Earth, Life & Social Sciences
Kampweg 55
3769 DE Soesterberg
P.O. Box 23
3769 ZG Soesterberg
The Netherlands

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77

TNO report
TNO 2017 R11575

Human Factors in Cyber Incident Response: Needs, collaboration and The Reporter

Date	October 2017
Author(s)	Dr. M.A.A. Huis in 't Veld Dr. R. van der Kleij Ir. G. Kleinhuis Drs. L. de Koning Drs. J. Kort Ir. P.P. Meiler J.A. van Schendel MSc Ing. S. Schultz Dr. H.J. Young
Number of pages	47 (incl. appendices)
Number of appendices	1
Project name	ERP HE Adaptive Cyber Automation
Project number	060.26935

Contents

1 Introduction

Computer Security Incident Response Teams (CSIRTs) play an increasingly important role in protecting companies against cyber-attacks. When a network is subject to a cyber-attack the CSIRT is responsible for stopping the adversary and mitigating the effects of the attack. Some larger organizations employ their own CSIRT, but it is not uncommon for organizations to have outsourced these functions to external parties, such as professional IT security companies. These companies then monitor the networks of many other organizations simultaneously from within their own monitoring centre, and respond with their CSIRT to each incident as it occurs.

Large cyber-incidents that occur infrequently are a challenge for these CSIRTs, as large quantities of information are released in a short period of time, the complexity of the problem that needs to be addressed is high, and the CSIRT working on the cyber-incident is likely to be a distributed team (when out-sourced). Many CSIRTs struggle with how to deal with these challenges, because there are at least three processes that need to be controlled: the cyber-incident itself (problems need to be fixed), the management of the incident (is everything under control yet?) and the communication within the team and with the client (including upper management). Also, in incident response, teams have to be formed ad hoc, and the majority of the organizations where the incident occurs are not very well known to the IT company that is being contacted. This poses problems for the definition and allocation of team roles, the information exchange between the affected organization and the CSIRT and, in many ways, resembles a multi-party crisis management situation.

It is of vital importance for companies to be able to guarantee their resilience to cyber-attacks. It is, for instance, both commercially and legally unacceptable for any company to lose data (privacy information of their clients) and money because of such an attack. And loss of online service for more than a few hours is socially and economically unacceptable. Therefore, once attacked, a company should be up and running again as soon as possible. CSIRTs play a crucial role in the recovery from a cyber-attack (as well as in many other issues such as prevention and fall-back). If they are able to quickly assess the situation, stop the attack, and come up with adequate solutions to prevent any loss of data or money and resolve the service, then this is extremely valuable.

Scientifically, this project falls under the general heading of ‘adaptive automation’, as explored in the Early Research Program Human Enhancement. Although the need for adaptive automation might be different than the type of automation explored until now, CSIRT-incident response teams are faced with the need to constantly remain adaptive (‘sustained adaptability’) while at the same time they need to automate as many of their incident management procedures as possible (including information management), given the time pressure and volume of data involved.

Sustained adaptability is needed because CSIRTs operate in a dynamic situation: the environment, stakeholders, demands, contexts, and constraints are constantly changing. The mode of controlling the situation is based on models and predictions, with multiple goals being dealt with simultaneously, with plenty of time (as subjectively experienced), and with elaborate evaluations of outcomes. As teams are confronted with setbacks, delays and unexpected events, their control modes may gradually deteriorate and transition to ‘tactical’, ‘opportunistic’, or even ‘scrambled’ (Hollnagel, 1993).

The focus when developing a CSIRT is currently primarily on the technological capabilities of the centre and the team. However, the need for human factors in cyber is increasingly being acknowledged as an important next step on the road to improving the speed and efficiency of CSIRT operators. The importance of factors such as proper training, situation awareness, competences, communication, and information management, and the lack of sufficient knowledge on these factors to become more efficient, is becoming more and more recognised (Rajivan & Cooke, 2017).

The focus of the current project on professional CSIRT teams is new and complements the research on how to increase security awareness within companies. Improvements to the overall security awareness within a company reduces the occurrence of easy-to-fix problems but increases the risk of complex attacks. Therefore this program puts the focus on the experts in the CSIRTs that need to handle these more complex cyber-attacks. For this, we draw upon our existing knowledge of control operations in military and crisis management settings. However, the current use case of CSIRT teams is unique in terms of the combination of speed of processing of large amounts of ambiguous information, need for close cooperation in ad hoc teams, the dynamics of the environment and need for fast sharing and sensemaking of information within the teams involved.

This report provides an overview and summary of the activities carried out in this project on adaptive cyber incident response in 2017. We have attempted to give the order and description of these activities a logical structure to increase the readability of the report. We advise the reader, however, to keep in mind that this report represents a documentation and synopsis of these activities as opposed to an integration.

Chapter 2 reports on the needs assessment we conducted to kick off the project. The focus here was to identify the most pressing problems experienced by CSIRTs in regards to behavioural and information processes. The results of this analysis formed the basis for the subsequent conceptual work on collaborative sensemaking and the development of our solution prototype, The Reporter.

Chapter 3 describes a process analysis of CSIRTs, which was performed to get a better understanding of how they work and what the potential bottlenecks are. A process, as the term is used in this project, is carried out by people and systems, with information as both the input and output. It is possible to develop a process profile for various purposes, where a profile is defined as a combination of people, systems, work processes, roles, organizations, information and goals. A profile can be used to identify attention points and to manage effective task distribution and information dispersal.

Chapter 4 provides an overview of the concept of collaborative sensemaking, which became central to this project as a result of the needs assessment. We describe the concept, how it can be applied to CSIRTs and how it can be supported in a cyber incident response environment.

Chapter 5 describes the solution prototype, The Reporter. The purpose of The Reporter is to support communication and work processes in the context of CSIRT operations, based on the principles of collaborative sensemaking. The basis of The Reporter is a support system that is task oriented, team oriented and human aware.

Chapter 6 describes the results of interviews with team members and observational work conducted in the project during an exercise involving cyber incident response. Based on these observational opportunities, we were able to 1) assess the validity of our conclusions from the needs analysis and 2) provide an indication of how the Reporter’s functionalities may meet the needs experienced by CSIRTs.

Chapter 7 describes the final event of the Early Research Program (ERP) within which this project was carried out. Here, we hosted a session on this project with the focus on informing participants of the project and the results, including a demonstration of a prototype of The Reporter.

Chapter 8 provides an overview of the main conclusions of this project and identifies directions for future research.

2 Needs assessment[1]

A needs assessment was conducted to identify gaps between current and desired incident handling practices. A needs assessment is a systematic process for determining and addressing 'gaps' between current results and desired result; or 'wants' (Kaufman, Rojas, & Mayer, 1993; Watkins, Leigh, Platt, & Kaufman, 1998). An additional goal of the needs assessment described in this paper was to provide directions for future research and development for improving the effectiveness of team performance in incident response.

To eventually provide for an effective solution strategy we constructed a needs assessment model consisting of four assessment categories: Organization, Team, Individual and Instrumental (see Figure 2.1). Organization needs pertain to incident handling behaviour or tangible outcomes, such as time to identification, or ability to remove threat. Team performance needs pertain to the state of the team or level of team performance required for satisfactory functioning, such as team structure. Individual needs pertain to individuals' attitudes about the organization or themselves, such as job satisfaction or competences. Instrumental (or technical) needs are interventions or products that are required to obtain a satisfactory level of functioning.

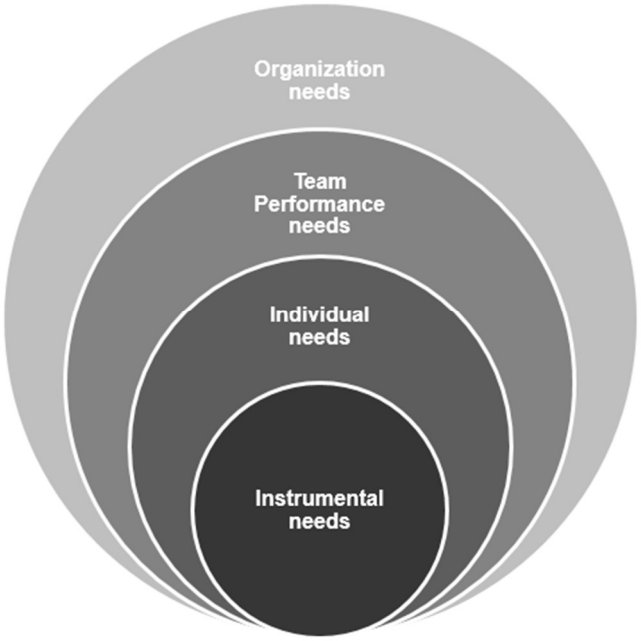

Figure 2.1. Cyber security needs assessment model.

An important step in needs assessment is gathering appropriate and sufficient data. There are many approaches identified in the literature for completing an assessment. We chose a multi-method data-triangulation technique relying on literature reviews and survey data (see also, Watkins et al., 1998).

[1] This chapter is based on Van der Kleij et al. (2017).

For the literature review a three step structured approach was used to determine the source material for the review as suggested by Webster and Watson (2002). The first step was to search relevant journal databases and the web for identification of relevant articles. The Scopus library database and Google Scholar search engine were used to get published content, but also to find content not yet indexed by library databases. The search terms challenges, needs, issues, CERT, and CSIRT, were used on Scopus database and in our web search. The search terms were used singular and in combination for all fields (including title, abstract, and full text). As a second step, backward reference searching was performed on the citations for the articles that were identified in step one to determine prior articles. Forward reference searching was used as a third step to identify articles citing the key articles identified in the previous steps. The library database search, the web search and reference searching methods resulted in 31 relevant contributions, which are cited throughout this report. Hence, in these contributions challenges or needs are discussed that could hinder or improve the performance of incident response teams.

Furthermore, a selection of Dutch public and private cyber security organizations were contacted to participate in an interview. This resulted in five semi-structured interviews with senior management of public and private sector CSIRTs.
The interviews were used to validate our findings from the literature search.
The protocol that we used was approved by our institutional ethics committee, as was our study design. These five CSIRTs included a governmental coordination centre, internal and commercial CSIRTs, which were all licensed at the time to use the name CERT by Carnegie Mellon University. The interviews included questions about challenges in incident handling that were identified in content from library databases and other sources. An example question is: “We identified several challenges in incident handling in literature. Could you have a look at these issues and explain to us which of these issues apply to your practice and why”?
Each interview took approximately two hours to complete. All subjects gave written informed consent in accordance with the Declaration of Helsinki to participate in the interview and to publish the research in scientific outlets. Transcripts of these interviews were made afterwards by the interviewers and were sent to all the interviewees who agreed to check them (cf. Rowley, 2012).

2.1 Results

As mentioned, we constructed a needs assessment model for categorizing needs and wants that play a role in incident response consisting of the four assessment groups described earlier. This model is composed of organizational categories (organization, team and individual) and one instrumental or technical category. Central to this is the idea that wants or challenges can have an organizational, team, individual, or technical origin or a combination thereof (cf. Security Incident Management Maturity Model [SIM3]) (Stikvort, 2015). In Table 2.1, for each of these four categories, we indicate which four needs and wants were most frequently indicated by the interviewees. Discussion takes place in subsequent paragraphs and in the discussion section.

Table 2.1: Overview of needs and wants of Incident Response Teams.

Organization needs
• Coordination and sharing information with outside parties
• Organizational & incident learning
• Measuring the effectiveness of incident handling
• Collaborative problem-solving capacity & shared incident awareness
Team performance needs
• Information sharing and decision making across personnel shifts & handoffs
• Work within a larger (multiteam) system consisting of multiple interacting teams, including IT personnel from customer
• Keeping everybody informed & staying informed, especially when working distributed
• Shared team knowledge: Information about the roles and expertise of each team member, including members of outside parties involved in the incident handling process
Individual needs
• Getting and retaining good skilled personnel & acquiring relevant competences
• Deciding on when to escalate an incident
• Ethical & legal aspects of the work
• Dealing with work load variations: managing peaks and underload
Instrumental needs
• Estimating the initial impact and risk of cyber security incidents
• Need for better interpersonal communication tools, especially during larger incidents
• Providing good & structured reports of incidents
• Creating useful (visual) overviews at any particular point in time for a different audience (e.g., customer, management, colleagues)

2.1.1 Organization Needs

In today's networked working environment resolving incidents typically requires social interactions, information sharing and collaboration between organizations. A CSIRT does not operate in a vacuum but within the context of a complex sociotechnical system (Rajivan & Cooke, 2017). The most important cooperation partners for CSIRTs are fellow teams (West-Brown, Stikvoort, Kossakowski, Killcrece, & Ruefle, 2003). Other teams could provide information in support of handling the incident. The interviews made clear that sharing information is not as easy as one might think. Many web-based tools are available to support information sharing between organizations. However, the extent to which teams are able or willing to exchange information and to cooperate on confidential issues depends on any existing trusted relationship they may have with each other. Formal (written) agreements between teams or organizations to exchange information and (national) platforms for trusted CSIRT communication are often in place to manage trusted information exchange. Although CSIRTs may benefit from trusted communication, our interviews confirmed that there are strong inhibiting factors as well (see also, Hellwig, Quirchmayr, Huber, Goluch, Vock, & Pospisil, 2016; Rajivan & Cooke, 2017; Silicki, Krzysztof, & Mirosław, 2008; Tetrick et al., 2016). For example, commercial CSIRTs' upper management generally do not like their team's resources spent on 'outside' parties, such as competing CSIRTs (see also, West-Brown et al., 2003). Moreover, client companies are usually not interested in information sharing with the CSIRT community (Hellwig, et al., 2016).
Companies are motivated to protect their reputation as a cyber safe and secure organization. It is important that the threats they face are quickly and quietly solved. Sharing information about a compromised system may put them in a vulnerable position (Tetrick et al., 2016, p. 113).

Incident learning can be seen as the process of creating, retaining and transfer of knowledge regarding incident handling within the organization. CSIRTs seem to struggle with incident learning (cf. Tøndel, Line, & Jaatun, 2014). The practice of incident response frequently does not result in the improvement of strategic security processes such as policy development and risk assessment. Ahmad, Hadgkiss, and Ruighaver (2012) add to these findings that when a post-incident review process does take place it usually focuses "on 'high impact' incidents rather than 'high learning' (i.e. potentially useful incidents from a learning perspective), incidents and 'near misses'" (p. 1). So called false positives and threat hunts with negative outcomes are often not documented in ticketing systems by analysts. Hence, there is the risk for analysts, in the already information overloaded cyber security environment, to respond to weak signals that have already been cleared as non-significant by fellow team workers.

Another important organizational need is the ability to measure the effectiveness of services and the effectiveness of the team itself. Relatively little is being done by the companies interviewed to measure how effective their incident response services are in handling incidents. This is further hindered by the fact that there are hardly any metrics available to objectively measure the effectiveness of incident handling (cf. Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014; see also Wiik, Gonzalez, & Kossakowski, 2006). To quote one of the interviewees: "we do not know how effective our services are." Granåsen and Andersson (2016) found that a combination of technical performance measurements and behavioural assessment techniques are needed to effectively assess team effectiveness. Many technical metrics are already regularly and successfully used to assess incident management, such as speed to solution, time to identification, number of errors, costs, and so forth. These are important for the lessons learnt phase of incident response (see also Tøndel et al., 2014). Other indicators, such as incident rates over time and mean time to repair, could also be beneficial to achieve a better view of the origin of incidents, which system domains and particular applications are involved, and so forth. What is sorely lacking, however, are behavioural metrics to assess processes such as team performance and cooperation.

Yet another organizational level need that we would like to mention is the ability to be better at the process of assessing the incident. It is often difficult to make a good assessment of the incident at the start of the incident handling process. CSIRTs often face unfamiliar problems and have to make sense out of a seemingly unstructured situation (see also, Wu, Convertino, Ganoe, Carroll, & Zhang, 2013). The interviewees often referred to the iceberg metaphor in describing their work, in which the greater part of the iceberg is hidden under water so the part that you see at the onset of the incident is much smaller than the part that is hidden.
An important CSIRT task is to find out how big the 'iceberg' actually is, according to the interviewees. It would be interesting to find out whether some sort of procedural support could be envisioned in aid of this process to benefit CSIRT performance.

2.1.2 Team Performance Needs

Cyber incident handling errors often occur during handoffs (Steinke, Bolunmez, Fletcher, Wang, Tomassetti, Repchick, & Tetrick, 2015). Handoffs are the moments during which work is passed from one person to another person, for instance between team personnel shifts.

However, handoffs can also take place within shifts, between individuals, people and technology, an individual and a team, and one team and another team, creating multiple places for errors and mistakes in the process. When incidents arise, there is a need for team members to be able to effectively communicate all information associated with those incidents throughout the team. For example, when the incident falls outside a team member's ability and it needs to be handed over to colleagues with greater ability or familiarity with the incident at hand (cf. Tetrick et al., 2016, p. 80). In the interviews the fact was acknowledged that handoffs can be especially challenging in large scale incidents, spanning several days and involving multiple parties.

Another important need is the ability for CSIRTs to work within a larger (multiteam) system, which consists of multiple interacting and closely connected component teams, from within the own organization, but sometimes including IT personnel from other organizations, such as client organizations (Chen et al., 2014; Tetrick, et al., 2016: p. 10). To quote Chen et al., (2014), "each team in the system has its own domain expertise, jargon, demographics, culture, structure, and temporal dynamics. In such contexts, team members must be comfortable working across team boundaries to collaborate and share information. Each team also brings its own expertise to the system, and all involved teams must work together effectively to accomplish a shared goal" (p. 62) (see also, Van der Kleij, De Vries, Walter, Van der Vegt, Visser, Essens, & Vogelaar, 2011). A specific component team can excel in teamwork but still fail to resolve cybersecurity incidents due to mistrust or a lack of communication among individual component teams (Tetrick et al., 2016, p. 10).

Chen et al. (2014) illustrate the difficulties multiteam systems face with an example of a provincial reconstruction team (PRT). PRTs are teams staffed with smaller military and civilian units helping local communities in instable countries with reconstruction work. Chen and colleagues describe an example in which, due to communication breakdowns between teams in the PRT, time and resources were wasted, delaying the handing out of critical medical aid. This highlights the necessity of communication and coordination across different system units.
As CSIRTs are also part of a multiteam system, often working on highly important tasks under time pressure, they are likely to face information-sharing challenges similar to those described in the PRT example. Effective between-team coordination and communication are needed for incident response teams to accomplish tasks efficiently and effectively.

Another need mentioned in the interviews is the ability to maintain a shared understanding of the incident and of the ongoing and planned tasks of fellow workers, especially in a geographically distributed setting. Maintaining an ongoing awareness of events and each other's endeavours is essential to achieving the coordination required for collaborative action (Van der Kleij & Te Brake, 2010). Incident response team members need to keep up with information about how particular tasks are progressing, what fellow workers are doing, who is communicating with whom, and so forth. Team members need knowledge of what other team members are doing. Without this knowledge it becomes difficult, or even impossible, to engage in coordinated teamwork.

A complicating factor is that incident response team members often work from different locations, that is, team members often work in geographically distributed teams. It is more difficult to monitor fellow team members' activities and pick up relevant information or cues in the absence of face-to-face communication. Consequently, team members must often work in an environment without any signals to indicate that a team member is busy, experiencing technical difficulties, stressed, dealing with unusual or unexpected circumstances, and so forth (Van der Kleij, Schraagen, De Dreu, & Werkhoven, 2009).

Most interviewees acknowledge that incident response teams are often formed on an ad-hoc basis. However, this does not mean that members do not know each other or are chosen randomly. Members are chosen based on expertise from a fixed pool of CSIRT employees. Notwithstanding the fact that members often have a shared understanding of how their expertise and roles fit together, the development of shared team knowledge is recognized as being beneficial to incident handling. Shared team knowledge includes information about the roles and expertise of each team member, including members of outside parties that are involved in the incident handling process (Steinke et al., 2015). With shared team knowledge, team members can more successfully coordinate their work.

2.1.3 Individual Needs

Although the need of finding and retaining good, skilled personnel and training personnel is certainly not new (see West-Brown et al., 2003), it remains relevant according to the parties we have spoken to. The expectation is that shortages of highly-skilled personnel on the market will only increase in the years to come (National Coordinator for Security and Counterterrorism, 2016). The staffing of CSIRTs requires a blend of technical and team skills (cf. Chen et al. , 2014; Steinke et al., 2015). Individual members often have to work with other team members and people from outside the parent organization. This means that several collective-level competences are important, including information sharing skills, collaboration skills, and a preference for working with others (Chen et al., 2014). The companies we have spoken to all confirm that there are often gaps in employees' social skill sets that require additional training, the hiring of additional personnel to interface between the more technical skilled personnel and customers, or that need to be taken into account when staffing smaller incident handling teams.

CSIRT work is mostly individual until a nonroutine or unfamiliar incident occurs (Chen et al., 2014). Tasks typically originate at the individual level, wherein one member identifies a potential incident and must decide whether to involve other team members to mitigate the incident, or to hand it over to a more experienced colleague. For instance, the interviews revealed that in incident response the intake of security incidents is usually performed by a low-level cybersecurity employee operating a helpdesk or call center (see also Tetrick et al., 2016, p. 80).
This member then has to decide whether mitigating the incident requires a handover or assistance from other more experienced members. Herein lies an interesting difference with other types of crisis management teams, such as firefighting teams, in which tasks usually begin at the team level, and individual members are not burdened with making decisions about when to initiate collaboration (Chen et al., 2014).

Moreover, under some circumstances, such as when time pressure is involved, individual members may erroneously conclude that the incident is familiar to them, and, consequently, fail to seek help from others (Tetrick et al., 2016, p. 83). A task analysis performed by Chen and colleagues suggests that when an event requires the other members' assistance, and the individual members decide to involve other people, several collective-level competences become important, including collaboration skills and information-sharing skills. Chen and colleagues argue that the work is multilevel in nature, comprising an individual and a collaborative level. This suggests that team members should possess the skills to know when and how to escalate events. Moreover, a set of information-sharing and collaboration norms should be established according to Chen and colleagues that "let team members accurately determine when an event requires other teams' or multiteam members' involvement" (p. 65).

A concern that was voiced by the interviewees is about integrity and consequences of ethical considerations during work on mental wellbeing of employees.
Team members sometimes encounter illegal material on client databases or are obligated to report findings to the government, for instance regarding security breaches resulting in, among others, theft, loss or misuse of personal data.
This could potentially damage the reputation of the client organization, resulting in an ethical dilemma for the incident response team member: reporting the incident or findings to legal authorities or telling the client organization to do so and trusting them to take appropriate measures.

Data breach notification laws are sometimes also responsible for peaks in workload that need to be managed by the team members accordingly. Both private and public organizations processing personal data are obliged to report any security breaches resulting in theft, loss or misuse of personal data to the Dutch data protection authority[2]. The data breach has to be reported without undue delay and if possible not later than 72 hours after the discovery of the data breach. This means that incident response teams, when theft, loss or misuse of personal data is involved or is suspected to be involved, have a limited time frame to discover what is lost and to prevent further loss of (personal) data. Hence, incident handling teams often have to work under time pressure. On top of that comes the fact that teams often have to work at night or during weekends. In an effort to save money, customers choose to seek support only after they themselves have failed to handle the incident successfully. Often this means that reporting of the incident takes place at the end of the work day, or even at the end of the work week, leaving the incident response teams the night or the weekend to work on the incident at hand.

2.1.4 Instrumental Needs

From the interviews it became clear that CSIRTs have various technical tools available to mitigate a wide variety of cyber security incidents. However, (advanced) technical tools to support the (internal) working methods of CSIRTs are largely lacking. Technical solutions for exchanging CSIRT related information can be based on standardized technical protocols like STIX, TAXII and CybOX[3]. The use of the right technical tools that support the work methods can greatly increase the effectiveness of CSIRTs.

---

[2] See also, https://www.government.nl/latest/news/2013/06/21/bill-on-obligation-to-report-data-leakage-sent-to-the-house-of-representatives
[3] https://stixproject.github.io/

The effectiveness may lie in the field of lead time of solving the incident, on the financial level and on increasing team knowledge and shared situation awareness within the CSIRT. Tools supporting work methods might include, for example, a tool to estimate the initial impact and risk of a reported cyber security incident in a structured way. The interviews revealed that the initial assessment of the size and risk of a specific cyber security incident is ascertained on an ad hoc basis and is predominantly based on the knowledge level of the CSIRT team member who first gets the incident reported.

There is also a need for better intra and inter team communication tools (Fransen & Kerkdijk, 2017). Current tools used as explained in the interviews, such as chat applications, phone calls and wikis, are often inadequate for updating shared awareness within the team, let alone between different teams, especially when there is a need for in-depth technical communication. An adequate communication tool would also support the initial decision to respond to a cyber security incident, for example in the event that information is designated as classified or if communication is necessary with government agencies in a specific format. Ticketing systems are necessary for logging all kinds of events concerning a (possible) cyber security incident but are identified as inadequate for supporting (team)work on larger scale incidents.

Yet another need that was revealed by the interviews is that for tools to provide good and structured reports. For accountability, good and structured written recording of cyber security incidents is indispensable. This implies that during the completion of the mitigation of the cyber security incident, logged events are available and accessible in an user friendly way. It became clear that a lot of logging is done and available, but technical tools to adequately translate this information into good and structured – and reader-friendly – reports is lacking.

Related to the previous need is the desire to be able to create useful (visual) overviews at any certain point in time during an incident for different audiences. Audiences may include the internal management of CSIRTs, the (management of an) organization that is affected by an incident, (commercial) business relations, government agencies or even the (public) media. The idea is that visualization tools for providing an overview of different situations during cyber security incident response will improve the understanding of the methods used by the incident handling team and will definitely help adjust the controlling. Applying visualizations will also create better understanding for different audiences for a better insight into the completion of the cyber security incident. The need for the overviews to provide the necessary information in an understandable and accessible way to different audiences implies that the tool must be able to support different levels of detail.

2.2 Discussion

A general finding from the interviews is that there is a great deal of variability in issues that CSIRTs face and in the desires for better team performance. At the same time, it became evident to us that no two CSIRTs are alike. There are many commonalities but also many differences between the CSIRTs we investigated. These differences may be due to several factors, such as type of CSIRT (e.g., internal or commercial provider), type of organization they work for (e.g., bank, manufacturing company, university, or federal agency), size of the CSIRT and the kind of services they offer. What this implies for an effective solution strategy is that innovations that work for one CSIRT might not work for others. We should keep this in mind as we consider solutions for better practice.

Taken together, if we look at the results, we see a number of mutual needs that can and should be addressed in order to improve CSIRT performance. First, learning from incidents at the organizational level seems to be in need of improvement. Problems were reported with ways to improve performance through systematically implementing a lessons learnt procedure, based on a good evaluation of the incident and how it was managed. This is crucial if CSIRTs are to evolve and structurally improve performance. Further, there is the question of training. This goes not only to keeping abreast of technological developments, but also in regards to softer, social skills such as communication and cooperation.

Second, the coming together of different component teams causes gaps in various manifestations between current and desired incident handling practices. First and foremost, perhaps, it is important to recognize that when different teams come together during a security incident, they are often not much more than a group of teams. In order to become a team of teams, in which they function as a multiteam system, they must develop new dynamics and ways of working together. Differences between team cultures hinder this process, as do differences in procedures between the teams' organizations. Information sharing is a particularly glaring problem in this context. Parties may not know what to share because they do not have a sufficient understanding of what another team needs, or they may not know with whom to share information. Furthermore, ulterior (commercial) motives, may make teams unwilling to share information. It would be interesting to investigate ways to improve the performance at this multiteam level.

Third, improvement of the assessment of the incident in terms of the extent of the problem and the seriousness of the possible consequences is a potential direction for improving performance. It is often difficult to make a good assessment of the incident and coordinate the seeking and synthesizing of data. An interesting solution strategy, in our opinion, is applying knowledge on collaborative sensemaking to the incident analysis working processes.
Collaborative sensemaking is, basically, the collaborative process of creating shared awareness and understanding out of different individuals' perspectives in situations of high complexity or uncertainty (Klein, Moon, & Hoffman, 2006).
If successful, the outcome of this process is collective understanding of the incident, at which point the proper decision to make is clear or greatly simplified (Klein, Wiggins, & Dominguez, 2010).

Fourth, characteristics of the work process are candidates for redesign.

These include the necessity to hand off work to others and ambiguities or omissions in work procedures. Consider the ethical dilemma in which a team member needs to decide to communicate privacy-sensitive information or the situation when a member needs to decide to scale an incident up or down. In principle, these need not be dilemmas: if the criteria for courses of action are clearly described in procedures, the individual need not be burdened with making these difficult – yet not incident-crucial – decisions on his/her own.

Finally, there is a need for better tools in support of team work. This may be due to unfamiliarity with the existence of certain groupware tools, such as for providing visualizations at the group level. Alternatively, it may be due to resistance to changing the way the teams have always worked, for example when it comes to using tools to estimate size and risk of an incident: This was always done based on team members' skills and experiences with similar incidents and there is no obvious need to do things differently.

3 Process of cyber incident management

This chapter describes the CSIRT process analysis. This process analysis is carried out according to a systems-architecture approach. A process, as the term is used in this project, is carried out by people and / or systems, with information as both the input and output. Each person in a CSIRT team performs his task(s) in a specific role. A person can perform more than one role but usually not at the same time. Each role has a specific profile associated with it, that characterizes the processes, systems, information and interactions (information exchanges), location of the role in the organisation, et cetera, that are important to that role.

It is possible to develop such a profile for various purposes and in various levels of detail. For our purpose, to design a support tool, a profile can be used to identify points of attention such as work overload, work underload, missing information, effective task distribution, information dissemination, et cetera. For this to work, a future support tool also needs real-time information on the actual activities of people and systems.

The processes et cetera were described according to the NATO Architecture Framework [NAF] and using the IBM Rational System Architect tool [IBM RSA]. The use of NAF implies that the different views on the processes, information exchanges, systems, roles, et cetera are widely recognizable. The use of a tool provides a way to access and export information about the processes et cetera in a structured way. This would allow a structured export that, for example, a support tool could also make use of.

The processes that are used by, for example, DefCERT can be seen as a proprietary implementation of the processes as described in [NIST SP 800-61], a guide for CSIRTs. Therefore we used NIST as a top-layer to describe the CSIRT processes.

In a CSIRT there are at least three processes that need to be controlled: the cyber-incident itself (problems need to be fixed), the management of the incident (is everything under control yet?) and the communication with the client (including upper management). This chapter focusses on the processes related to the cyber-incident itself. They will need to be refined once work on an actual support tool prototype will be done. The other processes, that are also relevant, can be described later.

CSIRT-incident response teams are faced with the need to constantly remain adaptive (‘sustained adaptability’) while at the same time they need to automate as many of their incident management procedures as possible (including information management), given the time pressure, dynamic situation and volume of data involved. A knowledge of the processes involved is a first step towards being able to assist with this issue.

3.1 Architecture

The NATO Architecture Framework (NAF) provides guidance for developing and describing NATO architectures. It has specific pre-defined ways, so-called views, to describe processes, systems, information and interactions (information exchanges), organisation, services, capabilities, et cetera. More importantly, NAF allows a structured way to indicate the relations among these views. This is important because without a structured approach is (too) easy to lose track of these interrelations. The fact that a lot of thought has already been given to the development of NAF means that we don't have to think about this again. The use of a tool such as [IBM RSA] helps to assure consistency among the different views. It also helps to collect and organise reference material for the entities that are described in the views. Each entity in a NAF view contains a descriptive text.

NAF's pre-defined views to describe processes, systems, information and interactions (information exchanges), organisation, et cetera are basically different views of the same system (in which *system* = *people* + *machines*). As an example, Figure 3.1 shows an example of two views of the same object (a house).
The intended occupant is interested in how it looks, the environment, et cetera. The company that builds the house is interested in the precise building plans, the consistency of the soil, availability of utilities, et cetera. Both views pertain to the same object. When something is changed in one view, it will have an impact on another view. NAF provides a way to keep these views consistent.

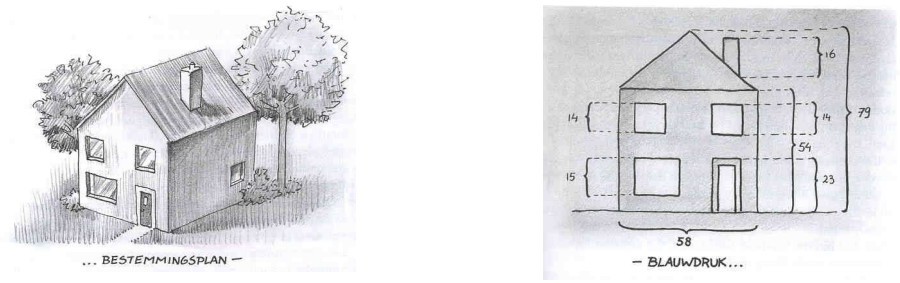

Figure 3.1 Different views on the same object.

A well-defined architecture helps to focus on what is important and it helps to provide information on the right level of detail. It helps to answer questions such as:

- Which systems are involved?
- What information exchanges are involved?
- Who (persons / roles) are working in or with this system?
- What are these people actually doing and with whom do they work together?
- Where in the organization are these activities being done (nodes)?

NAF provides fundamental linkages among the three upper-level views that are most effective to be used in this project, as shown in Figure 3.2. Each upper-level view consists of several sub-views. Note that not all views should be used, just those that are relevant.

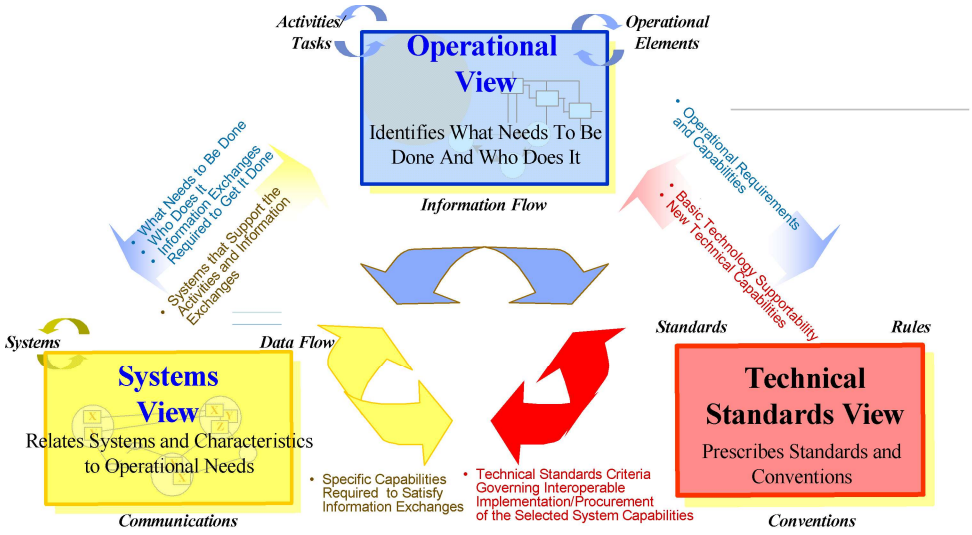

Figure 3.2 Fundamental linkages among NAF upper-level views.

3.2 Organisational view

As a first step it is good to know what part(s) of the organisation we are focussing on, and what the relationships with surrounding entities are. Figure 3.3 shows such a view.

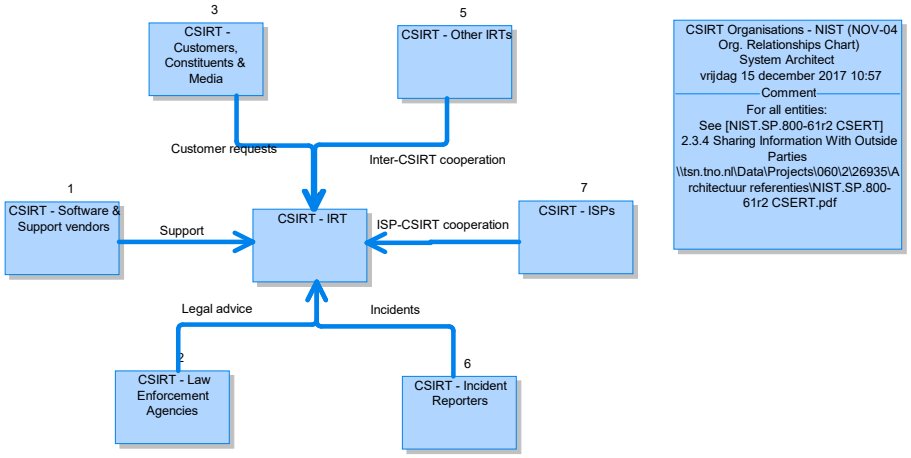

Figure 3.3 CSIRT and related organisations.

3.3 Role view

It is very useful to know who is involved in what role. An example of a view that depicts relevant roles is shown in Figure 3.4.

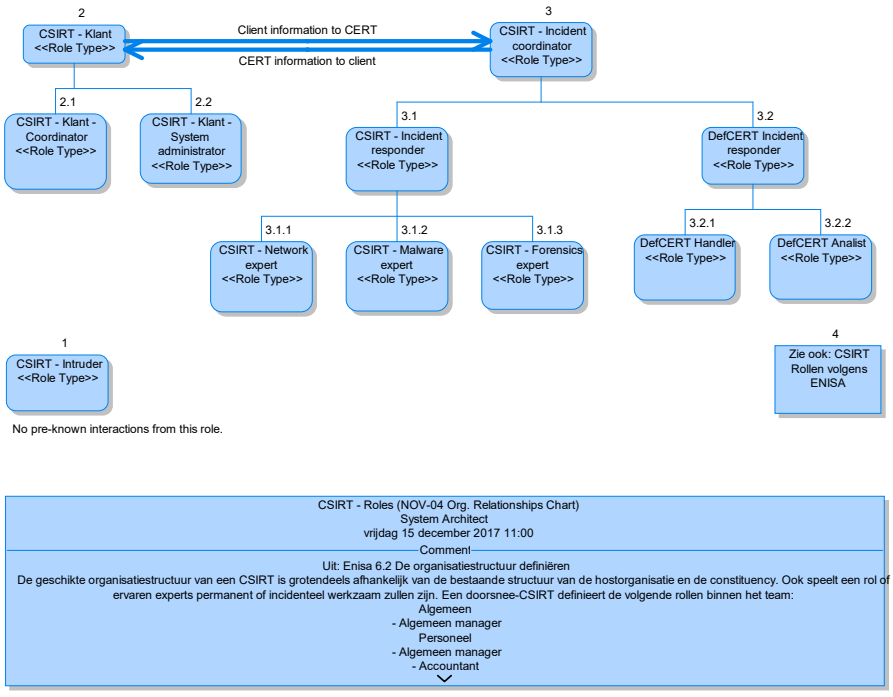

Figure 3.4 Role view of CSIRT and external roles.

Note that different implementations of CSIRTs would be described by a (slightly) different diagram. For example, DefCERT has implemented two specific sub-roles for the incident responder: the Handler and the Analist.

3.4 Process view

The process view is structured in layers. Each higher-level process can be decomposed in a set of sub-processes. This is done until the required level is reached. This is the level that is, in our approach, relevant for the to be developed support tool (see also Chapter 5). The four main CSIRT processes are depicted in Figure 3.5. We focussed on the Detection & Analysis process because this is a process that is very dynamic. It often involves events that the team must respond to in real-time. These events may cause, for example, work overload and a misaligned situational awareness. Tools might very well be used to alleviate these circumstances.

Note that the arrows in the process diagrams depict information flows. They do specifically not depict any temporal or activation relationship among processes (i.e. that one process precedes another process). All processes can be active at any time. The activation of the process in time can be illustrated in another type of diagram.

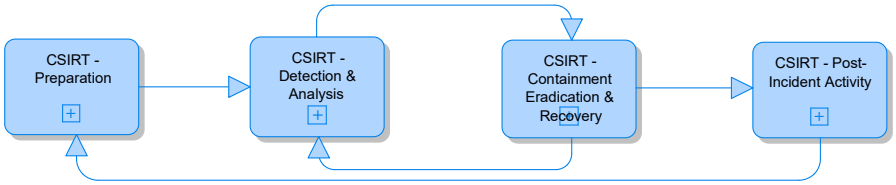

Figure 3.5 Main CSIRT processes.

The Detection & Analysis process is divided in several sub-processes, as shown in Figure 3.6.

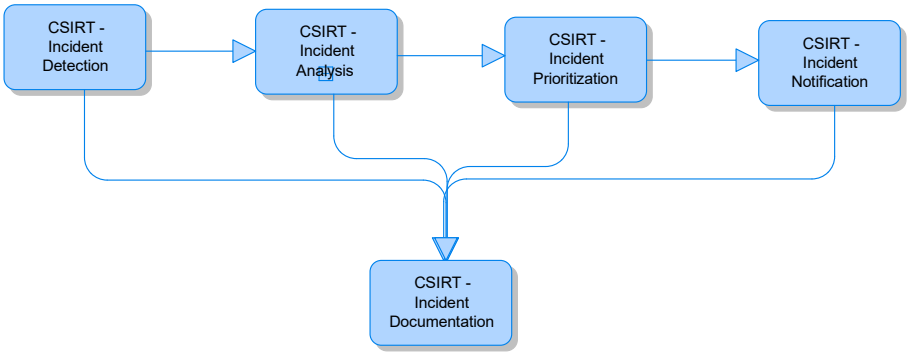

Figure 3.6 Sub-processes of the Detection & Analysis process.

3.5 Connecting processes to decision support: Profiles

Decision support itself can be seen as an entity that has a role related to the team. The roles, activities and information needs of the Incident Response Team (IRT), consisting of handlers and analysts, of the Team manager and of the decision support partly overlap each other.

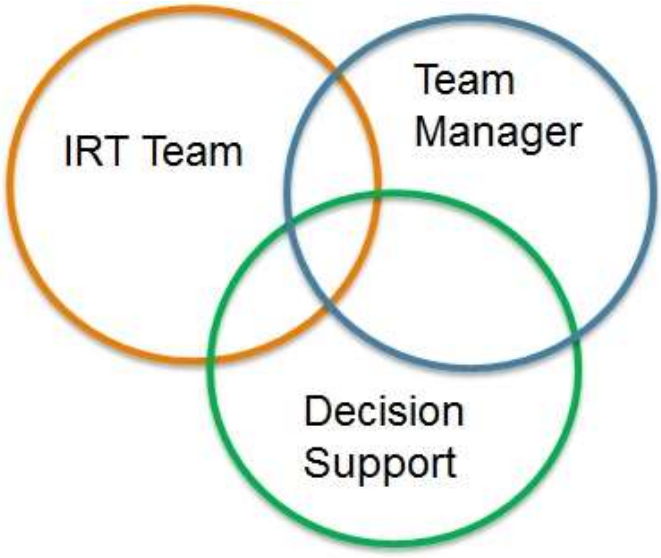

Figure 3.7 Overlapping roles of Team, Manager and decision support.

In the above case, the support needs to know what the IRT members and the Manager are doing. This is indicated by the parts that overlap with the decision support. Processes and information needs that are related to these roles but that are outside of the overlapping circle, need not be taken into account. This is a way to focus on the interesting aspects and to simplify the information that the decision support needs to handle as much as possible.

If we complete the architecture views to the required level, we will have information on the following:

- Processes in the CSIRT.
- Roles (people) and systems that perform the processes.
- The information that is exchanged by the roles and systems while performing the processes (information need).
- How people work in different processes, using different types of information and work with different systems for different purposes in different roles, sometimes in different (parts of) one (or more) organization(s) together.

For a specific task (for example a specific type of incident analysis) a combination of roles, systems, processes, information organization, et cetera can be identified. For each role, a profile that describes the relevant parts of the above systems, processes, information, organization, et cetera can be defined. Such a profile can be simple at first and could later be elaborated as necessary.

The following ideas could be experimented with. When a set of profiles is known to the decision support, it could identify what task(s) a persons is currently involved in. It could then use the profile for the following:

- Detect work or information overload, based on deviations of the expected mix of activities and information exchanges, as described by the profile.
- Provide tips for the redistribution of tasks among similar roles.
- Detect when roles are performing similar tasks and provide tips for them to work together more closely.
- Draw the attention of a role to something interesting that is happening.
- Provide input to systems to adapt the level of detail and the way that information is provided to a role.
- Generate tips for the division of tasks between man and machine. For example, in case of overload more work could be delegated from persons to (automated) systems. This might provide less accurate results for the tasks that are delegated to automated systems, but it will prevent information and / or work overload, thereby improving overall team performance.

4 Collaborative Sensemaking

4.1 Approach

In this chapter we will describe how the concept of 'collaborative sensemaking' can be applied to identify and develop support for CSIRTs. To achieve this goal we started with a short literature search on collaborative sensemaking. Based on literature we identified requirements and ideas for support of CSIRTs in their 'collaborative sensemaking' processes. Some of the ideas are based on interventions that were described in these articles.

In addition we focused on gaining insight into the working process of CSIRTs. This would enable us to identify the moments in which support was especially important. We collaborated with the team members who worked on the needs assessment (see Chapter 2) and on the process description of cyber incident management (see Chapter 3). And we developed a questionnaire to gain a better understanding of the team work of CSIRT and their process of sensemaking. We asked project members who were able to observe during a CSIRT team exercise (see Chapter 6) to consult the CSIRT team members using the questions of our questionnaire. Based on findings in the literature the on the one hand and knowledge gained of the CSIRT team process the other hand, we formulated design recommendations and ideas for support.

4.2 Needs of CSIRTs

From the first step in this research project, the needs assessment (see Chapter 2), it was concluded that one important need for CSIRTS is to improve their capacity to assess an incident in terms of the extent of the problem and the seriousness of the possible consequences. Figure 4.1 below shows the incident process (see also Figure 3.5). The figure shows that the step 'detection & analysis' is one of the necessary steps for CSIRTS in order to work with incidents. In this research project we take this 'detection & analysis' step as a starting point for improving the capacity of the CSIRTS to resolve incidents. For if this step is improved, i.e. more effectively or more efficiently executed, the subsequent steps can be executed better as well. The first argument is that if the CSIRT team detects incidents in an early stage, it will be better able to contain the impact of the incident. The second argument is that if the CSIRT team has a good understanding of what the incident is, than it can take appropriate measures. In all, our assumption is that improving the 'detection & analysis' step improves the whole CSIRT process.

Figure 4.1 Main CSIRT processes (see also Figure 3.5).

The step ‘Detection & Analysis’ merely consists of what can be referred to as *sensemaking*. *Sensemaking is conceptualized as the ongoing process by which people identify problems, construct meanings and develop explanations* (Weick, 1995). Sensemaking is a process that has been studied extensively and is still of interest for many researchers. How do people ‘make sense of something’?
We assume that we can derive lessons from the literature about sensemaking for CSIRTs to apply and improve their incident process.

Sensemaking is not the same as decision making. Where decision making addresses ‘what shall we do?’, sensemaking addresses ‘what is going on?’ (Landgren 2005, McMaster et al. 2012, p.2). In this context it can be translated into ‘is an incident going on?’ (detection) and if so, ‘what kind of incident is it?’ (analysis). The next section will describe in more detail what collaborative sensemaking is and what we can learn from previous research in this field.

4.3 Collaborative sensemaking

In Table 4.1 at the end of this section we provide an overview of different definitions and descriptions of (collaborative) sensemaking. We also describe two models of sensemaking in more detail in this section.

Klein, Moon and Hoffman (2006) have developed the data/frame model of sensemaking, see Figure 4.2 below. In this model, frames take the form of a retrospective narrative account, based on expertise and experience – and are used to organise data and anticipate future events (Pirolli and Card, 2005). Frames are a kind of hypotheses of what the world looks like. For Klein et al. (2006) the process of sensemaking involves the recognition and fitting of data into an appropriate frame, which then guides further data collection and influences the filtering of data viewed as relevant to the situation. These processes of frame construction and modification, and frame-defined data collection are thought to occur in parallel (Klein et al., 2006).

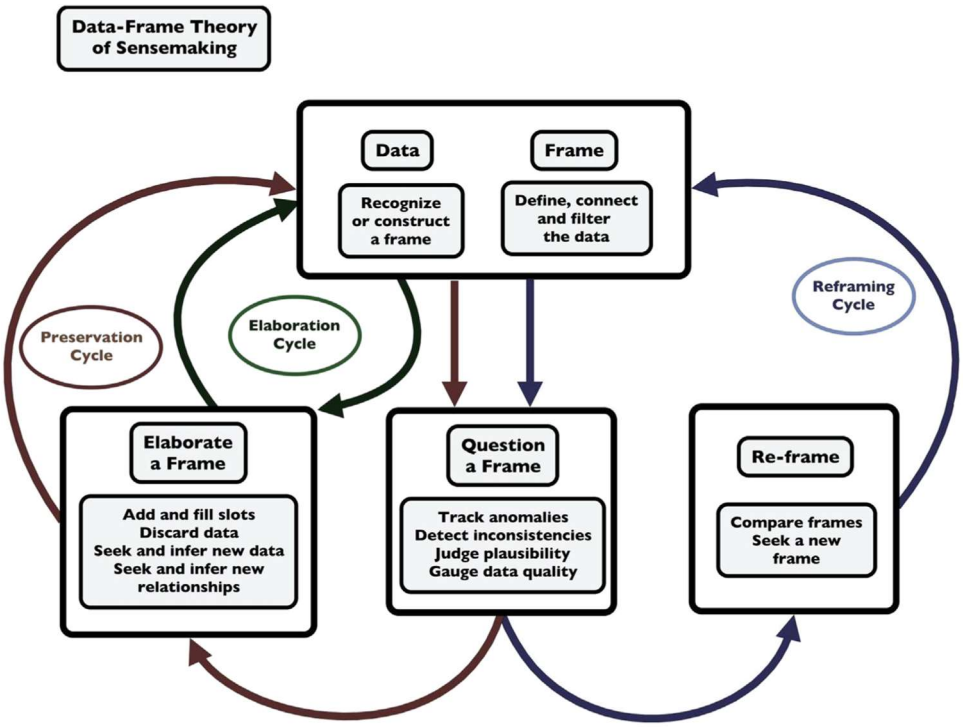

Figure 4.2 Date / frame model of sensemaking (Klein, Moon and Hoffman, 2006).

Another model of sensemaking is the notional model of sensemaking loop for intelligence analysis derived from Cognitive Task Analysis (CTA) by Pirolli and Card (2005). See Figure 4.3 for an overview of their model. The authors describe their model as a (…) “broad brush characterization of the whole process we have seen across several all-source analysts”. In the figure the rectangular boxes describe an approximate *data flow*, whereas the circles represent a *process flow*.
Processes and data are arranged by degree of effort (x-axis) and degree of information structure (y-axis). The figure depicts a process with lots of back loops, with two main sets of activities: one around finding information and the other around making sense of the information, with plenty of interaction between these two sets. The first loop is referred to as the *foraging loop* that involves processes aimed at seeking information, searching and filtering it, and reading and extracting information (Pirolli & Card, 1999) possibly into some schema. The second loop is referred to as the *sensemaking loop* (Russell, Stefik, Pirolli, & Card, 1993).
This sensemaking loop involves iterative development of a mental model (a conceptualization) from the schema that best fits the evidence.

Information processing as depicted in the figure can be driven by bottom-up processes (from data to theory) or top-down (from theory to data). The authors add that the outcomes from their task analysis suggest that top-down and bottom-up processes are invoked in an opportunistic mix.

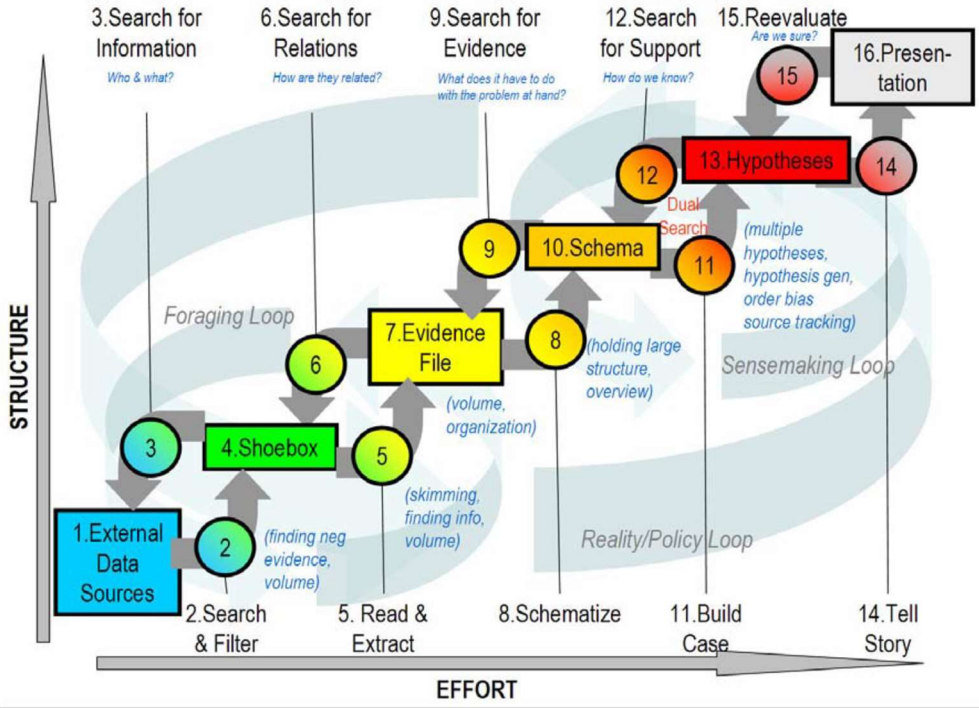

Figure 4.3. Notional model of sensemaking loop for intelligence analysis derived from Cognitive Task Analysis (CTA) by Pirolli and Card (2005).

Thus, sensemaking is the individual process CSIRT members typically are in when being confronted with an incident. Better said, when they are confronted with 'deviant system behaviour' – which might not even indicate an incident (yet). They have to find answers to questions like 'is this deviant system behaviour the consequence of an attack or an error in the software?' 'Is the IT-network suffering from a direct attack or has someone accidentally downloaded a virus?'

When the process of sensemaking is performed in a team, it is called *collaborative sensemaking*. It involves a *group of people with different worldviews* collectively engaging in making sense of chaotic and ambiguous situations (Ntuen, et al. (2006) in Umapathy, 2010). For collective sensemaking to emerge, interaction must necessarily take place between individuals. When discussing a situation, each individual expresses the sense he makes of it (Fayad, 2010).

The advantage of collaborative sensemaking, compared to individual sensemaking, is that different perspectives can be taken into account. This will support the detection and analysis process, because more different causes will be considered and discussed. A challenge in this context is to make the individual sensemaking process, which is often very intuitive and implicit, explicit to other team members. Another challenge is to deal with biases, that occur both on an individual level as well as on a team level. We explain a few biases below, the confirmation bias, overconfidence and group think.

Confirmation bias is the tendency of people to search for, interpret, favour, and recall information in a way that confirms one's pre-existing beliefs or hypotheses (Plous & Scott, 1993, p. 233). People often test hypotheses only by searching for evidence to confirm their hypotheses, rather than to falsify their hypotheses.

In addition, individuals, especially experts, are often overconfident about the accuracy of their decisions (Russo & Schoemaker, 1992 in: Schrader et al. 2016). In other words, they think they make better decisions than they actually do. This is referred to as the overconfidence bias. Lastly, group members have the tendency to reach consensus without critical evaluation of alternative ideas of viewpoints (Turner & Pratkanis, 1998). This is called groupthink.

The better these biases are overcome, the better the sensemaking process is. There are several techniques available to overcome cognitive biases. One way to support this is by applying critical thinking as indicated by Tetrick et al. (2016). Critical thinking is an important decision making skill and can be used to come up with alternative hypothesis for a problem. Tetrick et al (2016) highlight critical thinking as one of the most important decision-making skill for CSIRT analysts and managers. Critical thinking supports taking more rational steps, instead of reacting intuitively. Another technique is the 'five why analysis' (Ono, 1988). It is a strategy where team members ask themselves the question 'Why?' five times. This strategy is effective in discovering the core of a problem. The strategy is more effective when used in teams, because an individual might not be able to generate alternative hypotheses. A last strategy we would like to mention here is Premortem (Klein, 2007). In this strategy, team members imagine that they have failed to solve a problem and identify reasons for this.

Table 4.1. Definitions of sensemaking.

Authors/ article	**Definition of sensemaking**
Weick, 1995	Sensemaking is an ongoing process through which meaning is constructed and explanations developed in an effort to establish what is going on.
Gioia and Chittipeddi, 1991 (In: Fayad (2010))	Sensemaking relates to meaning construction and reconstruction by the actors involved in developing an interpretative framework for understanding an experience.
Thomas, Clark and Gioia, 1993, p. 240 (uit: Fayad (2010))	It is the process of both cognition and action that involves "environmental scanning, interpretation and associated responses".
Landgren (2004) (In: McMaster, R., Baber, C., Duffy, T.)	Landgren describes sensemaking as the progressive clarification of a situation which involves an iterative process of 'committed interpretation', where an individual's behaviour (actions) influences further sensemaking (and further actions).
McMaster, R., Baber, C., Duffy, T.	(…) Treating external representations as frames moves beyond the purely 'in the head' view of sensemaking and towards one in which sensemaking is a technologically mediated activity (Attfield and Blandford, 2011).
Pirolli and Card, 2005. In: Pfaff, M.S	Sensemaking refers to searching and organizing source information to create new knowledge.
Paul and Reddy 2010. (In: Pfaff, M.S. p213)	Collaborative sensemaking is when teammates must collaborate to make sense of a situation.

4.4 Collaborative sensemaking within CSIRTS

Analysts are continuously monitoring diverse IT-networks and IT-systems.
They monitor and search for deviants from 'normal functioning'.
The moment an analyst identifies such a deviation, he has to determine whether or not an incident has occurred. When he marks the deviation as an incident, he either tries to mitigate for it himself or asks for back-up. In the last case, a CSIRT team is established. Depending on the assessment of the analyst a small or large CSIRT team will be established. As a result CSIRTs have a continuous lifecycle of up- and downscaling and of being established and being dissolved.

In this process several stages of sensemaking occur. First, the analyst assesses the seriousness of a deviation. In other words, he is continuously making sense of large amounts of data in order to identify deviations. Subsequently, he has to estimate whether the deviation indicates an incident and how large the incident is or might become. Based on the outcomes of his assessment colleagues may be called for. In this case, they form a team and are jointly responsible for solving the incident. This newly established CSIRT has to collaboratively make sense of the incident in order to be able to divide tasks and effectively and efficiently handle the incident. In order to be able to do this, adequate hand-over of the insights of the analyst is most helpful. Team members also often have to cooperate with other colleagues within their company or within the client company.

CSIRT teams thus often are ad hoc teams, with team members working at different locations and working under great time pressure. This makes the detection and analysis process, including collaborative sensemaking, even more complex. Currently, analysts nor CSIRT teams have tools that support this process.

4.5 Supporting Collaborative sensemaking

Based on the insights presented in this chapter we think CSIRTs can best be supported with tools that both support sensemaking and support interaction between team members (see also Umapathy (2010)). For, only when both activities are supported, *collaborative sensemaking* is supported.

A supporting tool may support *sensemaking* by supporting the techniques we described above, i.e. critical thinking, pre-mortem, 5-why. So the tool could ask critical questions, or motivate team members to search for information that would contradict their hypothesis. The tool may support *interaction* members by supporting the sharing of their 'frames'. These frames could consist of their ideas about what the cause for the incident may be, their ideas about best ways of solving it, et cetera.

Some of the articles about (collaborative) sensemaking, also provide suggestions for how to support sensemaking or what is important when supporting sensemaking. In Table 4.2 we provide an overview.

Table 4.2 Suggestions for the support of collaborative sensemaking.

Authors	**What to support/ how to support sensemaking**
Fayad, F.	- To make sense of experience it is necessary to step out of it, observe it. - Interaction must take place.
McMaster, R., Baber, C., Duffy, T.	- Support social interaction
McMaster, R., Baber, C., Duffy, T.	- Make a distinction between formal and informal artefacts to support sensemaking.
Pfaff, M.S	- Draw attention to what is not yet done. - Facilitate discussion about data.
Umapathy, K.	- Make a distinction between support for individual sensemaking and collaborative sensemaking - Use templates to describe a problem. - This article provides a detailed description of requirements for collaborative sensemaking
Tetrick et al. Chapter 4	- Reduce overconfidence and confirmation bias. - Support critical thinking skills (e.g. using Five why analysis (Ono, 1988); Premortem (Klein 2007)

Here, we will describe the suggestions of Umapathy (2010) in more detail, as his paper provides explicit suggestions for supporting collaborative sensemaking.
As indicated above Umapathy (2010) makes a distinction in supporting 1) sensemaking and 2) supporting interaction between team members for his suggestions for support for collaborative sensemaking. In all he suggests the following requirements:

1 support for creating explicit representations,
2 support co-existence of different representations,
3 support for developing shared representation,
4 support for creating representations using templates,
5 providing workspace for developing shared representations,
6 support for building consensus and reaching agreement,
7 support for facilitating and moderating interactions,
8 support for exchanging documents,
9 support for retrieving and visualizing information.

Concerning 1) sensemaking the tool should:

- Support exploring different hypotheses and visual representations.
- Support critical thinking and prevent biases.

The tool should support creating (conceptual) representations of the problem.
In emergency management, for example, it is quite common to draw the impact and (expected) development of the crisis on a map, e.g. a large fire.

Sensemaking is typically a process of having different hypotheses of ‘what is going on’ in mind, until the assessment has completed. In order to prevent tunnel vision a supporting system could support by having these hypotheses continuously available.

Concerning 2) the interaction between team members the tool should:

- Support team awareness; knowledge of the different team members involved and their expertise, and how busy they are.
- Suggest moments to have interaction with other team members.
- Create a space where team members can come together as virtual team, when a face-to-face meeting is not possible.
- Support the sharing of different perspectives.
- Support the collection of different perspectives.

If the system is useful to create representation of this problem, it could also support developing a shared representation. Team members collectively can work on a representation of the problem and by doing that experience and discuss their different perspectives.

In the following chapter, the concept which we called ‘the reporter’ will be described.

5 The Reporter

This chapter describes The Reporter. The development of The Reporter was based on a human-centred design process (International Organization for Standardization, 2010). The reporter provides the decision support functionality, as mentioned in Chapter 3. This iterative process consists of different phases, as shown in Figure 5.1, and was guided by the mission statement to “develop a digital assistant that provides teams with process support during incident analysis.” The four iterative phases are:

- Understanding and specifying the context of use.
- Specifying the user requirements.
- Producing design solutions.
- Evaluating the designs.

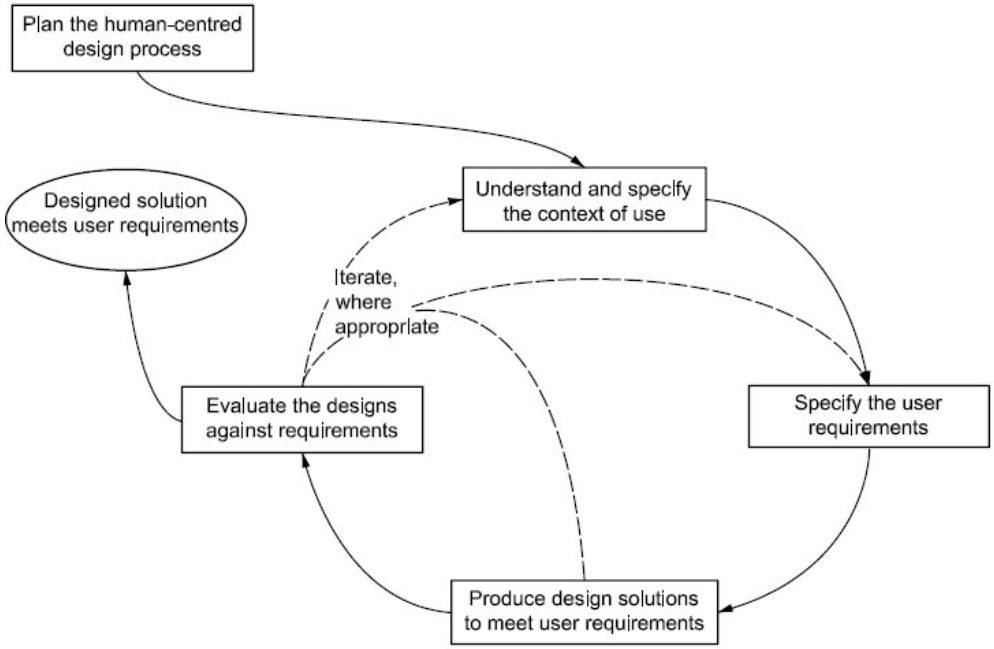

Figure 5.1 An overview of the different steps in a human-centred design process.

The first phase consisted of different research activities to explore and describe the context of CSIRTs. These activities have been discussed in Chapters 2, 3 and 4 and will therefore not be discussed here.

The following sections will describe the three other phases of the human-centred design process. These phases were followed in an iterative manner. For instance, during the “Produce design solutions” phase, the artefacts that were developed served to evaluate the different ideas and concepts for solutions, but their development also raised new questions which served as input for the research activities. Therefore, the results of the phases are not described in a strictly chronological order.

5.1 Specifying the user and organizational requirements

This phase focuses on “identifying user needs and specifying the functional and other requirements for the product or system” (International Organization for Standardization, 2010). As described in the previous chapters, the research activities undertaken during this project resulted in insight into the tasks, context and challenges of CSIRTs, as well as promising directions for a digital assistant to aid collaborative sensemaking among such teams. Several requirements for an assistant followed from these research activities, namely:

- The assistant can see, hear, recognize voices and understand spoken commands.
- The assistant can talk to team members, ask questions and give assignments.
- The assistant knows how tasks are distributed and who is working on them.
- The assistant is ‘human-aware’, that is, it can determine the mental condition of team members and can (re)distribute tasks based on that assessment.
- The assistant can support sensemaking, both technically and procedurally.
- The assistant can share information within the team, but also communicate progress with managers and other stakeholders.
- Assistants are interconnected via a network connection, supporting the team in distributed working.

To provide a list of these specifications for discussion, a poster was made to describe The Reporter (shown in Figure 5.3). This poster went through several versions and internal validation with the project team to identify the most promising features.

Figure 5.3 The Reporter poster, listing its intended features.

Ideation activities took place with a small group of experts to explore potential tools to aid the sensemaking process. After several ideation sessions, the work focused on converging on a single concept. One of the conclusions was that although we identified many challenges for CSIRT teams, we had not yet learned which ideas were the most promising or which challenges had the highest priority. Therefore the decision was made to develop a concept that could combine aspects of the other ideas. This way, evaluation could take place with CSIRT members and other professionals in the field of cybersecurity to compare and prioritise the possible directions.

5.2 Producing design solutions

During this phase, different concepts were developed and prototypes were built. The aim was to diverge into many possible directions and then, based on evaluation, converge on a single concept.

The first prototype that was designed was a static demonstrator to illustrate the concept of a digital assistant for CSIRTs. A physical camera was used as a prop to pitch and evaluate this idea within the project team and several senior programme board members. The pitch was accompanied by a storyboard and wireframes (shown in Figure 5.2) which illustrated a number of possible functions of The Reporter as well as its context of use.

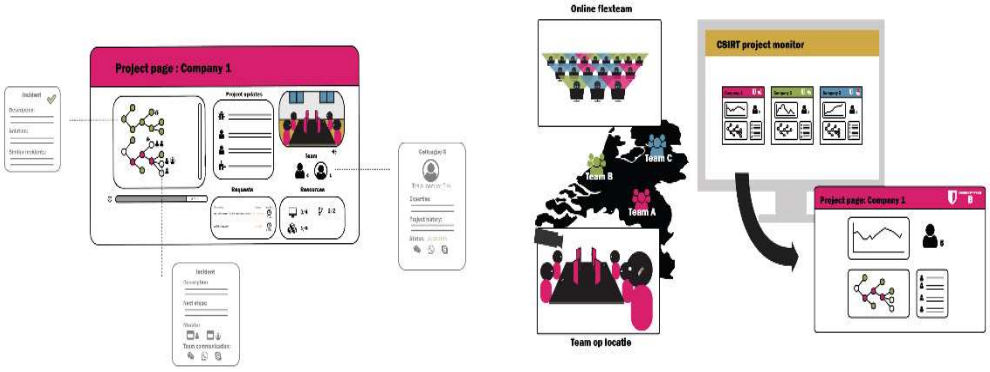

Figure 5.2 Wireframes to illustrate features of The Reporter.

In a following iteration, a Wizard-of-Oz style prototype was developed. The goals of this second prototype were to:

- Showcase the possible features of The Reporter and how these could aid CSIRTs.
- Illustrate the concept for potentially interested parties.
- Draw interest and raise enthusiasm among professionals.
- Invite feedback on the Reporter as a concept and on its different features.

To draw interest, we wanted the prototype to physically move around and to visualize the functions in an attractive way. However, to invite feedback, we accepted a rough prototype look as opposed to building a high quality product which would look finished.

The prototype, shown in Figure 5.4, consisted of a small frame that could be placed onto a table. Onto this frame, a small camera and a tablet computer were fixed. The camera was mounted on top of a flexible neck, which was able to move around randomly, thereby giving the illusion of an observing agent.

Figure 5.4 The third iteration of the Reporter prototype.

The tablet computer showed abstract visualisations which represented the different possible features of the Reporter. A number of these visualisations are collected in Figure 5.5.

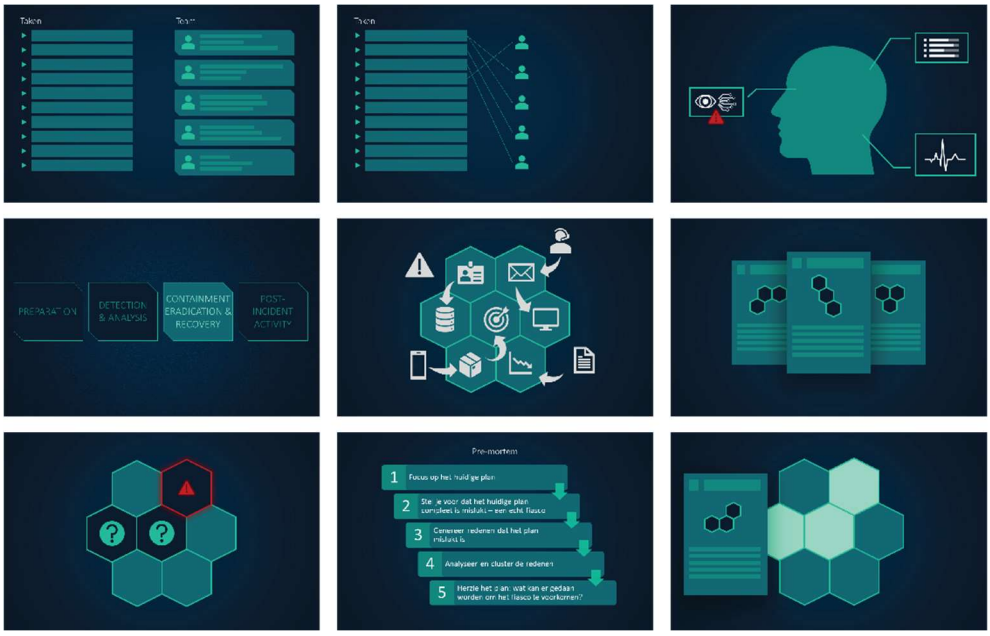

Figure 5.5 Visualisations of the different features of the Reporter, as shown on the tablet fixed to the prototype.

The visualizations were designed to illustrate the following features (from left to right, top to bottom), respectively:

- Overview of the CSIRT members and a backlog of team tasks & incidents and members assigned to these tasks.
- Matching of team members to tasks based on expertise.
- Human awareness through physiological measurements (e.g., team members wearing devices on their body measuring cognitive state, such as work load).
- Overview of the phases in incident response.
- Overview of the incident (Common Operational Picture).
- The working hypothesis about the incident and the situation at hand, as well as alternative hypotheses.
- Known unknows or other inconsistencies between the working hypothesis and available evidence.
- Conversational techniques to aid the sense-making process, in this case the pre-mortem technique (see also Chapter 4).
- Mapping available evidence on the incident onto the working hypothesis.

5.3 Evaluating the design

Evaluation of the different iterations serves to “obtain a better understanding of user needs” (International Organization for Standardization, 2010). The goals are to “collect new information about user needs”, and to “provide feedback on strengths and weaknesses of the design solution from the user’s perspective”.

While the first iterations were evaluated within the project team, the final prototype was designed to gather feedback from professionals in the field of cybersecurity. To this end, the prototype was presented to cyber security professionals during a conference session. About twenty professionals were present during this session. In the first part of this session, the prototype was presented. The second part consisted of three breakout sessions in which several parts of the reporter were discussed with the audience (see also Chapter 7).

An important lessons learned is that the audience was of the opinion that the assistant should take on a digital form, since CSIRTs often work in a distributed fashion. A digital agent also has the advantage that it is more easily integrated and matched with current systems, processes and software used over several organisations. Thereby better supporting the multi-team ways of working of CSIRTs.

6 Field experiences

This chapter presents the results of interviews with CSIRT members and describes observations during an exercise that was conducted in the project. The exercise concerned the response by a CSIRT to a cyber incident. These observational opportunities allowed us to 1) assess the validity of our conclusions from the needs analysis and 2) provide an indication of how the Reporter's functionalities may meet the needs experienced by CSIRTs.

6.1 Interviews

We conducted several interviews with personnel at DefCERT (Defensie Computer Emergency Response Team). We interviewed three individuals, each performing one of the three roles that constitute a DefCERT team. Note that the team can, and usually does, have multiple instances of each role. The roles are: handler, analyst and coordinator.

An overview of the main (non-classified) results of the interviews is presented below. These are based on First impression report (FIR) van Cognitive Task Analysis (CTA) DefCERT, which is itself based on the interview information, as recorded and interpreted.

6.1.1 Things that are working well

- There are several opportunities for coordinating meetings, such as triage meetings among analysts and handlers, a weekly incident review meeting and daily and weekly end-of-shift briefings. The end-of-shift briefings (by the handlers) discuss, among other things, extraordinary events that have occurred, new threat developments, et cetera. This helps to focus threat hunting.
- There are short and direct lines of communication between individuals, both within the team and with others outside of the team (horizontal communication). The other teams include for example the SIOC, public parties such as NCSC and private parties. This constitutes an (informal) network.
- There are experienced incident coordinators, who have their own well-developed network both within in the organisation as well as outside of the organisation. They help to prevent tunnel vision and bias.

6.1.2 What could be improved

- Scaling up of an incident to the level of a triage, as well as the decision to organize a meeting, at least partly depends on the responsible individual. This introduces a chance for personal bias. As an example, a person lower in rank may have difficulty "going against" the decision of an individual higher in rank. This also relates to the risk of what is called the emergence of a " tribal" culture.
- There is a "grey area" when determining whether an event actually is an incident. This is caused by different personalities and experience.
- The lessons learned from solved incidents are not retained well enough. How do we learn from how an incident was tackled before? How do we remember the solutions? This knowledge would help solve similar future incidents. Moreover, it is not clear how the results of hunts that do not provide an executable advice are being secured. This makes it more difficult to prevent other colleagues from unnecessary re-investigating.

- The chat-app that is used to facilitate shared awareness assumes initiation and active input by the team members. This is a weakness because, at times when SA needs to be best, the team members are busiest and therefore may not pay enough attention to the chat-app.

6.1.3 Research questions

We derived a set of research questions based on our observations and interviews. The impact of the research questions on the focus of this report is indicated in a bulleted list, which can be found in Appendix 1, as it falls outside the main scope of this project.

6.2 Exercise

The exercise Cyber Coalition 2017 (CC17) is a NATO and NLD MoD-wide cyber exercise, in which DefCERT (Defensie Computer Emergency Response Team) takes part. TNO was allowed to be present as an observer. During the exercise, DefCERT experienced several cyber incidents, to which the DefCERT analysts, handlers and incident coordinators had to respond. Two local trainers were available during the exercise, who also acted as the TNO points-of-contact.

6.2.1 Consolidated observations

After the exercise, the observations by the TNO team were discussed with the DefCERT exercise lead. This resulted in the following consolidated (mutually agreed upon) observations, which DefCERT allowed TNO to use in the current and future projects. The impact of these observations on the focus of this report is indicated by a "→" for each observation. The arrow refers to the table "Overview of needs and wants of Incident Response Teams" in Section 2.1.

1 There was not enough communication / coordination between DefCERT and DCC (Defence Cyber Command). Because conclusions and other results were insufficiently shared, personnel at DefCERT did not have a sufficient situation awareness (SA). In the course of a day, personnel did not know anymore what information was not available, or what information was available but just not shared.
   → Organization needs: Coordination and sharing information with outside parties and shared incident awareness.
   → Team performance needs: All items.
   → Instrumental needs: Need for better interpersonal communication tools, especially during larger incidents and creation of useful (visual) overviews at any particular point in time for a different audience (e.g., customer, management, colleagues).
2 The SA and incident context is only limitedly transferred to the analysts that need to work on the incident. This causes a lack of focus in the investigation by the analyst.
   → See impacts regarding item 1) above.
3 The first days of the exercise, the SA team mainly provided a representation of "the world" as it was interpreted by the SA team. This should be a more commonly-supported and created SA. This could be facilitated by allowing the analysts to reason about the possible scenarios.
   → See impacts at item 1) above.

4 Information is available from / in several different tools (whiteboard; excel; et cetera) and with different individuals. For now, there is no overview of what (parts of) SA information is available from what sources: there is no SA on SA information. This could be improved by the use of the same toolset, that can present the same information from different perspectives for different purposes. This could be done based on time, event-correlation or established event relationships, et cetera.
   → Instrumental needs: Creation of useful (visual) overviews at any particular point in time for a different audience (e.g., customer, management, colleagues).
5 The incident Coordinator performs a very important role. Still, this role is allocated to just one individual who acts on different levels. This creates a risk for DefCERT, which could be mitigated by distributing this role over several individuals or by allocating a backup-coordinator, in case the primary coordinator is not available for the team.
   → Team performance needs: Information sharing and decision making across personnel shifts & handoffs.
6 The cooperation with companies can be improved. These companies can provide much knowledge, information and experience that should be utilized fully.
   → Organization needs: Coordination and sharing information with outside parties.
7 There is no overview of the DefCERT information need. Several different team members request information from several different parties. It would be very useful if there were a centrally provided overview of what questions were asked by whom, and when, to which party.
   → Organization needs: Collaborative problem-solving capacity & shared incident awareness.
   → Team performance needs: Keeping everybody informed & staying informed, especially when working distributed.
   → Instrumental needs: Creating useful (visual) overviews at any particular point in time.

6.2.2 Analyst support tool

This is a first idea for a tool to support the team with information gathering and processing, mainly at the analyst level but also at the handler level. It is based on observations and discussion with personnel. It may be incomplete in some areas and/or too all-encompassing in other areas. Note this is a different type of tool than the Reporter. Ideally, an Analyst support tool and the Reporter could and should be linked, so that the Reporter can for instance incorporate knowledge of what individual team members are doing and what information they need.

The Analyst support tool would:

- Offer a complete and structured Situational Awareness representation.
- Provide the capability to zoom in, focus on nodes, retrieve more detailed information on any item.
- Be built on top of a database.
- Allow concurrent multi-user cooperation from different teams / locations.
- Keep track of who added what information, in what capacity, from what sources, with what reliability. Allow users to see this tracking information.
- Provide a timeline:

  - Show the track of (consecutive and parallel) events and show the interrelations among events.
  - Show when information became available.
  - Identify / correlate simultaneous and / or related events.
- Allow information with different classification levels to be used in the same system.
  ➔ This is a general military problem. NATO and NLD MoD do currently not allow mixing information with different classification levels in a single system.

6.3 Conclusions

The validity of our conclusions from the needs assessment (Section 2.1) is indicated in the previous section. Support was found for many needs.
The observations did not provide any counter-evidence for identified needs.

In this phase of research, it is difficult to actually determine a quantifiable degree to which the Reporter's functionalities could meet the needs that are experienced by CSIRTs. In general we could say that the more pressing the need, the more valuable a contribution of a functionality of the reporter would be. In the area of sensemaking the reporter tool would support exploring different hypotheses and visual representations, support critical thinking and prevent biases, and support creating conceptual representations of a problem. In the area of team functioning among (possibly physically distributed) team members the tool would support team awareness, suggest moments to have interactions, create a space where team members can come together as virtual team and support the sharing and collection of different perspectives. These functionalities would certainly contribute to alleviating the issues that were found from the observations.

7 Final workshop

The final event of the ERP Human Enhancement was held on November 16, 2017 in Bussum, The Netherlands and was titled *The Human Factor – Human and technology in balance.* Within this overall event, we organised a final workshop on this project in particular, which addressed three different goals:

1 To present the generated insights and results of the project.
2 To gather feedback on these insights and results for further development of the Reporter concept.
3 To address possible follow-ups with external partners.

The outcomes of the workshop are briefly addressed in this chapter. Section 7.1 addresses the organization and structure of the workshop. Section 7.2 describes the feedback gathered during the final workshop. Section 7.3 addresses the results in terms of follow-ups with visitors of the final workshop.

7.1 Structure of the final workshop

The final workshop was organized according to three main goals. In the first part of the session (about 45 min), insights and results were presented, followed by the second part of the session (about 45 min) with a demonstration of the Reporter concept and follow-up discussions. The follow-up discussions were organized around three different stands addressing specific topics of the Reporter concept: 1) the Reporter concept as a whole and the demonstrator; 2) the phases of the NIST process supported by the Reporter concept; and 3) future directions for further developments and interest of external partners in these future developments. For each stand a banner was designed to present the main topic of that stand.

7.2 Feedback on the Reporter and its different parts

During discussions after the presentation and demonstration of the Reporter concept we observed the final workshop was received with much interest and enthusiasm shown and expressed in:

- The number of people returning after the break (almost all external visitors).
- Many visitors showed interest and took home the scientific publication on the Reporter (i.e. Van der Kleij et al., 2017).
- The lively discussions at different stands, which progressed until after the planned session time.

Summarizing, we conclude that the interest in support for CSIRT teams is high, though the number of external visitors for this workshop was limited (five different organisations). The final workshop triggered many additional thoughts, ideas, perspectives and feedback on how to design the Reporter concept towards the future. The following sections briefly address these thoughts, ideas, perspectives and feedback.

7.2.1 Feedback on the Reporter concept(s)

What became most apparent after the presentations and demonstration of the Reporter concept was that there is first of all a clear need for better information awareness. Information awareness in this respect indicates information needs such as:

- Having at hand and available the information needed to perform one's immediate task (e.g. access to information, systems, people).
- Being able to identify and be aware of information relevant to one's task from other sources such as other team members (e.g. what are others working on, what is their progress or status (only when relevant or related to one's own task)).
- Having the correct tools supporting both information awareness and management of one's own work in relation to the work of others.

These needs apply to individual team members solving parts of the problem (e.g. the analysists) as well as team management. It was stated that developments in information awareness such as addressed above would be a good first step towards more efficiently working towards recovery after a cyber-attack. Secondary needs relate to automated team management such as process and progress management and collaborative sense-making. At the moment the preferred way of handling this is the human operator (e.g. team manager).

When further developing the Reporter concept the focus should be on multi-team support over several organisations and integration into or with systems that are already used by CSIRT teams. The Reporter demonstrator triggered discussions on the focus of support. Now, the reporter demonstrator mainly suggests individual support while support should be available for individuals spread out and working together over multiple organisations. These last thoughts tend towards a shared integrated system over multiple organisations with several different interfaces for individual team members. This also indicates a need for collaborative sense-making, though this was not explicitly identified by visitors as such.
Better information awareness during analysis, detection and recovery is at this moment the key issue.

7.2.2 Feedback on processes covered by the Reporter

Recalling Chapter 3, the different phases in the NIST cyber incident and recovery cycle are:

- Preparation.
- Detection and analysis.
- Containment, eradication and recovery.
- Post-incident activity.

The reporter concept covers and delivers support for the second and third phases: Detection & analysis, and Containment, eradication & recovery in the NIST cycle.

The preparation phase is already well covered in CSIRT organizations via several networks in which information is shared about threats, possible preparations to prevent and neutralize threats, etc. Much effort is already invested in the preparation phase to prevent and neutralize threats becoming incidents.
However, there is a need for support during especially analysis, containment, eradication and recovery during cyber incidents.

Efficiency in finding a solution and quickly working towards recovery is crucial in this phase, however very difficult due to lack of insights (the iceberg), and problem complexity that needs to be tackled in an often multi-team setting and with high time pressure. The other phases are characterized by less time pressure and a more structured approach. As we observed with the Reporter concept itself, having good and up-to-date insight in current information is essential in terms of what is already known, the solutions being worked on or explored, etc.

A second clear need related to processes supported by the Reporter is good insight into who is working on which tasks and how one's own work relates to the work performed by others in working towards a full recovery. At the moment this insight is difficult to obtain for both analysts and team managers. A dynamic profile that could provide this insight, based on the activities of an analyst is a good starting point to address this – for analysts and team managers. The proposed profiles in the Reporter (information needs, output to be delivered or delivered already, the systems used and being analysed, the current status of the work matched with a process, and needed or relevant communications/relations to the work of others) were positively received as interesting solutions. The main focus in making processes insightful should be on creating the needed insights/information. Once this is realized and has been proven to work, management could be transferred from human operators to the Reporter (e.g., process management), insight and discovering dependencies in tasks are however key at this moment.

Interesting future development should focus on creating a working profile that monitors current activities, provides better support during these activities (for an individual as well as the team) and monitors how different activities indicate a structure underlying the complete process to enable identification of overlapping or similar activities taking place. Step-by-step development of process support in this manner will also enhance adoption of solutions by organizations (i.e. an integrated system that is aligned with systems already in use).

7.2.3 Feedback on future developments

Developments in the area of Human Factors research for cybersecurity professionals in the future identified as most interesting by visitors either relate to better support for cybersecurity professionals or to eliminating the Human Factor as a weak point in cybersecurity incidents:

- Artificial intelligence and man-machine technologies in the digital domain were indicated as interesting areas of research that could provide better support for cybersecurity professionals. By providing better support for sense-making of what is happening, decision making at crucial moments and by eliminating a great deal of stress.
- Behavioural influencing and creating awareness were indicated as interesting research areas to limit and decrease the effects of the Human Factor being an interesting attack vector.

The most interesting practical applications of the Human Factor for cybersecurity professionals in the future focus according to the experts are:

- Tooling and support that apply during crucial moments and provide better insight for decision making and problem solving during the initial response (e.g. plan surprise counter attacks or block additional attacks and work towards recovery).

- Tooling and support that relieves the individual of stress and decreases time pressure through higher efficiency in dealing with the problem at hand. This kind of support is currently very limited.
- Tooling and support that make the human/user more aware and capable of identifying and therefore preventing cybersecurity attacks (e.g. anti-phishing tools that help identify and make people more aware of phishing mails).

With these future developments some additional requirements and concerns were voiced as well:

- Profiling and monitoring individuals does indicate a clear need for careful ethical considerations of solutions and support being developed and built if tools or support are to be adopted in practice by 'end-'users.
- For tooling and support to be commercially and practically viable, future developments and designs need to be built on and integrated with existing solutions (systems, processes and work/tasks). Developing tooling and support in several enhancements based on existing systems in that respect is very attractive but added 'functionality' should provide added value in each step.
- Support for cybersecurity professionals is very limited at the moment. Tooling and support provided to professionals in other crisis-teams in other domains might provide valuable references in dealing with and designing tooling and support for cybersecurity professionals.

7.3 Follow-up with workshop participants

All visitors indicated they want to be kept informed of future developments (e.g. future events in this area of interest and project continuation or follow-up).

A number of organisations, both public and private, indicated interest in discussing future developments on this topic and possibilities for different forms of future collaboration.

8 Conclusions and future directions

At the start of this project, the needs assessment identified various challenges to improving CSIRT performance. These boiled down to collaboration between and within teams on the one hand, and developing an understanding – that is, making sense of – the incident and the ensuing response on the other. These two challenges formed the basis for applying the concept of collaborative sensemaking and the subsequent development of The Reporter in order to better support CSIRT performance.

Many organisations both public and private wrestle with the challenges of how to support teams such that they can function optimally given the circumstances under which CSIRTs have to perform. Though CSIRTs acknowledge that not all work processes are as good as they would like, there is little awareness that non-technical processes can be supported and improved or how. In this sense, the work we have done in the present project can fulfil an important need and help resolve a pressing problem.

Making sensemaking explicit seems particularly new for CSIRTs, though CSIRTs have been doing this intrinsically all along. Interpreting the information to make sense of it – in other words, *sensemaking* – is not a self-evident concept, specifically when you add the collaborative element to the mix. In this project, we have considered the necessity of CSIRTs to not only improve their understanding of an incident, but to execute the process of creating a joint and shared understanding together as a team.

Finally, even in cases in which CSIRTs are consciously aware of the existence of non-technical problems there is little understanding of the possibilities for solving the problems on the one hand, and doing so by automating various processes on the other. That is to say by using technology and automation to support non-technical aspects of the work. In many cases, automated tools are already available, such as various decision support systems, and even when they are not, they are technically possible given what is currently technically possible. So, the solution direction seems to be more in increasing the awareness of (the value of) potential support tools and methods, and fine-tuning these to fit the unique context in which CSIRTs operate.

The current project has aimed to make explicit the most glaring problems experienced by CSIRTs and develop a concept and support tool with which to address them. Future research should focus on the continued development of The Reporter. The interviews reported in Chapter 6 indicate that some of the most urgent challenges involve the more complex aspects of team cooperation, such as how to balance improved team coordination and communication with the need for focus and uninterrupted time to work on a problem; how to balance the efficiency of standardised procedures with the need for adaptability and flexibility; or how to address effective knowledge management in terms of retaining and sharing knowledge and experience. In the coming year we hope to be able to address some of these issues, together with various stakeholders.

9 References

[IBM RSA]; IBM Rational System Architect tool; https://www.ibm.com/support/knowledgecenter/en/SS6RBX_11.4.3/com.ibm.sa_base.legal.doc/topics/rsysarch_overview_base.html.

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams. Challenges in supporting the organisational security function. Computers & Security, 31(5), 643-652.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Improving the effectiveness of CSIRTs. Global Cyber Security Capacity Centre: Draft working paper.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. IEEE Security & Privacy, 12(5), 61-67.

Cichonski. P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2. Retrieved from the Internet on 11 October 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Collection of DefCERT exercise observations by TNO; TNO; 2017

Collection of DefCERT interview results by TNO; TNO; 2017

Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology; NIST SP 800-61 revision 2; National Institute of Standards and Technology; Paul Cichonsky, Tom Millar, Tim Grance, Karen Scarfone; http://dx.doi.org/10.6028/NIST.SP.800-61r2.

DIS, I. (2009). 9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems. International Standardization Organization (ISO). Switzerland. Collection of DefCERT interview results; TNO; 2017

Email containing consolidated observations; N. Lokhorst; Eerste-luitenant, Adviseur DefCERT, DMO / JIVC / C4I&I / SOCC, DefCERT, Ministerie van Defensie; 01-12-2017.

ENISA; Computer Security and Incident Response Team (CSIRT) Setting up Guide; https://www.enisa.europa.eu/publications/csirt-setting-up-guide;

Fayad, F. (2010). Collective sensemaking in virtual teams. Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru.

Findley, K. A., & Scott, M. S. (2006). The Multiple Dimensions of Tunnel Vision in Criminal Cases. WIS. L. REV. 291-396.

First impression report (FIR) of Cognitive Task Analysis (CTA) DefCERT; TNO; Rick van der Kleij, Tom Hueting, Peter Paul Meiler, 2017.

Fransen, F., & Kerkdijk, R. (2017). Cyber threat intelligence sharing through national and sector-oriented communities. In: Florian Skopik (Ed.), Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level (pp. 187-224). Auerbach Publications.

Gladstein, D. L. (1984). Groups in context: A model of task group effectiveness. Administrative Science Quarterly, 29, 499-517.

Granåsen, M., & Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. Cognition, Technology & Work, 18(1), 121-143.

Hackman, J. R. (1987). The design of work teams. In J. W. Lorsch (Ed.), Handbook of organizational behaviour (pp. 315-342). Englewood Cliffs, NJ: Prentice Hall.

Hámornik, B. P., & Krasznay, C. (2018). A team-level perspective of human factors in cyber security: Security operations centers. In D. Nicholson (ed.), Advances in Human Factors in Cybersecurity (pp. 224-236), Advances in Intelligent Systems and Computing 593..

Hellwig, O., Quirchmayr, G., Huber, E., Goluch, G., Vock, F., & Pospisil, B. (2016, August). Major challenges in structuring and institutionalizing CERT-communication. In 11th International Conference on Availability, Reliability and Security (ARES). pp. 661-667. IEEE.

Hollnagel, E. (1993). Human Reliability Analysis: Context and Control. London: Academic Press.

International Organization for Standardization (2010). *Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems* (ISO Standard No. 9241-210:2010).

Kaufman, R. A., Rojas, A. M., & Mayer, H. (1993). Needs assessment: A user's guide. Educational Technology.

Klein, G. (1998). Sources of power: How people make decisions. Cambridge, MA: MIT Press

Klein, G. (2007). Performing a project premortem. Harvard Business Review, 85(9), 18-19.

Klein, G., Moon, B., & Hoffman, R. (2006). Making Sense of Sensemaking 1: Alternative Perspectives. Intelligent Systems , 21 (4), 71.

Klein, G., Moon, B., & Hoffman, R. F. (2006). Making sense of sensemaking 1: alternative perspectives. IEEE Intelligent Systems, 21(4), 70–73.

Klein, G., Wiggins, S., & Dominguez, C. O. (2010). Team sensemaking. Theoretical Issues in Ergonomics Science, 11(4), 304-320.

Landgren, J. (2005). Supporting fire crew sensemaking enroute to incidents. International Journal of emergency management. Vol. 2, No. 3.

McMaster, R. Duffy, T., Barber, C. (2012) The role of artefacts in Police Emergency response sensemaking. Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada.

Mitchell, D. J., Edward Russo, J., & Pennington, N. (1989). Back to the future: Temporal perspective in the explanation of events. Journal of Behavioural Decision Making, 2(1), 25-38.

NAF; NATO Architecture Framework; http://nafdocs.org/; https://en.wikipedia.org/wiki/NATO_Architecture_Framework.

National Coordinator for Security and Counterterrorism (2016). Cyber Security Assessment Netherlands (CSAN) 2016. Retrieved from the internet on May 18, from https://english.nctv.nl/binaries/CSAN%202016_def_tcm32-145252.pdf

Ntuen, et al. (2006) in Umapathy, 2010.

Pirolli, P., & Card, S. (2005, May). The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. In: Proceedings of International Conference on Intelligence Analysis (Vol. 5).

Pirolli, P., & Card, S. K. (1999). Information foraging. Psychological Review, 106, 643-675.

Plous, Scott (1993). The Psychology of Judgment and Decision Making.

Rajivan, P., & Cooke, N. (2017). Impact of Team Collaboration on Cybersecurity Situational Awareness. In Liu, Jajodia, & Wang (Eds.). Theory and Models for Cyber Situation Awareness (pp. 203-226). Springer. Cham, Switzerland.

Rowley, J. (2012). Conducting research interviews. Management Research Review, 35(3/4), 260-271.

Russell, D. M., Stefik, M. J., Pirolli, P., & Card, S. K. (1993). The cost structure of sensemaking. Paper presented at the INTERCHI '93 Conference on Human Factors in Computing Systems, Amsterdam.

Salas, E., Sims, D. E., & Burke, C. S. (2005). Is there a “big five” in teamwork? Small Group Research, 36(5), 555-599.

Silicki, K.,, & Mirosław, Maj. (2008). Barriers to CSIRTs cooperation. Challenge in practice–the CLOSER Project. 20th FIRST Annual Conference. Vancouver, Canada.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams Based research. IEEE Security & Privacy, 13(4), 20-29.

Stikvort, D. (2015). SIM3: Security Incident Management Maturity Model, S-CURE by PRESECURE GmbH, 2015, Available: https://www.trusted-introducer.org/SIM3-Reference-Model.pdf.

Tetrick, L., E., Zaccaro, S. J., Dalal, R. S., Steinke, J. A., Repchick, K. M., Hargrove, A. K., Shore, D. B., Winslow, C. J., Chen, T. R., Green, J. P., Bolunmez, B., Tomassetti, A. J., McCausland, T. C., Fletcher, L., Sheng, Z., Schrader, S. W., Gorab, A. K., Niu, Q., & Wang, V. (2016). Improving social maturity of cybersecurity incident response teams. Fairfax, VA: George Mason University. Available at: http://calctraining2015.weebly.com/the-handbook.html

The White House (2015, April). Statement by the President on executive order “Blocking the property of certain persons engaging in significant malicious cyber enabled activities”. Retrieved from the internet on 11 October 2017, from: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/statement-president-executive-order-blocking-property-certain-persons-en.

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. Computers & Security, 45, 42-57.

Turner, M., & Pratkanis, A. (1998). Twenty five years of groupthink research. Organizational Behaviour and Human Decision Processes, 73(2), 105–115.

Umapathy, K. (2010). Requirements to collaborative sensemaking. CSCW CIS Workshop, Savannah, GA, USA.

Van der Kleij, R., & Te Brake, G. (2010). Map-mediated dialogues: Effects of map orientation differences and shared reference points on map location-finding speed and accuracy. Human Factors: The Journal of the Human Factors and Ergonomics Society, 52, 526-536. DOI: 10.1177/0018720810377326.

Van der Kleij, R., De Vries, T., Walter, F., Van der Vegt, G., Visser, I., Essens, P., & Vogelaar, A. (2011). Coordinating across boundaries within multiteam systems: The importance of members’ personalities. 7th Biennial International Conference of the Dutch HRM network. November 10-11, 2011, Groningen, the Netherlands.

Van der Kleij, R., Kleinhuis, G. & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. Front. Psychology (Special issue Cognitive Sciences and The Human Factor in Civilian and Military Cyber Security), 12 December 2017, https://doi.org/10.3389/fpsyg.2017.02179.

Van der Kleij, R., Schraagen, J. M. C., De Dreu, C. K. W., & Werkhoven, P. (2009). How conversations change over time in face-to-face and video-mediated communication. Small Group Research, 40, 355-381. DOI: 10.1177/1046496409333724

Veinott, B., Klein, G. A., & Wiggins, S. (2010). Evaluating the effectiveness of the PreMortem Technique on plan confidence. The 7th International ISCRAM Conference (p. 1-9). Seattle, USA.

Watkins, R., Leigh, D., Platt, W., & Kaufman, R. (1998). Needs assessment-a digest, review, and comparison of needs assessment literature. Performance improvement, 37(7), 40-53.

Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26 (2), xiii-xxiii.

Weick, K.E. (1995). Sensemaking in Organizations, London: Sage.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2003). Handbook for computer security incident response teams (CSIRTs) (No. CMU/SEI-2003-HB-002). Carnegie-mellon univ pittsburgh pa software engineering inst.

Wiik, J., Gonzalez, J. J., & Kossakowski, K. P. (2006, June). Effectiveness of proactive CSIRT services. In IMF (pp. 67-81).

Woods, D.D. (in press). The theory of graceful extensibility: Basic rules of the adaptive universe. IEEE Systems, Man, & Cybernetics.

Wu, A., Convertino, G., Ganoe, C., Carroll, J. M., & Zhang, X. L. (2013). Supporting collaborative sense-making in emergency management through geo-visualization. International Journal of Human-Computer Studies, 71(1), 4-23.

A Research questions

We derived a set of research questions from the field experiences (Chapter 6), based on our observations and interviews. The impact of the research questions on the focus of this report is indicated in a bulleted list below, by a "→" for each research question. The arrow refers to the table "Overview of needs and wants of Incident Response Teams" in Section 2.1.

1 The design of the working area can be improved. It could be re-designed to facilitate better cooperation in between and outside of the different working domains (analyst, handler, expertise). Allow flex working space, take your laptop to where the work is being done?
   - → Organization needs: Collaborative problem-solving capacity & shared incident awareness.
   - → Work within a larger (multiteam) system consisting of multiple interacting teams.

2 Analysts can be disturbed by interruptions. This could increase work-pressure. At the same time, there is a need for teamwork among analysts. How can the design of the working area be improved to facilitate this?
   - → See 1) above.

3 The incident coordinator is an important element of the team. He diminishes boundaries between the different sub-teams and he facilitates the development of team cognition. How can the coordinator best be supported in this task? Which competences and behaviour are required? What can communications technology provide? What do developments in this discipline imply for this role?
   - → Organization needs: Collaborative problem-solving capacity & shared incident awareness.
   - → Team performance needs: Information sharing and decision making across personnel shifts & handoffs and work within a larger (multiteam) system consisting of multiple interacting teams, including IT personnel from customer; Shared team knowledge: Information about the roles and expertise of each team.
   - → Individual needs: Dealing with work load variations: managing peaks and underload.

4 How can knowledge best be retained and shared? This includes e.g. knowledge about "false positives."
   - → Team performance needs: Information sharing and decision making across personnel shifts & handoffs; Work within a larger (multiteam) system consisting of multiple interacting teams; Keeping everybody informed & staying informed, especially when working distributed.

5 How can an adaptive capacity be built into the team to ensure maximum flexibility? Incidents may be very different, yet at the same time a form of standardisation (protocol) is required.
   - → Organization needs: Coordination and sharing information with outside parties; Organizational & incident learning; Measuring the effectiveness of incident handling; Collaborative problem-solving capacity.

→ Team performance needs: Shared team knowledge: Information about the roles and expertise of each team; Information sharing and decision making across personnel shifts & handoffs; Work within a larger (multiteam) system consisting of multiple interacting teams, including IT personnel from customer; Keeping everybody informed & staying informed, especially when working distributed.

→ Instrumental needs: Estimating the initial impact and risk of cyber security incidents; Need for better interpersonal communication tools, especially during larger incidents; Providing good & structured reports of incidents; Creating useful (visual) overviews at any particular point in time for a different audience (e.g., customer, management, colleagues).

6 How can (software) tools best be deployed, adapted, extended, or further developed? What other tools may be needed?

→ Instrumental needs: Estimating the initial impact and risk of cyber security incidents; Need for better interpersonal communication tools, especially during larger incidents; Providing good & structured reports of incidents; Creating useful (visual) overviews at any particular point in time for a different audience (e.g., customer, management, colleagues).