATINGS OF STRESS LEVEL DURING DIFFERENT PHASES OF AN INCIDENT

	Average	% above 5
During the intake phase, I would rate my stress level	3.5	38.1%
During the deployment phase, I would rate my stress level	4.8	61.9%
During the incident phase, I would rate my stress level	5.3	52.4%
After an incident, I would rate my stress level	3.0	9.5%

PERCENTAGE OF CERT TEAM MEMBERS INDICATING SYMPTOMS OCCUR

	Occurs	Occurs often
Lose my appetite	52.4%	14.3%
Drink (non-alcohol) less than I normally do	61.9%	14.3%
Drink more alcohol than I normally do	71.4%	28.6%
Smoke more than I normally do	9.5%	4.8%
Have trouble falling asleep	81.0%	19.0%
Have trouble with sleeping trough	71.4%	28.6%
Have muscle pain	57.1%	9.5%
Have a headache	81.0%	4.8%
Have breathlessness	23.8%	4.8%
Have palpitations	19.0%	4.8%

FEELINGS OF CERT-EMPLOYEES DURING DIFFERENT PHASES OF A RANSOMWARE ATTACK

I am feeling...	During intake %	During the deployment %	During the incident %	After the incident %
Excitement	61.9%	90.5	90.5%	14.3%
Anxiety or nervousness	33.3%	28.6%	14.3%	4.8%
Guilt related to work	9.6%	28.5%	23.8%	23.8%
Guilt related to private life	28.6%	57.2%	47.6%	42.8%
Loneliness	0.0%	0.0%	4.8%	14.3%
Compassion with the customer	52.4%	52.4%	76.2%	33.3%
Surprised (shock and amazement)	4.8%	4.8%	9.5%	0.0%
Disgust or aversion	0.0%	0.0%	0.0%	4.8%
Insecurity	9.5%	4.8%	9.5%	4.8%
Irritability related to the team	4.8%	4.8%	9.5%	4.8%
Irritability related to the customer	0.0%	4.8%	4.8%	9.5%

STATEMENTS ABOUT FEELING COMFORTABLE

	Disagree %
I feel comfortable in handing over my role to another colleague during an incident	9.5%
I feel comfortable with starting later in the morning while my colleagues already start early	61.9%
I feel comfortable with leaving early in the evening while my colleagues continue to work	57.1%
I feel comfortable with leaving the incident response team before the incident is finished	33.3%

RATINGS OF IMPACT ON PRIVATE LIFE IN DIFFERENT CIRCUMSTANCES

	Average	% above 5
I would rate the impact of an on-site incident of 3 days on my private life	4.2	38.1%
I would rate the impact of an on-site incident of 10 days on my private life	7.3	81.0%
I would rate the impact of an remote incident of 3 days on my private life	3.3	19.0%
I would rate the impact of an remote incident of 10 days on my private life	5.3	71.4%

ASPECTS THAT CERT MEMBERS FIND IMPORTANT DURING INTAKE PHASE

	Important or very important
Team planning	81.0%
Your planning	76.1%
Performing the intake with a colleague	71.4%
Knowledge of the incident topic	71.4%
Time to prepare an intake	23.8%

ASPECTS THAT CERT MEMBERS FIND IMPORTANT DURING DEPLOYMENT PHASE

	Important or very important
The type of deployment (remote or on-site)	71.4%
Time to discuss the possible deployment with family/friends	66.7%
The expected duration of the incident	66.7%
Being able to go home before deployment	57.1%
The incident response team members	57.1%
Have my own car available at the location if on-site	52.4%
Time to think about whether you are joining the incident response team	52.3%
Whether I am on stand-by duty	47.6%
Whether I am available for all phases of the incident	47.6%
The location of the incident if on-site	33.3%

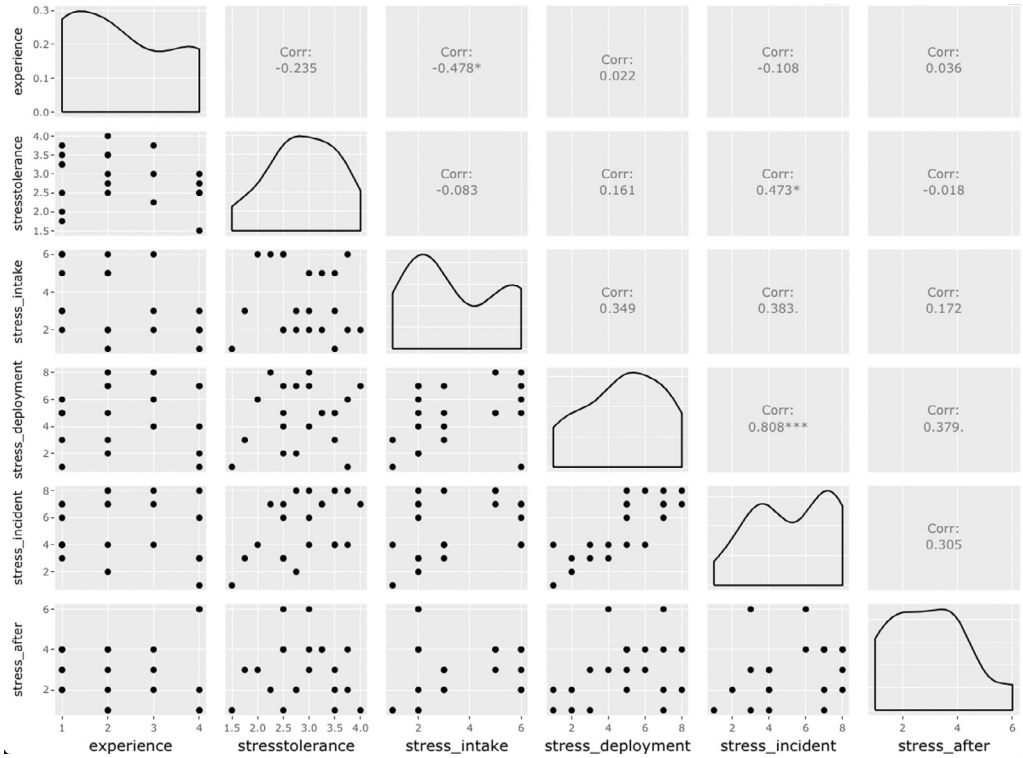
ASPECTS THAT CERT MEMBERS FIND IMPORTANT DURING AN INCIDENT

	Important or very important
Quality of the food	85.7%
Quality of the hotel	85.7%
Relax moment in the evening (alone)	85.7%
Clear role division	85.7%
Clear incident handling structure	85.7%
Enough sleep	66.7%
Eating together	66.6%
Time alone	61.9%
Regular team evaluations	61.9%
Eating together outside the office	61.9%
Relax moment with the team in the evening	61.9%
Time and equipment to sport	23.8%
Possibility to work in shifts	19.0%

ASPECTS THAT CERT MEMBERS FIND IMPORTANT AFTER THE INCIDENT

	Important or very important
Cool down period	90.5%
Time to apply lessons learned	71.5%
Team evaluation	71.4%
Incident evaluation	57.2%
Contact with the customer	28.6%

RELATIONSHIPS BETWEEN LEVEL OF EXPERIENCE, STRESS TOLERANCE, AND STRESS AT VARIOUS PHASES DURING AN INCIDENT



APPENDIX 2: DETAILED INFORMATION INTERVIEW STUDY 2

APPENDIX 2: DETAILED INFORMATION INTERVIEW STUDY 2

BACKGROUND

To get insight into changes in emotions, thoughts, and behaviour after a ransomware incident in the management of affected companies, we conducted a series of interviews. Two main questions that we aimed to answer with those interviews were:

- What is the perceived mental and physical impact of the ransomware impact on people's own life?
- What is the mental and physical impact of the ransomware incident on employees in the company that were directly involved in resolving the threat=?

PARTICIPANTS

In total, people of 11 different companies took part in the interviews. All were directly involved in, or responsible for, dealing with the ransomware attack. Although not always explicitly mentioned in the interviews, the job titles included for example an IT-manager, a Chief Operational Officer (COO) or a Chief Information Officer (CIO).

PROCEDURE

Nineteen companies were contacted with a request to take part in the interview. With 11 of these companies, interviews have been conducted for this whitepaper. With 2 companies 2 interviews have taken place, which resulted in 13 completed interviews. We analysed the results at the level of the company, so we grouped the results together for those companies where multiple interviews took place. Reasons for not participating were mostly lack of time/interest, but one company rejected in a very noteworthy way, by stating: *"The ransomware has indeed had quite a mental impact on the organization and employees. We have now lost quite a few employees (probably because of this). We would rather not bring it up again. Both for ourselves and for the employees, this is not wise."*

The interviews were conducted by seven Northwave employees of different departments, such as the behaviour department or technical departments (CERT). Of the finished interviews, nine interviews were conducted by two interviewers simultaneously, four interviews were conducted by a single interviewer. Five interviews were done physically, and eight interviews were conducted using Teams. The interviews were semi-structured, where the interviewer used a structured topic list with structured follow-up questions but leaving room for the respondent's input. The interviews have been recorded and were worked out after the session in question was completed. The data were processed anonymously. One interviewee did not agree with recording the interview, this interview was processed by a second interviewer during the interview itself. All interviews started by explaining the purpose of the interviews and by creating a safe environment, so that the interviewees could speak freely.

MEASUREMENTS

The interviews were categorized in three different themes: 1) Personal experience 2) Experience of employees within the organization 3) Northwave's role. Within each theme, questions were asked about the different phases. Since the interviews were semi-structured of nature, not all questions were asked in all interviews and in some interviews, additional questions have been asked when deemed necessary.

Sample questions phase 1

- Where did the ransomware incident start for you? And then...?
- What was your initial reaction?
- To what extent did you feel the incident was your fault?

Sample questions phase 2

1. At the time of the incident, to what extent were you suffering from physical complaints?
2. To what extent were you experiencing emotional or psychological symptoms at the time of the incident?

Sample questions phase 3

1. To what extent were you still experiencing physical symptoms after the ransomware attack?
2. To what extent were you still suffering from emotional or psychological symptoms after the ransomware attack?
3. What is it like to talk about the incident again now?

INTERVIEW DATA ANALYSES

To bring order to the interview data, Northwave went through three steps: open coding, axial coding, and selective coding. The interviews were read through according to the four-eye principle and key pieces of text were highlighted. The shaded excerpts were then coded. Coding snippets of text is also known as open coding[13]. Afterwards, all codes from each interview were put into a table. The codes were then divided among the topics included in the interview questionnaire. In this table, the researchers looked for similarities and differences between codes, where possible, codes were combined into one association and ranked. This is called axial coding[13].

OVERVIEW OF CODED DATA

The tables below give an overview of in how many interviews a certain topic was mentioned, including an illustrative quote.

PHASE 1 – WEEK

Topic	Times mentioned	Quote
Smoking	1	*I started smoking again*
Neglect of private life (no time for family, friends, sports, hobbies)	5	*I had no family life. I brought my sick son to work otherwise I didn't see him.*
Aggressive thoughts	1	*I almost kicked out a glass door*
Sleep deprivation	7	*The first days I didn't sleep at all.*
Stress	11	*Then the panic broke out. It felt like the floor was sinking beneath you.*
Crying	2	*I cried really hard*
Problem solving	2	*I drove to my girlfriend to empty my head*
Cardiovascular complaints	3	*I had an extremely high blood pressure.*
Thoughts about/fear for resignation	2	*I it happens I again, I will resign, or get fired.*
Guilt	3	*Blame played a great role in the IT team*

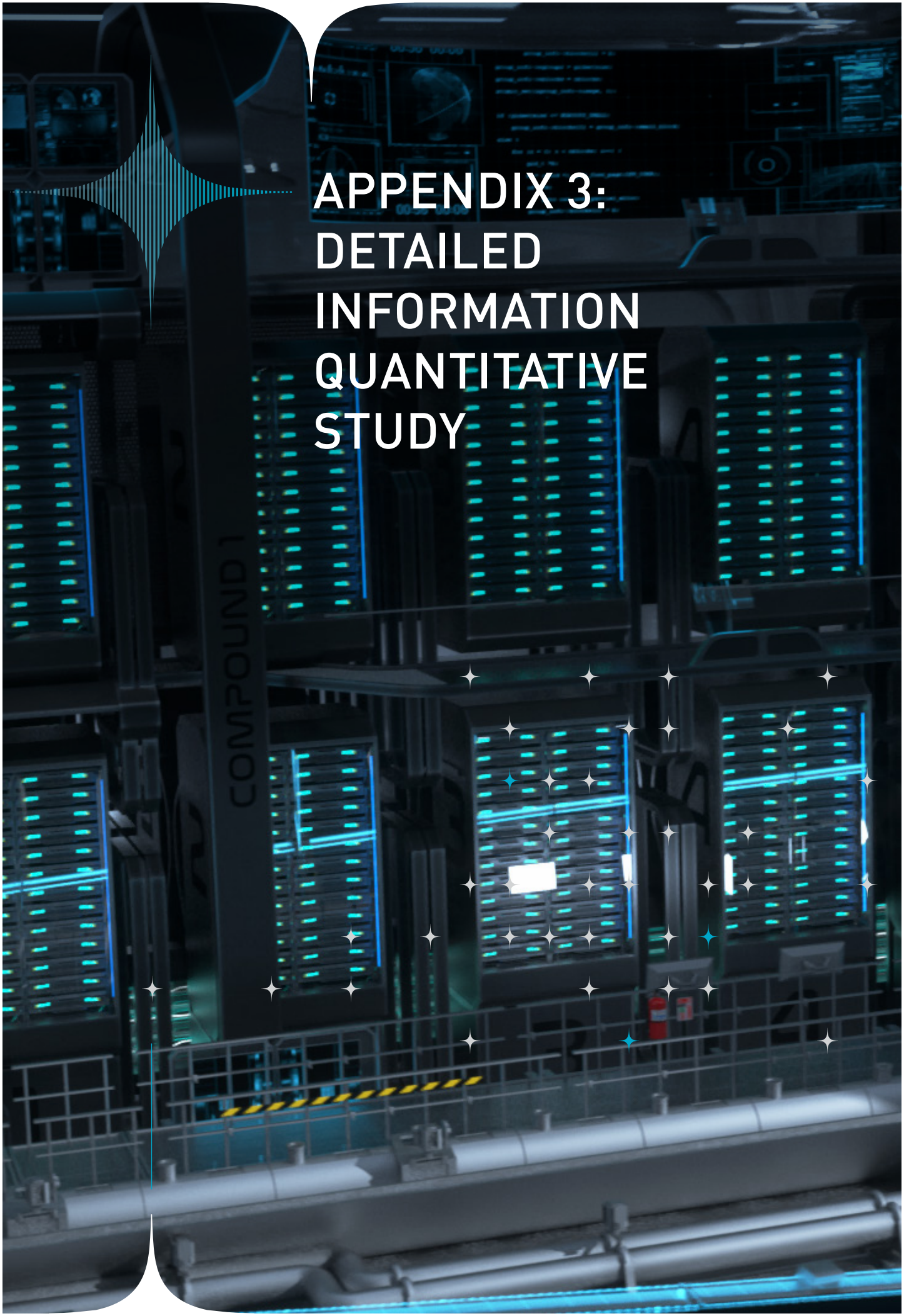
13. Verhoeven, P. S. (2014). Wat is onderzoek? Praktijkboek methoden en technieken voor het hoger onderwijs.

PHASE 2 – MONTH

Topic	Times mentioned	Quote
Gaining weight	2	*Gained 7 kilos in the longer term*
Extremely tired	6	*We made 12-14 hours a day, for weeks.*
Employee dropout	5	*Some people in the IT team broke down because they could not handle the pressure.*
Neglect of private life (no time for family, friends, sports, hobbies)	5	*I stopped exercising, stopped hobbies.*
Sleeping problems	4	*I sleep poorly and have a short fuse.*
Support from home	2	*Being able to tell your story to your loved ones. That also helped me.*
Guilt	2	*Yes, I feel guilty, I really had no awareness on th is subject at all.*

PHASE 3 – YEAR

Topic	Times mentioned	Quote
Emotional topic	4	I feel tears coming up when talking about it [8 years ago]
Seeking psychological help	1	This is the worst thing that has ever happened to me. I have a coach to guide me through this.
Sleeping problems	4	After 6 months I still have trouble sleeping
Higher workload	2	10% of the time I'm still busy working on the incident
Prolonged exhaustion	2	I am more upset about the smaller things
Frustrated	2	I was angry with myself because I had not put enough weight on Cyber Security
Concentration problems	2	I'm constantly distracted.
IT team mentally exhausted	5	The exhaustion was still existing after six months for the IT team.
Better teamwork	6	IT employees have become more connected, and they have received a lot of compliments, they are very much appreciated.
High cyber awareness	2	people are asking much more questions and are much more aware of cyber security, so that is very positive.
Faster implementation of security measures	3	Security recommendations are implemented quickly.
Valuation IT team	5	
Looking back on the IT people, I'm very proud of them, they all tried their best and gave everything.		
Thoughts about/fear for resignation	1	After six months I was planning to fire the head of IT, I was really angry with him.
Guilt		I still feel guilty, it has had a huge impact on my life [3 years ago]



APPENDIX 3: DETAILED INFORMATION QUANTITATIVE STUDY

APPENDIX 3: DETAILED INFORMATION QUANTITATIVE STUDY

BACKGROUND

To confirm findings in our own CERT and observations in the qualitative study, we conducted a quantitative study in the form of a survey which consisted of different scientifically approved scales (see measurements section). The survey was completed by employees of companies that were the victim of a ransomware attack. The questionnaire contained questions about the physical and mental complaints in the different phases of the MIRA phase model (see measurements for details).

PARTICIPANTS

In total, 356 participants had completed the questionnaire on October 26th, 2022, when the data were downloaded for analyses. Alchemer offers a procedure to scan data for unreliable responses, by identifying people who answered questions very quickly (n = 26) and people who seemed to answer questions in a pattern (e.g., by answering every question with 1, n = 3). We inspected data for all participants who were flagged, and deleted responses for 2 participants, who answered all questions with the same response, including questions that were negatively worded. The answers of the participants who were identified as speeders did not seem to differ from other participants, so we included those in the sample.

Furthermore, we deleted data of 2 participants who answered very few questions (76% - 95% missing values). Thus, the final sample of the study included 352 participants. Participants included more men (78.8%) than women (21.2%). All participants were between the ages of 17 and 65 (M = 43.9, SD = 12.2).

There were various levels of involvement in the attack, as displayed in the table below.

TO WHAT EXTENT WERE YOU INVOLVED IN (RESPONDING) TO THE ATTACK?

	N	Percent
Directly involved	105	38.1%
Indirectly involved	113	32.1%
Not involved	134	29.8%

For those who indicated they were directly involved in dealing with the ransomware attack, we asked more specifically what role they fulfilled. Most people had a single role (e.g., being in the IT team), but 38.1% had multiple roles (e.g., both IT and contact with costumers). Table X displays the various roles people had during the incident. As only the group of employees that were involved in IT was big enough to do analyse

WHICH DESCRIPTION BEST FITS THE ROLE YOU HAD AT THE TIME OF THE ATTACK?

Role	Percentage
Board or management team	20.0%
IT	42.9%
Crisis communication	11.4%
Legal	1.0%
Mapping business processes	9.5%
Contact with costumers	21.0%
Contact with own employees	34.3%
Different role	11.4%

PROCEDURE

The same 19 companies that were contacted with a request to take part in the interview were also requested to take part in the survey. At the time of analysis, 6 companies agreed to participate and distributed the questionnaire among their employees. There are still some prospective companies to which the questionnaire will be distributed later. The number of participants per company varied between 1 and 248, with an average of 58.7 participants per company.

MEASUREMENTS

SOMATIC SYMPTOMS SCALE

The Somatic Symptom Scale[14] (SSS-8) was used to measure the severity of symptoms during the first week after the attack. The scale consists of 8 items. The participants indicated the extent to which they experienced somatic symptoms on a 5-point Likert scale ranging from 0 = "not at all" to 4 = "very much". An example item is "In the first week after the attack, to what extent did you suffer from back pain?". The reliability of the scale is high with α = .84. We used the scale in 3 ways. First, we analysed each item separately, by counting the percentage of participants who indicated that they experience somatic symptoms (ranging from "a little" to "very much"). Second, we computed a scale-score by summing up all scores. This scale-score was used in group comparisons. Finally, we divided those scores in common cut-off scores, reflecting minimal (0 to 3), low (4 to 7), medium (8 to 11), high (12 to 15) and very high (15 and above)[14].

SYMPTOMS FIRST MONTH AFTER THE ATTACK

A self-constructed scale was used to measure the occurrence of symptoms during the first month after the attack (MIRA phase 2). The scale consists of 9 items. Participants indicated whether they experienced these symptoms during the first month after the attack by answering with "yes", "no" or "do not know / do not recall". An example item is "In the first month of the attack, did you suffer from headaches?". The scale showed signs of high reliability, with Cronbach's alpha was high α = .77. We also computed a scale score, by summing the total number of complaints participants reported. We also analysed each question separately, by computing the percentage of participants who answered "yes" to experiencing a symptom in the first month after the attack.

IMPACT OF EVENT SCALE

The Dutch version of the Impact of Event Scale[9], the Schokverwerkingslijst (SVL)[15], was used to assess signs of distress, in the form of the occurrence of post-traumatic stress symptoms, namely the frequency of intrusive and avoidant phenomena after the attack (phase 3). The scale consists of 15 items. The participants indicated how often the statements applied to them since the attack on a 4-point scale, with 0 = "not at all" 1 = "rarely", 2 = "often" and 5 = "often". An example item is "I dreamt about the attack". The scale had good reliability, with α = .90. We counted the percentage of participants who indicated that the item applied to them from "occasionally" to "often" and labelled this "occurs". We also counted the percentage of participants who indicated that the item applied to them "often" and labelled this "occurs often". To compute a scale score, we summed the scores across all items. We used common cut-off scoresref[16], resulting in the categories subclinical (0 to 8 points), mild (9 to 25), clinical – moderate (26 to 43) and clinical – severe (43 or more points).

9. Sterling, M. (2008). The impact of event scale (IES).
14. Gierk, B. et al. (2014). The somatic syptom scale-8 (SSS-8): A brief measure of somatic symptom burden.
15. Brom, D., & Kleber, R. J. (1985). De Schok Verwerkings Lijst.

POSTTRAUMATIC GROWTH INVENTORY

The short form of the posttraumatic growth inventory[16] (PGI-SF) was used to assess the degree to which the participants experienced growth because of the attack (MIRA phase 3). The scale consists of 10 items. Participants indicated to what degree they experienced growth on a 6-point scale ranging from 0 = "I did not experience this change as a result of the attack" to 5 = "I experienced this change to a very great degree as a result of the attack". An example item is "I discovered that I am stronger than I thought I was". The scale showed good reliability with α = .88. We counted the percentage of participants that indicated that they experienced each occurrence, ranging from "I experienced this change a little bit as a result of the attack" to "I experienced this change to a very great degree as a result of the attack" and labelled this "occurs". We also counted the percentage of participants that indicated that they experienced each item "to a great degree" or "to a very great degree" and labelled this as "occurs strongly". Finally, we computed a scale-score by computing the average across all items.

POSTTRAUMATIC MALADAPTIVE BELIEFS

The posttraumatic maladaptive beliefs scale[17] (PMBS) was used to measure maladaptive beliefs about current life circumstances that may occur following the attack (MIRA phase 3). The scale consists of 15 items. The participants indicated their level of agreement with statements on a 7-point scale ranging from 1 = "strongly disagree" to 7 = "strongly agree". An example item is "I don't feel safe anywhere anymore". The scale showed good reliability, with α = .77. Each item was analysed separately, no scale scores were computed. For the positively worded items we counted the percentage of participants who indicated "somewhat agree" to "strongly agree". For the negatively worded items we counted the percentage of participants that indicated "strongly disagree" to "somewhat disagree".
We computed a scale score by taking the average across all items.

CLOSENESS TO COLLEAGUES

A single self-constructed item was used to measure the closeness of colleagues. The item is "how would you describe the closeness of your colleagues in the first month after the attack?" Participants indicated to what extent they felt closer to their colleagues in the first month after the attack (phase 2) on a 6-point scale ranging from "I felt strongly isolated from my colleagues" to "I felt closer than ever to my colleagues".

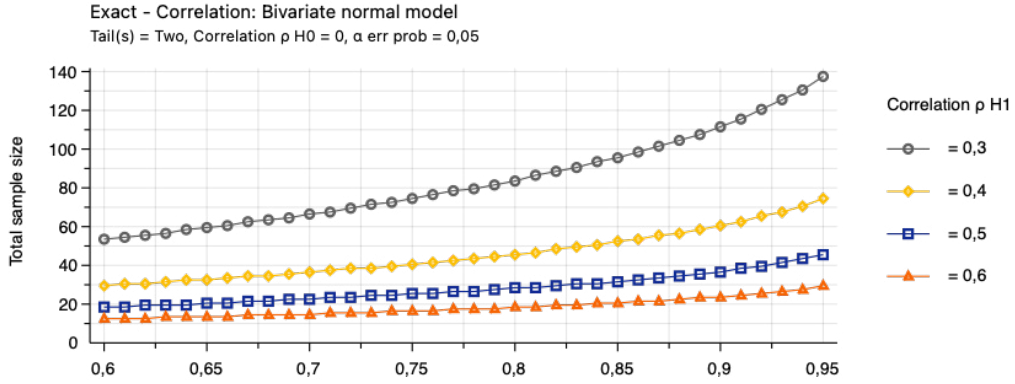
ANALYSES

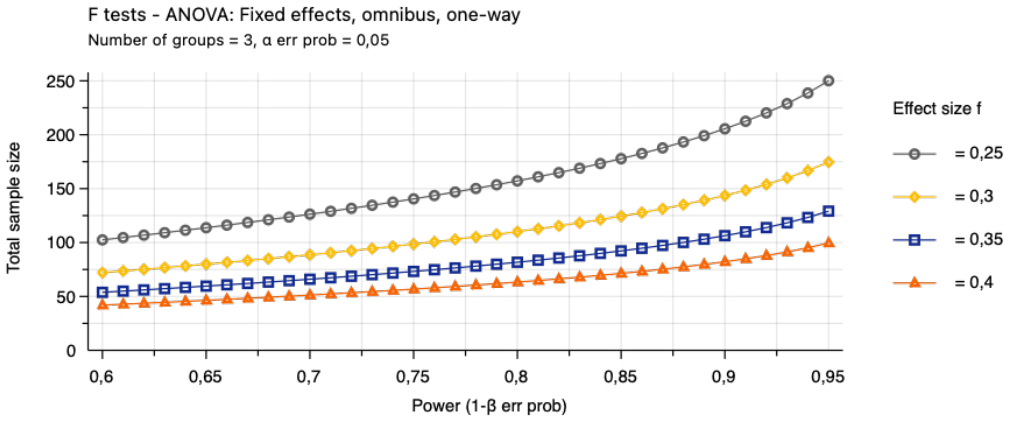
SAMPLE SIZE

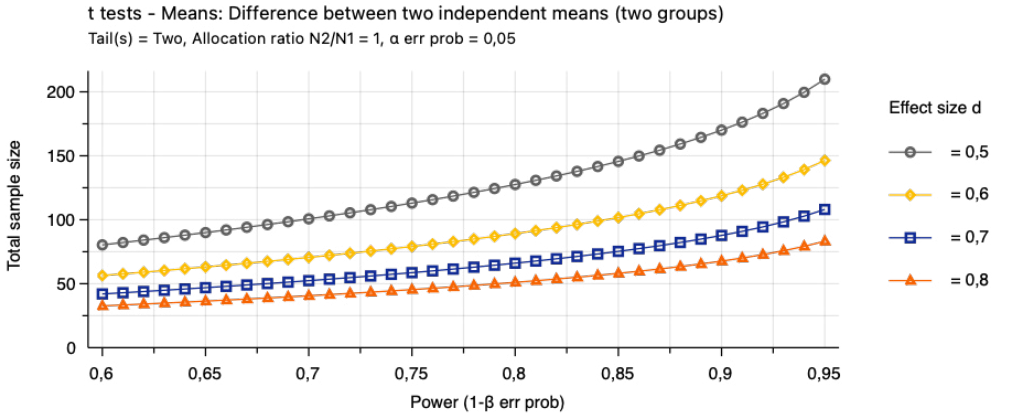
We conducted power analyses using G-power[18] to determine what an appropriate sample size for our research questions would be. We examined power for the 3 most used tests in the research, namely correlations, t-tests, and ANOVAs for most research questions, therefore we examined power for these analyses. These analyses were conducted to find the appropriate sample size to determine medium (d = 0.5) effects according to Cohen[19] with a power (1 – β) of .80, and an error probability (α) of 0.05. These are default and recommended settings for power analyses[20]. All power analyses were conducted for two-tailed analyses, because these are stricter than one-tailed analyses (i.e., they require a larger sample), and because theoretically, we did not always have an a-priori idea about the direction of the effects.

The figures on the next page display the results of these power-analyses for different effect-sizes ranging from large to medium, and for different levels of power. To detect medium effects, the minimum required sample size for correlations is 84, the minimum required sample size for t-tests is 128, and the minimum required sample size for ANOVAs with 3 groups is 159. With our sample of 352 participants, we thus had sufficient power to detect effects.

16. Cann, A. et al. (2010). A short form of the Posttraumatic Growth Inventory.
17. Vogt, D.S. et al. (2012). Posttraumatic Maladaptive Beliefs Scale: Evolution of the Personal Beliefs and Reactions Scale.
18. Faul, F. et al. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences.
19. Cohen, J. (1988). Statistical power analysis for the behavioral sciences.
20. Kang, H. (2021). Sample size determination and power analysis using the G* Power software.


Exact - Correlation: Bivariate normal model
Tail(s) = Two, Correlation ρ H0 = 0, α err prob = 0,05
Total sample size
140
120
100
80
60
40
20
0
0,6
0,65
0,7
0,75
0,8
0,85
0,9
0,95
Correlation ρ H1
= 0,3
= 0,4
= 0,5
= 0,6


F tests - ANOVA: Fixed effects, omnibus, one-way
Number of groups = 3, α err prob = 0,05
Total sample size
250
200
150
100
50
0
0,6
0,65
0,7
0,75
0,8
0,85
0,9
0,95
Power (1-β err prob)
Effect size f
= 0,25
= 0,3
= 0,35
= 0,4


t tests - Means: Difference between two independent means (two groups)
Tail(s) = Two, Allocation ratio N2/N1 = 1, α err prob = 0,05
Total sample size
200
150
100
50
0
0,6
0,65
0,7
0,75
0,8
0,85
0,9
0,95
Power (1-β err prob)
Effect size d
= 0,5
= 0,6
= 0,7
= 0,8

PLAN OF ANALYSES

For most questions, we provide descriptive statistics. For details on how percentages were calculated, see the measurements above. We calculated percentages for those directly involved in resolving the ransomware attack, those indirectly involved, those not involved, and for the total sample (i.e., all three groups combined).

To examine differences between groups, we used a combination of various tests, depending on the level of the variables. Please note that although we report percentages (e.g., percentage of employees who agreed to a certain item) in the report, these analyses were done on the original variables to use as detailed data as possible.

First, to examine differences between those directly, indirectly, and not involved in resolving the ransomware attack, we conducted ANOVA analyses. If the omnibus test proved significant, we performed post-hoc analyses with LSD correction. For differences between those groups in nominal variables, we used chi-square tests.

To examine gender-differences and differences between IT and non-IT employees, we used t-tests for scale variables, Mann-Whitney U tests for ordinal variables, and chi-square tests for nominal variables. To examine age differences, we used spearman correlations, as many variables were measured at an ordinal level, and not all variables were normally distributed. In addition, we used t-tests with age as the outcome for binary variables.

Finally, we also used (Spearman) correlation analyses to examine relationships among symptoms in the 3 phases of the MIRA phase model.

All analyses were conducted with an alpha level of .05 and using two-tailed analyses.

RESULTS

The tables below display a complete overview of all analyses. Each table displays the results separately for each level of involvement with the ransomware attack, and for the total group of employees who filled out the questionnaire.

PHASE 1

SCORES ON THE SYMPTOMATIC SYMPTOM SCALE 8

Symptom	Directly involved	Indirectly involved	Not involved	Total
Stomach or bowel problems	12.4%	15.9%	7.5%	11.7%
Back pain*	30.5%	31.9%	18.7%	26.4%
Pain in your arms, legs, or joints	4.8%	10.6%	9.7%	8.5%
Headaches*	43.8%	37.2%	22.4%	33.5%
Chest pain or shortness of breath	8.6%	8.9%	6.7%	8.0%
Dizziness	8.6%	6.2%	7.5%	7.4%
Feeling tired or having low energy*	54.3%	46.9%	26.1%	41.2%
Trouble sleeping*	60.0%	51.3%	35.1%	47.7%

* significant differences between groups.

We found significant differences between groups for back pain, headaches, feeling tired or having low energy and trouble sleeping. Interestingly, these only differed significantly between those involved and those not involved, there were no significant differences between those directly involved and those not involved.

OFFICIAL CUT-OFF SCORES FOR THE SYMPTOMATIC SYMPTOM SCALE 8

Symptom	Directly involved	Indirectly involved	Not involved	Total
Minimal	59.0%	59.5%	76.9%	66.0%
low	21.0%	21.6%	12.7%	18.0%
Medium	11.4%	7.2%	2.2%	6.6%
High	7.6%	2.7%	5.2%	5.1%
Very high	1.0%	9.0%	3.0%	4.3%

PHASE 2

REPORTED SYMPTOMS AFTER THE FIRST MOMTH OF A RANSOMWARE INCIDENT

Symptom	Directly involved	Indirectly involved	Not involved	Total
Problems with eating (such as poor appetite or binge eating)	8.8%	4.0%	4.9%	5.7%
Trouble sleeping*	42.3%	41.9%	28.2%	36.8%
Fatigue*	57.0%	43.0%	30.0%	42.5%
Headaches*	28.4%	27.7%	14.6%	22.9%
Heart palpitations	8.2%	7.7%	5.6%	7.0%
Worrying or negative thoughts	60.6%	69.1%	56.7%	61.9%
Difficulty concentrating*	23.7%	31.8%	16.1%	23.6%
Severe emotions (such as anger or sadness)	18.6%	25.5%	16.7%	20.1%
Weight loss or weight gain	11.7%	4.0%	4.8 %	6.6%

* significant differences between groups.

We found significant differences between groups for trouble sleeping, fatigue, headaches and difficulty concentrating. The group directly involved reported more trouble sleeping and more fatigue than the group not involved.

PHASE 3

CUT-OFF SCORES FOR THE IMPACT OF EVENT SCALE

	Directly involved	Indirectly involved	Not involved	Total
Subclinical	50.0%	45.1%	62.7%	53.3%
Mild	37.5%	38.1%	37.5%	34.5%
Clinical - moderate	6.7%	8.8%	6.7%	7.4%
Clinical - severe	5.8%	6.7%	1.5%	4.8%
Clinical help needed - total	12.3%	15.5%	8.2%	12.2%

The impact of event scale measures distress after traumatic events. The table above displays scores in each group according to official cut-off scores. Scores above 26 are seen as so severe that clinical help is needed. In this sample, 12.3% of those directly involved and 15.5% of those indirectly involved fall into this category.

PERCENTAGE OF EMPLOYEES WHO INDICATE THAT SYMPTOMS ON THE IMPACT OF EVENT SCALE OCCUR FOR THEM

	% Directly involved		% Indirectly involved		% Not involved		% Total	
Symptoms	Occurs	Occurs often	Occurs	Occurs often	Occurs	Occurs often	Occurs	Occurs often
1. I thought about it when I didn't mean to*	82.7	27.9	87.6	23.9	73.9	13.4	80.9	21.1
2. I avoided letting myself get upset when I thought about it or was reminded of it*	38.1	7.6	50.0	5.4	30.1	2.3	38.9	4.9
3. I tried to remove it from my memory	33.3	2.9	51.4	5.4	33.6	3.8	39.2	4.0
4. I had trouble falling asleep or staying asleep because of pictures or thoughts about it that came into my mind*	44.2	3.9	41.6	9.7	24.6	4.5	35.9	6.0
5. I had waves of strong feelings about it	34.3	4.8	21.4	4.5	17.3	2.3	23.7	3.7
6. I had dreams about it*	24.8	1.9	27.7	4.5	12.9	0.0	21.2	2.0
7. I stayed away from reminders of it	20.2	3.9	33.0	6.3	22.6	5.3	25.2	5.2
8. I felt as if it hadn't happened or wasn't real*	13.3	1.0	20.0	0.9	24.6	2.2	19.8	1.4
9. I tried not to talk about it	18.1	2.9	27.4	7.1	17.9	1.5	21.0	3.7
10. Pictures about it popped into my mind	25.7	1.0	32.1	2.7	18.1	2.3	24.9	2.0
11. Other things kept making me think about it	45.2	12.5	54.1	14.4	40.2	8.3	46.1	11.5
12. I was aware that I still had a lot of feelings about it, but I didn't deal with them*	59.8	16.7	49.6	9.9	36.8	5.3	47.7	10.1
13. I tried not to think about it*	31.4	2.9	43.4	8.0	27.8	3.8	33.9	4.8
14. Any reminder brought back feelings about it*	33.3	0.0	36.6	3.6	21.8	1.5	30.0	1.7
15. My feelings about it were kind of numb	15.4	0.0	19.1	0.9	6.7	1.5	13.2	0.9

* Significant differences between groups.

The group indirectly involved scored higher than the group not involved for questions 1, 2, 4, 6, 13 and 14. The group directly involved scored higher than the group not involved on questions 1 and 12. The group not involved scored higher than the group directly involved on question 8.

PERCENTAGE OF EMPLOYEES WHO AGREE WITH NEGATIVE STATEMENTS FROM THE POSTTRAUMATIC MALADAPTIVE BELIEF SCALE

	Directly involved	Indirectly involved	Not involved	Total
I don't feel safe anywhere anymore	7.6	17.9	10.5	12.0
The world is very dangerous	63.8	69.4	55.6	62.5
I don't trust anyone anymore	14.4	27.0	15.8	19.0
I avoid other people because they might hurt me	11.5	16.2	9.0	12.1
I have lost respect for myself	2.9	4.5	3.0	3.5
I don't feel confident that I can make good decisions for myself	10.6	17.3	13.6	13.9
Because I don't feel able to protect myself, I have lost my sense of freedom	2.9	6.4	3.0	4.1

There were no significant differences between groups.

PERCENTAGE OF EMPLOYEES WHO DISAGREE WITH POSITIVE STATEMENTS FROM THE POSTTRAUMATIC MALADAPTIVE BELIEF SCALE

	Directly involved	Indirectly involved	Not involved	Total
Other people can be genuinely loving toward me	38.1	46.9	44.7	43.4
I am a good person	17.3	16.5	20.3	18.2
It is possible for me to have close and loving feeling with other people	20.4	21.8	17.7	19.8
I trust my own judgement	15.4	14.3	13.5	14.3
Some people can be trusted	19.2	13.8	10.6	14.2
I feel as though I can depend on other people*	10.6	16.4	9.8	12.1
Most people are basically caring*	16.4	24.6	16.5	19.0
I comfort myself very well when I'm upset*	17.3	27.3	16.7	20.2

* Significant differences between groups.

There were few differences between groups in the posttraumatic maladaptive belief scale. Only fort the final 2 positive statements, scores were higher for those not involved than those indirectly involved.

DID YOU CHANGE JOBS AS A DIRECT OR INDIRECT CONSEQUENCE OF THE RANSOMWARE ATTACK?

Job change	Directly involved	Indirectly involved	Not involved	Total
No, nor have I considered that	79.0	82.1	92.5	85.2
No, but I have considered looking for other work (or am still considering it)	17.1	15.2	6.7	12.5
Yes, I still work at the same organization but now have a different position	2.9	2.7	0.7	2.0
Yes, I now work at another organization	1.0	0.0	0.0	0.3
Total considered or still considering job change	21	17.9	7.4	14.8

Note: we indicated: "directly or indirectly implies that you would not have searched for other work if the attack would not have happened".

POSITIVE EXPERIENCES

PERCENTAGE OF PEOPLE EXPERIENCING POSTTRAUMATIC GROWTH ACCORDING TO POSTTRAUMATIC GROWTH SCALE

	Directly involved		Indirectly involved		Not involved		Total	
	Occurs	Occurs strongly	Occurs	Occurs strongly	Occurs	Occurs strongly	Occurs	Occurs strongly
1. I changed my priorities about what is important in life*	34.3	8.6	41.6	6.2	35.3	0.8	37.0	4.8
2. I have a greater appreciation for the value of my own life*	32.4	4.8	35.4	7.1	27.8	2.3	31.6	4.6
3. I am able to do better things with my life	26.0	5.8	29.7	3.6	26.2	1.5	27.3	3.5
4. I have a better understanding of spiritual matters	6.7	1.0	11.6	1.8	9.9	1.5	9.5	1.4
5. I have a greater sense of closeness with others*	39.1	3.8	32.4	3.6	18.8	2.3	29.2	3.2
6. I established a new path for my life	13.5	1.9	11.8	0.9	11.3	0.8	12.1	1.2
7. I know better that I can handle difficulties*	66.7	16.2	62.0	9.7	38.8	3.0	54.6	9.1
8. I have a stronger religious faith	1.9	1.0	4.5	0.0	0.8	0.8	2.3	0.6
9. I discovered that I'm stronger than I thought I was*	46.7	12.4	31.5	3.6	15.2	0.8	29.9	5.2
10. I learned a great deal about how wonderful people are*	61.8	15.7	51.8	10.9	42.5	4.5	51.2	9.8

* Significant differences between groups

There were significant differences between groups on several items. Those indirectly involved scored higher than those not involved on questions 1, 2, 7 and 9, and higher than those directly involved on question 9. Those directly involved scored higher than those not involved on questions 5, 7 and 10.

HOW WOULD YOU DESCRIBE THE CLOSENESS WITH YOUR COLLEAGUES IN THE FIRST MONTH AFTER THE ATTACK?

	Directly involved	Indirectly involved	Not involved	Total
Strongly isolated	1.0	5.4	0.0	2.0
Isolated	1.9	8.9	10.4	7.4
Somewhat isolated	7.6	13.4	23.1	15.4
Quite close	36.2	46.4	48.5	44.2
Close	33.3	15.2	14.9	20.5
Closer than ever	20.0	10.7	3.0	10.5

NEEDS

WHAT DID YOU NEED AFTER THE ATTACK?

	Directly involved	Indirectly involved	Not involved	Total
1. I would have liked (more) professional help afterwards to deal with the attack*	20.2	20.0	6.8	15.0
2. I would have liked more reflection on the mental impact of the attack*	32.4	25.0	15.8	23.7
3. I would have enjoyed contact with people who have also experienced a ransomware attack*	27.9	29.7	11.3	22.2
4. I would have liked to experience more support from my supervisor regarding the mental impact of the attack on me and others*	21.0	15.2	9.7	14.8
5. I would have liked to know more about the mental impact of ransomware attacks	31.4	33.6	25.4	29.8
6. I would have liked concrete tools to deal with the attack myself	31.4	39.3	26.3	32.0
7. I would have liked to know how I could help others around me to cope with the attack*	42.9	43.4	29.3	37.9
8. I would have liked to discuss and reflect with colleagues about the attack*	66.7	55.8	50.0	56.8

Both those directly involved and those indirectly involved score significantly higher than those not involved on questions 1, 3 and 7. Those directly involved also score higher than those not involved on questions 2, 4 and 7.

DIFFERENCES BETWEEN PEOPLE

DIFFERENCES IN MENTAL IMPACT BETWEEN IT AND OTHER DIRECTLY INVOLVED

	IT	Other
Symptoms first week (SSS-8)	4.6	3.9
Symptoms first month	3.1	2.8
Distress since attack (post-traumatic symptoms, IES)	12.4	12.6
Posttraumatic growth (PGI-SF)*	10.3	6.4
Posttraumatic maladaptive beliefs (PMBS)	40.7	41.9
Considered or still considers changing jobs (percentage)	22.2%	20.0%
Closeness with colleagues	4.47	4.76

* Significant differences between groups

DIFFERENCES BETWEEN PEOPLE IN IT AND NOT IN IT IN POST TRAUMATIC GROWTH

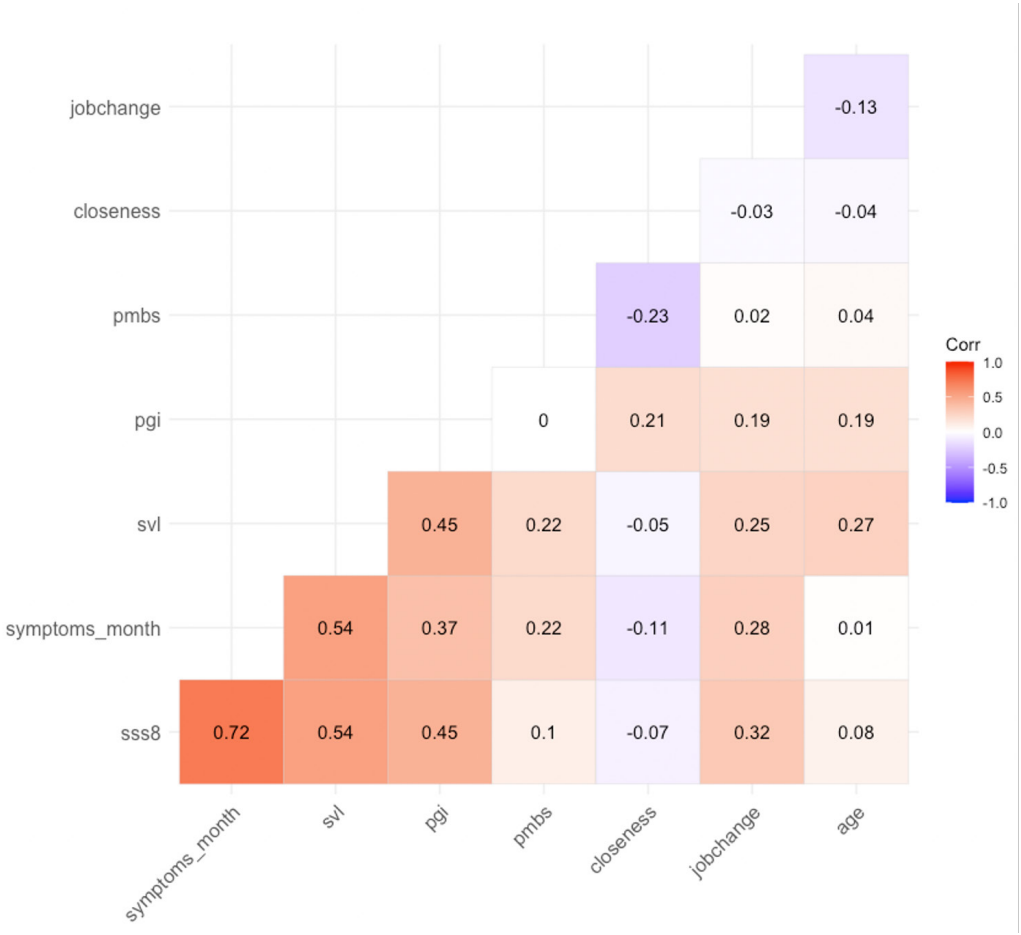
Items	Involved with IT	Not involved with IT
I changed my priorities about what is important in life*	1.3	0.6
I have a greater appreciation for the value of my own life*	1.1	0.5
I am able to do better things with my life*	1.0	0.4
I have a better understanding of spiritual matter	0.1	0.1
I have a greater sense of closeness with others	1.0	0.8
I established a new path for my life	0.4	0.2
I know better that I can handle difficulties	2.0	1.6
I have a stronger religious faith*	0.1	0.0
I discovered that I'm stronger than I thought I was*	1.6	0.9
I learned a great deal about how wonderful people are	1.8	1.4

* Significant differences between groups

GENDER DIFFERENCES IN MENTAL IMPACT

Scale	Average men	Average women
Symptoms first week* (SSS-8)	3.3	5.1
Symptoms first month	2.3	3.3
Distress since attack* (post-traumatic symptoms, IES)	10.6	17.1
Posttraumatic growth (PGI-SF)	6.6	6.7
Posttraumatic maladaptive beliefs (PMBS)	42.0	41.9
Considered or still considers changing jobs (percentage)	14.8%	13.7%
Closeness with colleagues	4.1	4.0

* Significant differences between groups



Correlations between symptoms experienced in different phases. Sss8 is the total number of symptoms experienced in week 1. Symptoms month is the total number of symptoms in the first month.

REFERENCE LIST

1. SonicWall (2022). SonicWall Cyber threat report.
2. IBM (2022). Security Incident Responder Study. Available at https://www.ibm.com/downloads/cas/XKOY5OLO
3. APA, dictionary of psychology. Available at https://dictionary.apa.org/coping
4. Therapist AID LLC (2018). Healthy and unhealthy coping strategies. Available at https://www.therapistaid.com/therapy-worksheet/healthy-unhealthy-coping-strategies
5. Lim, J. and Dinges, D. F. (2010). A meta-analysis of the impact of short-term sleep deprivation on cognitive variables. Psychological Bulletin, 136, 375–389. Available at https://doi.org/10.1037/a0018883
6. Cheng, J. (2022). The Human Consequences of Ransomware Attacks. ISACA JOURNAL, 3, 1-4. Available at https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/the-human-consequences-of-ransomware-attacks
7. Henning, J. (2016). Crypto-Malware. Researchscape International. Available at https:// kapost-filesprod.s3.amazonaws.com/published/56da036de9d2fe94b70001b1/crypto- ransomwaresurvey-results. pdf?kui=ZJ4TAAmGPXQxX_G_GZGigA
8. Horowitz, M., Wilner, N., & Alvarez, W. (1979). Impact of Event Scale: A measure of subjective stress. Psychosomatic medicine, 41, 209-218. Available at https://doi.org/10.1097/00006842-197905000-00004
9. Sterling, M. (2008). The impact of event scale (IES). Australian Journal of Physiotherapy, 54, 78. Available at https://doi.org/10.1016/s0004-9514(08)70074-6
10. Qureshi, M. I., Iftikhar, M., Abbas, S. G., Hassan, U., Khan, K., & Zaman, K. (2013). Relationship between job stress, workload, environment and employees turnover intentions: What we know, what should we know. World Applied Sciences Journal, 23, 764-770. Available at https://doi.org/10.5829/idosi.wasj.2013.23.06.313
11. Tedeschi, R. G., & Calhoun, L. G. (2004). Posttraumatic growth: conceptual foundations and empirical evidence. Psychological inquiry, 15, 1-18. Available at https://doi.org/10.1207/s15327965pli1501_01
12. Matud, M.P. (2004). Gender differences in stress and coping styles. Personality and Individual Differences, 37, 1401–1415. Available at https://doi.org/10.1016/j. paid.2004.01.010
13. Verhoeven, P. S. (2014). Wat is onderzoek? Praktijkboek methoden en technieken voor het hoger onderwijs. Boom. ISBN 978-90-2440-694-4
14. Gierk, B., Kohlmann, S., Kroenke, K., Spangenberg, L., Zenger, M., Brähler, E., & Löwe, B. (2014). The somatic symptom scale-8 (SSS-8): a brief measure of somatic symptom burden. JAMA internal medicine, 174, 399–407. Available at https://doi.org/10.1001/ jamainternmed.2013.12179
15. Brom, D., & Kleber, R. J. (1985). De Schok Verwerkings Lijst [The Dutch version of the Impact of Event Scale]. Nederlands Tijdschrift voor de Psychologie, 40, 164–168.
16. Cann, A., Calhoun, L. G., Tedeschi, R. G., Taku, K., Vishnevsky, T., Triplett, K. N., & Danhauer, S. C. (2010). A short form of the Posttraumatic Growth Inventory. Anxiety, Stress, & Coping, 23, 127-137. Available at https://doi.org/10.1080/10615800903094273
17. Vogt, D. S., Shipherd, J. C., & Resick, P. A. (2012). Posttraumatic Maladaptive Beliefs Scale: Evolution of the Personal Beliefs and Reactions Scale. Assessment, 19, 308–317. Available at https://doi.org/10.1177/1073191110376161
18. Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behavior research methods, 39, 175-191. Available at https://doi.org/10.3758/bf03193146
19. Cohen, J. (1988). Statistical power analysis for the behavioral sciences. Routledge. ISBN 978-1-134-74270-7
20. Kang, H. (2021). Sample size determination and power analysis using the G* Power software. Journal of educational evaluation for health professions, 18. Available at https://doi.org/10.3352/jeehp.2021.18.17