Cognition, Technology & Work (2024) 26:709–731
https://doi.org/10.1007/s10111-024-00779-1

RESEARCH

Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval

Annika Andreasson[1] · Henrik Artman[1,2] · Joel Brynielsson[1,2] · Ulrik Franke[1,3]

Received: 5 May 2023 / Accepted: 24 August 2024 / Published online: 27 September 2024

Abstract

In recent years, the Swedish public sector has undergone rapid digitalization, while cybersecurity efforts have not kept even steps. This study investigates conditions for cybersecurity work at Swedish administrative authorities by examining organizational conditions at the authorities, what cybersecurity staff do to acquire the cyber situation awareness required for their role, as well as what experience cybersecurity staff have with incidents. In this study, 17 semi-structured interviews were held with respondents from Swedish administrative authorities. The results showed the diverse conditions for cybersecurity work that exist at the authorities and that a variety of roles are involved in that work. It was found that national-level support for cybersecurity was perceived as somewhat lacking. There were also challenges in getting access to information elements required for sufficient cyber situation awareness.

Keywords Cybersecurity · Information security · Cyber situation awareness · Public sector · Security management

1 Introduction

That contemporary society is undergoing rapid digitalization is no longer news. This digitalization was accelerated by the COVID-19 pandemic, as the world had to face a new reality (Amankwah-Amoah et al. 2021). Many countries have established digitalization strategies, e.g., Denmark (Ministry of Finance 2022), UK (Department for Digital, Culture, Media, and Sport 2022), the Netherlands (Nederland Digitaal 2021), Sweden (Regeringskansliet 2017), to show clear governmental leadership in the area. In addition, in 2021, the members of the European Union, Norway, and Iceland signed a declaration for a green digital transformation as part of the efforts to reach the UN Sustainable Development Goals (European Commission 2021). In this declaration, they commit, amongst other things, to working toward an acceleration of making public services, including those related to education, healthcare, agriculture, and e-government, available online and actively encourage teleworking during and past the pandemic (European Commission 2021).

The envisaged benefits of digitalization, however, will not materialize if cybersecurity efforts are not on a par with digitalization efforts. While it might seem a bit narrow in focus at first sight, Sweden is an interesting case to look at in this respect because the country consistently ranks high in terms of digitalization. For instance, Sweden placed fourth among all EU nations in the Digital Economy and Society Index (DESI) 2022 (European Commission 2022) published by the European Commission. Finland, Denmark, the Netherlands, and Sweden—the top four EU nations in the index—are in fact regarded to be among the world's leaders in digitalization. Nevertheless, in international cybersecurity assessments, Sweden frequently receives worse marks. As an example, Sweden's position in the 2020 ITU Global Cybersecurity Index (GCI) (ITU 2020) was merely twenty-sixth

✉ Annika Andreasson
anniandr@kth.se
https://www.kth.se/profile/anniandr

Henrik Artman
artman@kth.se

Joel Brynielsson
joel@kth.se
https://www.kth.se/profile/joel/

Ulrik Franke
ulrikf@kth.se

[1] KTH Royal Institute of Technology, Stockholm, Sweden

[2] FOI Swedish Defence Research Agency, Stockholm, Sweden

[3] RISE Research Institutes of Sweden, Kista, Sweden

compared to seventeenth in 2017, which was the previous time Sweden actively participated in the study.[1] Hence, Sweden, as a subject of study, is interesting because of the conflict between being a leader in digitalization and, perhaps, lagging behind in cybersecurity. This conflict certainly exists in one form or another in other countries as well.

One objective in the Swedish national cybersecurity strategy is that "[c]entral government authorities, municipalities, county councils, companies and other organisations are to have knowledge of threats and risks, assume responsibility for their cyber security and conduct systematic cyber security efforts" (Government Offices of Sweden 2017). Swedish administrative authorities are part of the central government authorities mentioned in the strategy and they are also the focus of this study.

Swedish administrative authorities often process information in shared IT systems and are subject to legal requirements on information security aimed at Swedish government authorities, where the above-mentioned objective from the national cybersecurity strategy was put into regulation. However, the different nature, size, and resources of these authorities could lead to variations in the ability to protect IT systems and information, which could, e.g., leave room for potential attackers to use one authority as an attack vector for gaining access to the next authority.

In the aftermath of the COVID-19 pandemic, an invasion war in Europe, and Sweden's accession to NATO, Swedish municipalities, county councils, and government agencies have been subjected to different types of cyberattacks. Kalix municipality suffered a crippling ransomware attack, the Swedish Environmental Protection Agency had large amounts of data exfiltrated, the Swedish Armed Forces and several other societal actors' external websites were targeted by distributed denial-of-service (DDoS) attacks, as was the Swedish election authority during election night in 2022 (Lindström 2022; Tanaka and Flores 2023).

In this landscape with increasing potential threats, an increasing number of assets, in a work environment where employees work in hybrid settings outside the authority perimeter, it is vital that employees working with cybersecurity at Swedish administrative authorities have cyber situation awareness, i.e., "know what's going on" in the cyber domain (Franke and Brynielsson 2014). The purpose of this study is to characterize the conditions for cybersecurity work at Swedish administrative authorities. Hence, the study serves to investigate the following research question:

- What characterizes the conditions for cybersecurity work at Swedish administrative authorities?

To answer the overarching question, the following sub-questions were formulated:

- What are the organizational conditions for cybersecurity work in terms of individual, authority, and national level?
- What do cybersecurity staff do to acquire the cyber situation awareness required for their role?
- What experience do cybersecurity staff have with incidents?

The remainder of the paper is structured as follows. Section 2 provides background on the regulatory framework for information security in administrative authorities and presents the regulatory authority the Swedish Civil Contingencies Agency, introduces cyber situation awareness, and presents related work. The method used is explained in Sect. 3. Section 4 presents the results, which are then discussed in Sect. 5. Finally, Sect. 6 concludes the paper and suggests directions for future work.

2 Background and related work

This section briefly describes the regulatory framework and the role of the Swedish Civil Contingencies Agency regarding issuing legislation and offering support for information security at administrative authorities. Additionally, the section introduces the concept of cyber situation awareness, and presents related work.

2.1 Regulatory framework

In Sweden, the legal act SFS 2015:1052 (2015), Ordinance Regarding Crisis Preparedness and Supervisory Authorities' Actions at Heightened Alert, gives the Swedish Civil Contingencies Agency (MSB) the mandate to issue regulations related to government authorities' information security. In accordance with SFS 2015:1052 (2015), MSB issued three regulations that came into force on October 1, 2020, targeting cybersecurity at government authorities. At the time of this study, the authorities should comply with the regulations:

- MSBFS 2020:6 (2020) Regulations Regarding Information Security at Government Authorities: These regulations set the basic requirements for how the authorities should work with information security based on the standards ISO/IEC 27001/2.
- MSBFS 2020:7 (2020) Regulations Regarding Security Controls for Information Systems at Government Author-

[1] Sweden ranked thirty-second in 2018, but did not actively participate in the data collection.

ities: These regulations outline the minimum security requirements for the authorities.

- MSBFS 2020:8 (2020) Regulations Regarding IT-incident Reporting at Government Authorities: These regulations describe what constitutes an incident to be reported to MSB.

In addition to the regulations themselves, MSB provides supporting materials and practical guidelines for implementation. Government authorities shall report IT incidents, meeting certain requirements, to MSB.[2] While the MSB regulations are the main legal acts for information security at administrative authorities, there are other European Union and national legal acts affecting cybersecurity at administrative authorities, e.g., GDPR (Council of the European Union 2016), the Protective Security Act (SFS 2018:585 2018), and the Public Access to Information and Secrecy Act (SFS 2009:400 2009).

MSB is also the host for the Swedish national computer security incident response team (CSIRT), known as CERT-SE. This team is responsible for supporting Swedish society in preventing and managing IT security incidents. CERT-SE serves as Sweden's primary point of contact for similar functions in other countries and works to enhance cooperation and information exchange with these counterparts. CERT-SE's open-source intelligence communication includes weekly newsletters and flash messages for critical threats.

2.2 Situation awareness

An important aspect of cybersecurity is situation awareness (SA) or, more colloquially, "knowing what's going on." Various theories and definitions of SA have been suggested in the research literature (Salmon et al. 2008). Mica Endsley's definition deriving from work with fighter pilots, is one of the most frequently cited and intuitive definitions:

> Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. (Endsley 1995)

Endsley's model is an individualistic cognitive model comprising three tiers: Level 1 "perception," Level 2 "comprehension," and Level 3 "projection" (Endsley 1995). While the three levels of SA represent an increasingly complex understanding of the situation, they should not be seen as a linear progression of stages (Endsley 2015).

Often discussed in relation to SA is the concept of the common operational picture (COP) (Conti et al. 2013; Steen-Tveit and Munkvold 2021). A COP is an artifact that presents a "picture" of what's going on, while SA is a mental state of the operator being, to some extent, aware of what's going on (Franke et al. 2022). A COP can support both individual and team SA. In times of incidents, emergencies, and crises, the COP is used to facilitate the sharing of pertinent information elements (Wolbers and Boersma 2013; Comfort 2007).

Within the cyber domain, the concept of SA has garnered increasing scholarly interest. Academic researchers are progressively focusing on this important aspect of cybersecurity. For cyber situation awareness (CSA), Franke and Brynielsson (2014) take Endsley's definition and see CSA as a specific instance of SA that applies to the cyber domain. However, the cyber domain is distinct from other domains in the sense that the characteristics of "time" and "space" are difficult to determine when it comes to defining a situation, since cyberattacks can occur within a split second and might not be discovered until much later, and be initiated by attackers from across the globe. As a way of dealing with the issue with different aspects of time, Franke et al. (2022) suggest discerning between *network-centric* and *domain-centric* CSA, where the network-centric type has a technical emphasis and a short-term timescale and the domain-centric type has an organizational/mission emphasis and a longer-term timescale. This distinction also allows for broadening the scope of people in an organization that need to achieve relevant CSA. McKenna et al. (2015) identify that different roles, such as cyber analyst, network operations center (NOC) manager, director of IT, and CEO, all need to have an adequate level of CSA within a timeframe specific to their role. Gutzwiller et al. (2020) emphasize this broadened scope by pointing out a research gap where there is a need to define what CSA is for different types of roles involved in cybersecurity work.

The current landscape of research relating to CSA concerns many diverse areas, e.g., CSA in security operations centers (SOCs) (Ofte and Katsikas 2023; Munsinger et al. 2023), CSA for critical infrastructure (Nafees et al. 2023; Dayaratne et al. 2023), visualizations for CSA (Jiang et al. 2022; Ask et al. 2023), techniques for CSA measurement (Brynielsson et al. 2016b), and data mining for CSA (Husák et al. 2020). Nevertheless, the organizational perspective on CSA remains limited.

Endsley's individualistic model of SA has been criticized, and, e.g., recent research on situation awareness in SOCs suggests that CSA should be understood from the dual perspective of the human operator and the system (Ofte and Katsikas 2023). From a sociotechnical approach, work practices are distributed among several persons as well as different forms of tools, which together form conditions for how information is propagated within the organization, see, e.g., Artman and Wærn (1999). In line with such a sociotechnical approach, this study aims to illuminate the organizational

[2] The security service, police, and defense authorities are excepted from this rule.

conditions for staff who are responsible for cybersecurity to form and maintain an adequate level of CSA.

2.3 Related work

Recent literature emphasizes the increasing complexity and criticality of cybersecurity roles within administrative authorities. For instance, Chałubińska-Jentkiewicz (2022) notices the growing number of individuals and organizations that have become involved during recent years, and highlights the need for personnel working in different fields to cooperate and exchange information across borders, to be able to work more effectively. In the study, it is concluded that administrative, military, and civilian fields are being digitized at speed, resulting in the creation of parallel cybersecurity units that could benefit from more cooperation.

The growing range of responsibilities that cybersecurity professionals must manage, including not only technical defenses but also compliance with evolving regulations and the management of sophisticated threat landscapes, are highlighted in discussions regarding forthcoming cybersecurity strategies serving to advance nations to leading positions in cybersecurity. Regarding the case of, for example, Australia, Svantesson (2023) points specifically to challenges related to the cybersecurity workforce, the regulatory frameworks, and the cybersecurity ecosystem.

Yet other recent literature discusses the need for caution due to increased exposure to cyberthreats, highlighting the social aspects due to roles at administrative authorities. Frandell and Feeney (2022) point specifically to the need for manager vigilance and buy-in to be able to reduce incidents, and to the need for agencies to prioritize both social and technical solutions to cyberthreats. In their study, they relate social factors regarding values and perceptions with technical factors regarding design and capacity, and conclude that these factors are intertwined and interact, and must be understood together to understand how social and technical factors are associated with governmental cyberthreats. Their work underscores the need for administrative authorities to invest in both human and technological resources to maintain robust cybersecurity defenses.

This paper studies cybersecurity at Swedish government authorities. Much has been written about governments and cybersecurity in general, for instance, addressing topics such as whether governments should regulate with a light touch (Moore 2010) or use more coercion to foster security (Weber 2017), as well as other high-level governance issues (Sterlini et al. 2020). There is also abundant literature describing government cybersecurity work from political science and legal perspectives, e.g., books on how cybersecurity is governed in particular countries such as Switzerland (Cavelty 2014), France (Baumard 2017), and Germany (Schallbruch and Skierka 2018). Furthermore, there are studies of how government agencies respond to cyber crises (see, e.g., Boeke 2018) and cyberterrorism (see, e.g., Wirtz and Weyerer 2017). However, all these strands of literature are quite different from the study reported here, which focuses instead on concrete, everyday work in non-specialist government authorities and, in particular, on the individuals carrying it out.

Thus, a set of closely related work is comprised of empirical studies of government officials in their work roles. For example, Caruson et al. (2012) surveyed Florida county officials about cyberthreats and awareness, concluding that there is a lack of preparedness, which can be attributed to a lack of knowledge and sense of urgency. Similarly, Hatcher et al. (2020) surveyed officials in US municipalities about cybersecurity plans and policies, demonstrating that though such documents exist, they need to be better integrated into daily management processes. Similar findings are also reported by Norris et al. (2021), who administered a nationwide survey about cybersecurity in US local government and corroborated the fact that local governments do not manage cybersecurity well. However, though such studies are similar in their focus on government officials in their work roles, they also differ importantly from the work reported here. More precisely, this study (i) addresses national rather than local government, (ii) offers a European (Swedish) rather than US perspective, and, most importantly, (iii) offers qualitative rather than quantitative findings.

3 Method

A qualitative research approach was used to explore the conditions, including work descriptions, mandate, practices of discovering incidents, and maintaining CSA, for cybersecurity staff at Swedish administrative authorities. Semi-structured interviews were conducted with the respondents over a two-week period in November 2020.

3.1 Respondents

The respondents in this study were recruited through a previous study on Swedish administrative authorities and cybersecurity during the COVID-19 pandemic (Andreasson et al. 2020). In the questionnaire distributed to all administrative authorities for that study, the respondents were asked if they were interested in participating in another study focusing on CSA. The questionnaire was aimed at persons responsible for the cybersecurity work at the authority. 44 respondents indicated interest by providing their email addresses and were subsequently invited to participate in the current study. Out of the 44 invited respondents, 20 accepted and were scheduled for an interview. At the time of the interviews, one interview was canceled at the respondent's request after

Table 1 Respondents' role, information security work share, years at authority (when known), and authority size (S = fewer than 100 employees, M = 100–500 employees, L = more than 500 employees)

Resp.	Role	Full-time	Years at auth.	Auth. size
R1	IT manager	No	4	S
R2	Project manager	No	1	S
R3	Information security coordinator	Yes		L
R5	IT security coordinator	No	7	L
R6	IT manager	No	7	S
R7	Security manager	No	7	M
R8	Information security manager	No	3.5	L
R10	Information security manager	Yes	14	L
R11	Information security coordinator	Yes	3	M
R12	Security strategist	No		S
R13	IT manager	No		M
R14	IT coordinator	No	5	S
R15	Information security manager	No	10	M
R16	Security manager	No	11	M
R17	Security manager	No	1.5	L
R18	IT administrator	No	2	S
R19	IT security architect	Yes	14	L

having read the project information and informed consent form, one respondent did not show up at the time of the scheduled interview and did not respond to two follow-up requests for rescheduling the interview, and one respondent was excluded from the study after stating, during the interview, that their role had no bearing on cybersecurity, but had been actively involved in the crisis management of COVID-19.

In total, 17 respondents representing 17 administrative authorities were included in the study. The respondents have different roles and a majority of them do not work with cybersecurity full-time, as can be seen in Table 1. They have both technical and nontechnical backgrounds. Some respondents have more than one role; the role indicated in Table 1 is the role they identified themselves as when responding during the interview. For the purposes of this paper, authorities with fewer than 100 full-time employees are referred to as small (S), 100–500 employees are considered medium (M), and more than 500 employees are considered large (L). The respondents cover 9 out of 11 government ministries.[3]

3.2 Interview procedure

The interviews were primarily conducted online due to COVID-19 recommendations in place at the time of interviewing. When scheduling the interviews, the respondents were sent information about the project they were asked to participate in, along with a consent form. The interviews were conducted using different digital collaborative tools, with or without video. The interviewer had the video switched on at all times, as offered by the tool. One interview was conducted over the phone as the respondent's internet connection was unstable. The interviews were scheduled for 60 min and were recorded with audio only on a separate voice recorder. The interviews were then transcribed verbatim by the interviewer before analysis. A summary of the interview was shared with each respondent afterwards, providing an opportunity to clear up possible misunderstandings.

At the beginning of the interview, the interviewer described the context and purpose of the interview, and provided an opportunity for questions before starting the recording. If the respondent, due to COVID-19 restrictions, had not been able to sign and return the consent form, verbal consent was taken at the time of the interview. The interview guide developed was loosely structured around five focus areas, leaving room for the respondents to freely talk about what they experience as important, while still being of interest to the research project (Patton 2002). The five focus areas were (i) respondent, (ii) authority, (iii) "knowing what's going on" (i.e., SA), (iv) incident experience, and (v) COVID-19.

As the main interest of this study was to investigate the conditions for CSA, i.e., the perception of events, their significance, the potential future consequences, and how to maintain an appropriate level of CSA when handling such events, the interviews were structured to examine the respondents' roles and mandates to act, as well as their

[3] At the time of the interviews, there were 11 ministries in Sweden.

processes for receiving, assessing, and responding to information about the current status of their authority's digital systems. Given that this research was conducted through interviews rather than observations of actual incidents, the interviewer prompted respondents to ground their responses in tangible practices and specific incidents. This approach was adopted to ensure that the data collected reflected real-world experiences and practices rather than hypothetical scenarios, thus capturing what information elements the respondents perceived, how they valued diverse sources of information, and how they made use of that information when going forward.

The interview guide was structured around seven main questions covering the five focus areas mentioned above. The first question in the interviews asked the respondent about their background and their work, and let them speak freely from there. During the interview, the interviewer checked that the sub-areas of each question were covered. If the respondent did not mention an area, the interviewer prompted with a question worded as suited the respondent's role and experience to cover the area. When a respondent addressed a question not yet asked, the interviewer moved to that area of inquiry, covered it, and then returned to the previous area. This way, the respondents drove the interview with their responses and examples by speaking freely. Thus, questions in the interview guide might not have been asked verbatim or asked at all if the area had already been covered by the respondent. The interview guide with the main questions and sub-areas can be found in Appendix A.

The interviews lasted between 43 and 72 min and touched upon the focus areas to varying depths, depending on the respondent's role and time constraints.

3.3 Data analysis

Thematic analysis, informed by the six phases outlined by Braun and Clarke (2006), was used on the empirical material from the interviews. The six phases, while listed in order, are not linear but rather recursive and iterative in nature: (i) *Familiarization with the data*. The researcher performing the interviews listened actively to the recordings before transcribing each interview. After transcribing all interviews, the transcripts were read through multiple times, and preliminary notes were taken. The transcripts were then initially analyzed by two of the authors, together discussing and noting potential codes. (ii) *Generating initial codes*. The transcribed interviews were imported to Taguette (Rampin and Rampin 2021), which was used when working on generating the initial codes. Initial coding was primarily inductive, allowing it to reflect the content of the empirical material. This process generated 887 text extracts coded with 73 codes. (iii) *Creating themes*. Potential themes were created from 45 of the codes. The themes were analyzed deductively to a degree to make sure that the themes generated were meaningful to the research questions. Three main themes were identified along with subthemes. (iv) *Reviewing themes*. The data extracts for each theme were exported to a spreadsheet, reviewed iteratively, and re-coded if needed. (v) *Defining themes*. Names were settled for each theme. The final thematic map can be seen in Fig. 1. A table with the final themes, subthemes, the codes related to those themes, as well as the number of respondent interviews where the code occurs, i.e., how many of the 17 respondent interviews that contain the code, and the code frequency, i.e., how many data extracts in total that are coded with the code, can be found in Appendix B. (vi) *Producing the report*. Final analysis was done, data extracts highlighting the themes were chosen and translated from Swedish to English,[4] and results were reported and discussed.

4 Results

The purpose of this study was to characterize the conditions for cybersecurity work at Swedish administrative authorities, and the analysis of the empirical material shows that there is considerable variation among the respondents regarding the conditions for and experience of cybersecurity work. As shown in Fig. 1, the thematic analysis led to the creation of three themes detailing the conditions of cybersecurity work at the Swedish administrative authorities: (i) Organizational conditions, (ii) Information elements, and (iii) Incident experience.

Organizational conditions: This theme explores the organizational conditions that impact cybersecurity work at the administrative authorities. It includes three subthemes related to the respondent's role, administrative authority, and national-level support. The findings presented here shed light on the organizational context for cybersecurity staff at the individual, authority, and national levels, thus addressing the first research sub-question.

Information elements: The second theme focuses on the information elements that contribute to the respondents' CSA. These information elements stem from different areas as outlined in the subthemes: intelligence, technology, organization, and compliance. Identifying the various sources of information elements that go into cybersecurity staff's CSA can help improve the quality of those sources. This theme addresses the second research sub-question regarding what cybersecurity staff do to acquire the cyber situation awareness required for their role.

[4] All data extracts were translated from Swedish to English by the authors.

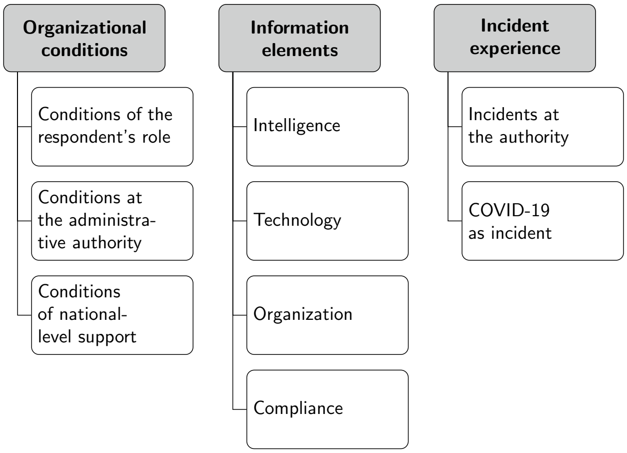
Organizational conditions
Conditions of the respondent's role
Conditions at the administrative authority
Conditions of national-level support
Information elements
Intelligence
Technology
Organization
Compliance
Incident experience
Incidents at the authority
COVID-19 as incident

Fig. 1 Themes and subthemes

Incident experience: The third theme concerns the respondents' incident experience, covering two subthemes: incidents at the authority level and the impact of COVID-19 as an incident. Understanding these experiences provides valuable insights into the challenges faced by cybersecurity staff and how previous incident experience can improve CSA. This theme addresses the third research sub-question concerning cybersecurity staff incident experience.

4.1 Organizational conditions

This theme presents and discusses the organizational conditions for cybersecurity work perceived by the respondents, answering the first research sub-question. The theme has three subthemes: (i) the conditions of the respondent's role at the administrative authority, (ii) the conditions at the administrative authority, and (iii) conditions of national-level support.

4.1.1 Conditions of the respondent's role at the administrative authority

The first subtheme addresses the respondents' experiences of their own role at the administrative authority, specifically their perceived mandate to take action in their roles.

More than one respondent, when discussing their own role and the mandate associated with that role, expressed that their role was advisory. They bring issues to the attention of the role with decision-making power and advise on actions. As Respondent 11 stated:

> [W]hat I can do really in my role is to inform management and ultimately the director then that here I see something that is not according to the regulations, or that can lead to a risk we need to consider. [R11]

When the role involves providing advice, the employee, as the subject-matter expert, faces significant pressure to effectively communicate the risks and potential consequences to management. This communication is crucial so that management, who may not be security experts themselves, can make informed decisions about the best course of action.

Respondent 10, on the other hand, perceived themselves to have a wide mandate and decision-making power in their role:

> Well yes! I even have the possibility to depart from the director general's decision if necessary, [...] which I need to handle with some care. [R10]

For this respondent, knowing that the power is there provides a stable foundation for the role's decision-making, while also acknowledging that there could be consequences if handled carelessly.

Going outside the mandate of the role was expressed by Respondent 1. When discussing if there was an explicit mandate allowing them to take drastic action, they said:

> No, there isn't. However, I would probably do that regardless. [R1]

This respondent has an idea of how great the consequences of inaction in pivotal moments could be and, by deciding to act in such a moment, expressed that they have faith in their own ability to judge situations and when to act decisively under certain circumstances when the threat is deemed severe enough, even in the absence of an explicit mandate.

4.1.2 Conditions at the administrative authority

The second subtheme relates to how the respondents perceive the conditions under which they operate, especially with regard to management attitude, clear responsibility for information security work, and the authority's ability to detect and respond to incidents.

The respondents gave voice to variations in management attitude to cybersecurity. The MSB regulations (MSBFS 2020:6 (2020); MSBFS 2020:7 (2020); MSBFS 2020:8 (2020)) were mentioned by some respondents as helpful when it comes to getting management support. With the regulations putting legal requirements on management in place, the government, through MSB, signals the national importance of cybersecurity. Respondent 2 believed that their repeated arguing for how MSB views information security has led to changes in management attitude:

> [I]t has sunk in that "well, okay, this is something that needs the management's prioritization." [R2]

In this case, management responded to the government's signals that cybersecurity needs to be on the management's agenda.

A change in management can impact how cybersecurity is regarded at the top level. New management might not have similar experience or understanding of the complexity of cybersecurity. For Respondent 1, a new acting director general led to a shift in attitude. Where the previous director general had a cautious approach, the new acting director general did not understand the issues related to implementing new solutions:

> And that could be, from a technical perspective or from a security perspective, extremely difficult since what they are asking for then, is detrimental to security. [R1]

A change in management can thus have significant consequences for the cybersecurity stance at an authority where there might be trust issues and knowledge gaps between new management and cybersecurity staff that have not yet been bridged.

Another respondent reported that they perceive they have the trust of the management. Respondent 6 mentioned how management trust and financial backing led to a transfer of decision-making power:

> I have the go-ahead from management that I can call for emergency help kinda [...] without awaiting their approval. [R6]

By putting the power to request emergency assistance within the remit of the cybersecurity staff, management displays an understanding of the importance of time when handling cybersecurity incidents, as well as trust in their own staff's expertise to decide when external resources are needed. Management support by cutting a bureaucratic step, can save vital time in incident handling.

The basis for systematic cybersecurity work in organizations is that management exhibits leadership and dedication to the issue. This is stressed in the international standard for information security (ISO/IEC 27001:2017) as well as in the national MSB regulations (MSBFS 2020:6 2020).[5] Still, as shown by the respondents, management support varies among authorities.

When the administrative authority organizes its information security, the MSB regulation states that responsibility should be clear and the roles working with information security should have the mandate required (MSBFS 2020:6 2020). Some respondents' organizations are more mature in this regard than others. Respondent 10 responded to a query about whether the authority lives up to the requirements of clear areas of responsibility in the regulation:

> Well, I should hope so since we are ISO certified and have been doing this for 24 years, so something must have stuck during these years. [R10]

That some authorities have higher maturity could be a result of taking part in international collaborations requiring ISO/IEC 27001 certification or being subject to other European or international regulations, for example.

For other respondents, the MSB regulation is driving a formalization of areas of responsibility for information security within the authorities, which was not there before. Complying with legal requirements is pushing management to implement updated policy. Respondent 2 pointed out that a new policy is prepared for decision:

> [I]n there we have [...] appointed roles as information security manager, there is a chief technical officer, CTO, there is a CIO appointed, I will also have an information security council. [R2]

There are also respondents working where the responsibilities are less clear. Respondent 8 mentioned that:

> I don't think it is so formally defined [...] you do what you think is within your role. And as long as several parties agree, there is no fuss. [R8]

The respondent is aware of the dangers of an informal organization where there is no documentation to serve as a reference when sorting out responsibilities, but still feels no need to formalize it. With no clear division of responsibilities, no one can be held accountable or be cleared from accountability when incidents occur.

Having the ability to promptly detect and handle incidents is another legal requirement in regulation MSBFS 2020:6 (2020). There is variety among the respondents on how they view their authorities' ability also in this regard. However, no respondent claimed that the ability is very good.

Respondent 14 identified that their organization is not one of the main targets for attackers, and said about their authority's ability:

> It is not at the same level as defense organizations, it is significantly better than that of a small company, perhaps just because we are a government authority. [R14]

While the respondent acknowledges that the incident handling ability is not at the level of military organizations, the requirements on government authorities' information security still make them better prepared than non-regulated organizations.

Some of the respondents work at administrative authorities where IT operations are outsourced, which could have

[5] The older standard ISO/IEC 27001:2017 is the standard referenced in MSBFS 2020:6 (2020).

an effect on the ability to detect and handle incidents. In such cases, the provider could be the first to discover incidents relating to operations, as for Respondent 7:

> IT operations are outsourced to a contractor [...]. And they have very good monitoring there, in a technical sense. [R7]

The effects of outsourcing IT operations and, thereby, the ability to detect and handle incidents are difficult to determine. The administrative authority's ability to discover operational incidents is most likely dependent on what is negotiated in the service level agreement (SLA) with the supplier, defining what incidents to report and within what timeframe.

There is also the less explicit Respondent 19, who, upon being asked about the administrative authority's ability, tersely said:

> Nah, it's not good. [R19]

This respondent recognizes that the ability is not good, but refrains from elaborating, thus not exposing possible weaknesses in their organization.

4.1.3 Conditions of national-level support

The third subtheme deals with national-level support. Several respondents expressed that the level of government support offered does not meet their needs. Respondent 2 mentioned that the Swedish Association of Local Authorities and Regions (SKR)[6] has issued tools for information classification, and that they lack equivalent tools at the government level. This tool shortage leads to authorities classifying information at different security levels, also in shared systems:

> That the same information is protected in similar ways by different authorities. [...] [I]nformation [...] ought to have the same need of protection no matter if it is with me or somewhere else. [R2]

This discrepancy between how authorities view the same information gives the impression of information classification being somewhat impromptu and could pose a risk.

There is also the case when regulatory bodies like MSB or the Swedish Security Service offer guidance for legal compliance that is not deemed sufficient by the respondents. Respondent 12 contacted the Security Service with a question regarding the guidance regarding special protective security[7] assessments:

> [T]he response I got was that we are aware of [the guidance] being pretty limited...[...] [I]t is so important that the whole chain is there from the steering not only within the authority but also so to speak, the holistic perspective when it comes to the protection of Sweden. [R12]

The lack of sufficient guidance jeopardizes national security when the authorities are not given the tools to do their bit to uphold national security to the best of their ability. When detailed instructions on what to do to be compliant are lacking, each authority makes its own interpretation of what compliance looks like.

A couple of respondents mentioned the challenges for smaller authorities. The support offered by the government does not take into account that smaller authorities have other needs than medium or large ones. Respondent 14 said:

> [W]e are a small authority. [...] [S]tate [...] support is targeting larger authorities. [...] [W]e have other needs, perhaps. And we don't quite play in the same division as these other large [...] organizations. [R14]

The support aimed at administrative authorities is not suited for all types of authorities. For example, smaller authorities sometimes have a hard time using publicly procured IT services as they are tailored for larger purchases.

Respondent 16 suggested specific government support that they would like to have when they lack in-house competency:

> [I] think it would be somewhat profitable for the government to provide [...] information security consultants, and perhaps have more detailed opinions on how to do things. [...] More hands-on, you could say everything from MSB is pretty fuzzy. [R16]

This respondent sees great advantages in having specialized government consultant resources who know how to work practically with information security compliant with MSB regulations, as they experience the guidance from MSB is not clear enough. As there is a shortage of cybersecurity professionals, this suggestion could be seen as utilizing the available competencies more efficiently.

Some respondents reported a lack of security intelligence from the government agencies. One respondent mentioned that the National Defence Radio Establishment (FRA) annual report, which is a step in the right direction, still is

[6] SKR is an organization for local governments in Sweden where all regions and municipalities are members.

[7] For more information on protective security, see https://www.sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/what-we-do/protective-security.html.

not enough for authorities to be able to take adequate security measures to protect Sweden. Respondent 15 elaborated:

> Through us, they can reach our ministries and then they might get access to God knows what. I think it is very shortsighted not to ensure that the entire state apparatus is provided with security intelligence in a better way. [R15]

Respondent 19 would like to have information that could be likened to an attacker persona (Atzeni et al. 2011; Brynielsson et al. 2016a; Tariq et al. 2012):

> I think it is more interesting for us actually to have intelligence on who the potential actors are[.] [T]his actor might want to do something with this purpose [...] and their *modus operandi* is...[T]hat could [...] help with the prioritization and consideration of having the right protective measures or detection mechanisms[.] [R19]

What Respondents 15 and 19 express is a view that protecting their authorities is part of protecting the nation, and they do not receive what, in their view, would be adequate intelligence from the specialized authorities. With access to such intelligence, they would be better placed to advise on what protective measures are needed for their authorities. They deem the other national authorities as the trusted natural source for such information.

4.2 Information elements

This theme deals with what information elements the respondents use to form an awareness of what's going on at the authority to be able to carry out their assigned task effectively. This theme is divided into four subthemes: (i) intelligence, (ii) technology, (iii) organization, and (iv) compliance.

4.2.1 Intelligence

Intelligence refers to the type of information that originates outside the organization that could have a bearing on operations. In general, intelligence gathering is an area that is deemed important and required by regulation MSBFS 2020:7 (2020), but nonetheless seems difficult to prioritize for some respondents. Respondent 8 reflected:

> [I]ntelligence gathering is important, but somewhere it is [...] a matter of priorities. You might not be able to do as much as you wish. [R8]

This respondent identifies intelligence gathering as a significant task but prioritizing intelligence gathering over other tasks might be difficult to justify, perhaps as the benefits from this activity are difficult to measure compared to other possible activities.

Respondent 6, on the other hand, mentioned that open-source intelligence (OSINT) gathering is part of their everyday routine:

> [I] always start my day by [...] doing this intelligence gathering. [R6]

For this respondent, the OSINT gathering is deemed to be of such importance that it is the first activity at the start of the working day. This way they can find out if there have been developments that need to be addressed promptly.

An intelligence source mentioned by several respondents is the Swedish national CSIRT, CERT-SE, hosted by MSB. When CERT-SE issues flash messages about serious vulnerabilities, these messages are generally acted upon. Respondent 17 said:

> [W]e try to listen to CERT-SE and when we get information from them, we try to check: is this a problem that we have? [R17]

Receiving information from CERT-SE could be seen as the benchmark minimum in intelligence gathering at Swedish administrative authorities. When CERT-SE speaks, cybersecurity employees at government authorities pay attention. The importance of MSB and its subsidiaries as a trusted information source for the public sector is in line with the findings presented by Andreasson et al. (2021).

When IT is outsourced, respondents report trusting their IT provider and their third-party providers to gather relevant intelligence:

> [T]here [is] a risk that [...] we trust our IT provider and their third-party providers, in the shape of Microsoft and third-party providers of security software [...] to follow this development and deliver something that is good enough for our purposes. [R1]

Here, the obligation to gather intelligence is informally transferred to the provider, which is recognized as a risk.

Participating in networks dedicated to security is another way of gathering intelligence. SNITS,[8] the state network for staff working with information security as their main task, was highlighted by several respondents. Respondent 2 explained how they utilize the network:

> If you have a question, you can always send it to the network and ask for a response or, sometimes, there are people who select what authorities to send specific questions to... [R2]

[8] For information about the SNITS network, see https://www.informationssakerhet.se/kompetensutveckling/natverk-for-offentliganstalda/.

Participating in this network gives access to persons working with similar issues and, through them, a wider pool of knowledge. The participants can learn from each other, collaborate on shared problems, and get inspiration.

For respondents at smaller authorities, where information security is a minor part of the job, there is no similar network, as Respondent 14 noted:

> But there is no network for all these small authorities[.] [R14]

When participating in larger digitalization networks for administrative authorities, respondents from smaller authorities say that the issues brought up there are not relevant to them and that their solution needs are on a quite different scale than for the larger authorities. This way, the smaller authorities lack such an arena for intelligence gathering.

In some of the respondents' networks, there are also people with more specialized knowledge about different threats and threat actors. Through these contacts, respondents can get access to solutions that they might not otherwise find through their own OSINT gathering. There is, to a certain extent, a willingness to share specialized knowledge about threat actors. As Respondent 5 put it:

> [I]f we get some kind of ransomware, we could get it confirmed that it is this group that has encrypted[.] [...] [T]hey usually use this so try to decrypt it like this. [R5]

Quite a few of the respondents have a background in the national defense and security authorities. Respondent 17 mentioned:

> We listen a bit to [the National Defence Radio Establishment], we listen a bit to [the Swedish Military Intelligence and Security Service][.] [W]hen you have been in those circles you have some connections... [R17]

There are advantages for respondents to have these informal network connections. They have an awareness of what these authorities do, and where the line is drawn for classified information. With this knowledge, they can navigate their contacts and know how to ask for the information they need in their current work.

Authorities that also handle protective security and signal protection have staff participating in external networks dedicated to those issues. Cooperating with them to disseminate knowledge about what they do and the information they have is important as their activities also have a bearing on the cybersecurity work carried out by the respondents. Input from protective security and signal protection is needed to get a more complete operational picture. Respondents reported diverging views on how well this cooperation works. Respondent 11 mentioned an intense collaboration to get a good overall picture:

> [W]hat are you doing over here that can impact the information security work, or vice versa. Protective security is a very good example as information security plays a part there, so it is a natural need to collaborate between the networks. [R11]

Another respondent works in an organization where the different branches involved in security have a more difficult time working together. Respondent 3 discussed protective security and information security:

> There is a history of viewing these as two separate issues. And that makes it difficult [...] [P]rotective security has been a separate silo and information security has been that other thing, which is not quite as important, so [...] protective security is more like...we do what we have always done. [R3]

This organization misses out on the benefits of coordinating the information security work with protective security as the responsible for protective security, in the respondent's view, is not interested in collaborating to solve issues related to information security. In this authority, they work in separate silos.

General media reporting also forms part of the intelligence gathering. Respondent 1 said:

> [W]hat is it journalists write about? When something actually has happened. That's not particularly preventive. [R1]

While this is accurate, general media reporting can still be helpful in obtaining initial information about threats and vulnerabilities and act as a prompt to investigate if the authority is at risk.

4.2.2 Technology

The second subtheme covers different aspects of technology usage for gathering information. While respondents did not go into the specifics regarding their technical protections, they discussed in general terms the technical solutions' place in their work and to what they pay attention.

Respondents addressed the importance of staying up to date on basic cyber hygiene efforts like patching and lifecycle management. Knowing what devices and what versions you have on your network is of great importance when determining what risks there are to the organization. Respondent 15 recalled discovering that Apple released out-of-band updates for old iOS units:

> [N]ow there were updates and then they are probably released because this is so darn serious. [R15]

Having this knowledge, R15 opened a ticket, investigated, found several units with this operating system at the authority, and took action to mitigate the risk.

Logs are mentioned as another important part of knowing what's going on. Several respondents recognized the importance of logs, but for Respondent 16, logs were an issue as they did not follow up on them:

> And internally I would say that the control is lower as we do not have any organized log checking, for example. [R16]

Logs are not fully utilized if they are not analyzed. Having access to logs is a basic step in understanding what is happening. With operations outsourced, logging is an important part to include in the SLA with the provider. Respondent 1 related:

> We have extensive requirements on logging of what happens in our networks [...] Also logging of the work of the providers and administrators [...] to be able to [...] go back and look at [them] when something actually has happened. [...] [W]e will never be able to protect ourselves against things happening. However, we can build security measures that help us understand what has happened. And then maybe prevent it in the future. [R1]

These logs are not used pro-actively, but rather as a tool after the fact. However, the respondent shows that they wish to move in a more pro-active direction.

Another technical solution for knowing what's going on mentioned by respondents is dashboards, from the importance they play in their daily work to the desire to have dashboards tailored to their own authority. Respondent 6 said that the status page of their dashboard is the first thing they look at in the morning for guidance on the state of IT. The supplier-provided dashboard for their IT-environment has a score-based system. Respondent 6 said:

> [Y]ou get this list of things, and it is prioritized by how much you can lower this vulnerability score. I mean, what is it that raises your security the most, and then we check them off. [R6]

The dashboard and the scoring system could be seen as a gamification of security, where the work is guided by reaching as low a score as possible. It is also the supplier-provided scoring system and evaluation of the risks that shape the security work, and not the respondent's own evaluation.

Another respondent wanted to set up their own dashboards. Deciding what the important security indicators are, and then following them up in an automated fashion is a function desired by Respondent 8:

> [I] would [like] to have a dashboard with different kinds of established monitoring points and then basically green, red, and yellow. [R8]

This kind of dashboard allows for the authority to establish their own business-as-usual baseline with associated monitoring, and use that as a traffic light system to signal the state of the environment in a simple way. This would support the respondent's CSA.

Respondent 19 expressed that they miss having certain tools and dashboards that would give them better situation awareness:

> What I miss is actually better tools for log analysis and better tools to gather endpoint data and different vulnerabilities [...] [and] some nice dashboards to look at it. [...] [T]hen I would be more comfortable that we have a better understanding of what's going on. [R19]

The respondent has a good idea of what would be required for them to have an improved situation awareness, but why this has not yet materialized is unclear.

4.2.3 Organization

Organization is the third subtheme, and this theme concerns information stemming from knowledge concerning the administrative authority. Deep-seated knowledge about the organization provides a solid foundation when trying to understand what's going on.

Respondent 6 recalled instances when automatic alarms are triggered by suspicious user activity, but where the respondent's experience tells them that this activity is in line with their users' normal behavior. They pointed out:

> But there is nothing, so to speak, that you know from the start that it is okay; that is something you need to build up experience of. [R6]

The respondent makes it clear that experience about the organization is needed, and also that having that experience is possible due to working in a smaller authority with only two persons working with IT:

> [W]e help each other out, but it is not bigger than it can be grasped by one person. And that is a very big advantage. [R6]

In this case, the size is an advantage as the two people working with IT are familiar with the behavior of other employees and the providers they have. This kind of intimate knowledge is almost impossible to achieve in larger organizations.

Another angle on organizational knowledge is understanding the level of exposure of the authority and its employees. Respondent 10 mentioned they had hired an external firm to gather OSINT on employees:

> Because that's the start of all...attacks[.] [I]f you are a professional [...] you put a lot of time into mapping [...] individuals... [R10]

Having knowledge about employee exposure can form a starting point for working with exposure-related risks at the authority. Dark web monitoring could be part of intelligence gathering and also be an efficient way of getting management attention if the exposure is large.

Tracking incidents is one way of knowing what's going on at the authority. However, Respondent 11 mentioned the difficulty of getting the full picture when there are several authorities sharing an IT department, and that there is a challenge to get access to incident information pertinent to their own authority:

> [T]he overall incident picture is with the IT department [...] [a]nd it is on our to-do list to try to get access to that piece of the puzzle. [R11]

Here, the information about incidents is not distributed optimally. Parts of the organization do not get access to information needed for making decisions for protecting their information. Better processes for information sharing are required for the respondent to achieve the CSA that they expect.

When IT operations are outsourced, authorities are dependent on their suppliers to report when incidents happen. Respondents 16, 14, and 13 reported different experiences with their suppliers. Respondent 16 said:

> [T]hey should report according to our agreements [...] but perhaps that has not worked out 100%. [R16]

There is also the question of what happens after the supplier reports an incident. Respondent 14 recalled communicating with a supplier:

> [T]hey told us what measures they had taken. That's really enough for us, that we know that they have done so. [R14]

Respondent 13 felt confident regarding the work of their suppliers, but said:

> [T]here is always room for improvement. Add more requirements, one can ask for more reports[.] [R13]

Having sufficient information about incidents is needed for good CSA. However, if reports are not filed or followed up on, as indicated by Respondent 16, there is a risk to security. If not all incidents are reported, making informed decisions about security measures is harder. Not following up further than accepting the actions taken by the provider, as stated by Respondent 14, also poses some risks. For Respondent 13, there is no mention of what to do with possible additional reports.

4.2.4 Compliance

The fourth subtheme covers compliance elements. This concerns information-gathering stemming from using regulations and standards, i.e., the ISO 27001 standard and the regulations issued by MSB, as a benchmark for security. Measuring how well the authority lives up to these is a way to convey a common operational picture to the management of the authority. Respondent 11 stated:

> [I] know what's going on when I can [...] use the MSB regulations and the ISO standard and put green, yellow, or red. Because that's what my director general, management, is asking for. In an easily understandable way, how are we doing here? What should we focus on? So it is my goal to be able to provide that [...] common operational picture to management. [R11]

For this authority, the status serves as a common operational picture used for making strategic decisions about the authority's future actions on information security, showing a more mature approach to information security.

For Respondent 3, living up to the standard is the goal they strive toward. However, they perceived there is no clear route on how to reach the benchmark, thus allowing for creative ways to do so:

> That's kind of the balance between having very predictable processes and being creative and solving a problem toward a specified goal instead of through specific steps. [T]he standard is the benchmark, and reaching that benchmark can be done in many different ways. [R3]

This highlights that there is no universal solution for complying with the regulations, and the guidelines leave the implementation to the authorities.

4.3 Incident experience

This theme concerns respondents' experience of incidents at the authorities. The theme is divided into two subthemes: (i) information security incidents at the authority, and (ii) experience of COVID-19.

4.3.1 Incidents at the authority

The first subtheme, information security incidents at the authority, was a subject the respondents discussed with caution. Respondent 2 expressed:

> I dunno if I can share anything [...] I can share phishing attacks and things like that, that have happened historically, [...] but attacks, in general, is not something I can share. [R2]

The respondent is ambivalent about sharing their experience of incidents apart from incidents common enough not to implicate the authority specifically. A cautious approach could be due to an unwillingness to discuss particular weaknesses the authority has had in its cybersecurity stance or that this type of information would be classified as secret under the Public Access to Information and Secrecy Act (SFS 2009:400).

A similar hesitancy in speaking about incidents as shown by Respondent 2 can be seen in Respondent 7's comment:

> I can't really speak about an actual event. [R7]

and then later, the respondent mentioned:

> [W]ell, it has happened on occasion that people have clicked on links you should not click on. [R7]

but nothing more specific.

An unwillingness to discuss incidents, apart from them possibly being classified as secret, could be an indication of not wanting to expose oneself professionally. Admitting to having experienced incidents could be felt to reflect badly on the respondent. However, not sharing incident experience keeps others from learning from that experience.

Incidents caused by human error or where humans are used as the attack vector were mentioned more freely, e.g., employees sending emails to the wrong addressee [R16], or interacting with emails containing ransomware or phishing links [R13]. Those incidents might be easier to discuss as the error lies with the user, and the incident does not reflect poorly on the respondent. Such incidents are par for the course in most organizations.

Other types of incidents mentioned were incidents that affected a shared system among many authorities in Sweden [R5], availability issues arising from external users downloading public records affecting availability [R10], or possible GDPR incidents in a supplier's system [R13]. All these incidents are examples of incidents where the authorities' own cybersecurity are not directly at fault in a technical sense, but rather in an organizational or requirement-specification sense.

Some respondents mentioned that learning from incidents is important. This learning, however, takes different forms. Respondent 13 mentioned following up on incidents with their operating supplier:

> What we followed up was actually with our IT operations provider because it is they [...] who do the practical work. [R13]

Here the supplier is an integrated part of the security work when it comes to understanding what has happened, and both organizations benefit from understanding the incident.

Learning from incidents can also be viewed in a longer perspective, where lessons learned form the basis for what should be prioritized in the future security work of the authority. Respondent 7 talked about conclusions drawn from incidents:

> [W]e have drawn these conclusions and we try to include them as controls and put them in a three-year plan [...] and then we have the director general decide on a yearly plan with the things we prioritize this year. And there's where the lessons learned come in as one type of control[.] [R7]

Learning from past incidents as a factor in the decision-making for strategic information security, shows maturity in the systematic information security work at the authority.

There is a challenge in learning from incidents when the incidents have occurred in IT systems shared by several authorities. Respondent 11 stated:

> Yes, lessons learned have taken place, but I do not know how exactly [...] they will affect our local work at the authority, and that is something we need to work on. [R11]

There have been lessons-learned sessions, but not all who would benefit from the knowledge have been able to take part. For distributed authorities, it is important that what has been learned does not stay at the central level of the authorities sharing a system, but that all levels of the organization can benefit.

4.3.2 COVID-19 as incident

The COVID-19 pandemic is a subtheme on its own. This event is a specific incident that all respondents have experienced and had to deal with in their work. Respondent 7, who said they could not discuss any real incidents, mentioned:

> Corona! The pandemic is an event in itself. [R7]

The pandemic as an event is unfolding over a long period of time, influencing how work is carried out at the authorities, and challenging the security at the authorities in different ways.

At the beginning of the pandemic, the Swedish Public Health Agency issued an authority regulation and general advice stating that, wherever possible, all employees should work from home (HSLF-FS 2020:12 2020). Respondents mentioned that adjusting to the regulation to work from home was easy as the authorities already had the digital tools necessary to work from home in place, and were used to collaborating with other authorities using digital tools. As expressed by Respondent 3:

> So that transition has been fairly easy I think. [R3]

The pandemic brought an uptake in the use of tools across the organization. Working from home was easy in the sense that the digital tools were available; it was a matter of staff fully utilizing the approved tools available to them. However, employees working from home carry other types of risks than when working at the office. Respondents bring up risks with employees working outside the authority perimeter. The main risk mentioned was employees using WiFi outside the control of the authority. Respondent 15 pointed out potential risks they saw with employees connecting to their home networks:

> There are teenagers and there are smart lights and fridges and garage door openers. [R15]

These represent different kinds of risks as teenagers might have an online behavior different from employees, and the smart devices could have vulnerabilities that attackers could exploit, and through these, the employee devices could be compromised.

Trying to mitigate the risk with employees working outside the office included having a clear policy for working from home, where the home network was considered to be approved whereas a public WiFi was not, and distributing mobile WiFi to employees deemed working with more sensitive information (though not information classified as secret). It is not only the employees' endpoints being outside the authority that pose a risk; it is also the employees themselves. Respondents brought up that they had reminded employees working outside of the office of secrecy issues, not participating in online work meetings that could be overheard or keeping documents at home. Respondent 12 queried:

> Do we process sensitive information in our role as a case officer? Is there someone in the household or where we are working who can hear this or see documents relating to our role and not to our private life? [R12]

While the respondents generally perceived the authority had digital tools supporting working from home, several of them mentioned that the need for different tools arose when collaborating across organizations. Some respondents mentioned that there were frustrations when employees could not freely use any tools available. Restrictions to allow new tools do not stem solely from a security perspective, as Respondent 3 highlighted:

> [T]he frustration with "why can't we use any tools that we want" is not only about security, but also about procurement and financial issues. We can't just purchase everything we feel like, without thinking about management and how it will be used. [R3]

The established and required procedures for procuring and implementing new tools were challenged during this crisis.

4.4 Summary of results

The following section synthesizes the results outlined in the main themes presented in detail in Sects. 4.1–4.3.

Organizational conditions: The organizational conditions theme is categorized into three subthemes relating to individual, authority, and national conditions. The staff involved in cybersecurity at the administrative authorities have varied mandates in their roles, ranging from advisory subject matter experts to staff with a wide mandate, and even staff who will act without a mandate in the event of serious incidents. At the organizational level, management attitudes to cybersecurity vary significantly, and a change in leadership, such as a new director general, can fundamentally alter an authority's approach to cybersecurity. The MSB regulations (see Sect. 2.1) are seen as serving as a facilitator driving the formalization of information security work by clearly delineating management responsibilities. However, the support offered at the national level does not meet the needs of the cybersecurity staff; smaller authorities struggling with implementing systematic information security need help with the basics, while other authorities express a need for access to more detailed government cyberthreat intelligence.

Information elements: There are various sources for information elements that cybersecurity staff rely on to form the CSA required for their role. These information element sources form four subthemes: intelligence, technology, organization, and compliance. The intelligence subtheme relates to information elements originating outside the organization. Some respondents report insufficient time to dedicate to this area. CERT-SE is widely regarded as a trusted source of intelligence and is considered the benchmark minimum for intelligence gathering. Additional intelligence sources contributing to CSA include the SNITS network for government authority information security staff, informal private networks, and media outlets. The technology subtheme concerns information elements stemming from technology. Staff look at basic hygiene factors such as patching and life-cycle management, to understand what they have in their environment. Logs are seen as another important input, but these are not used proactively, but rather to figure out what has happened after the fact. Dashboards visualizing key parameters are available to few, but having access to customizable dashboards for individual needs is a desired tool for improving CSA. The organization subtheme outlines information elements stemming from the administrative authority. Smaller authorities with long-term staff have the experience and overview to quickly determine what events constitute business as usual for their authorities. Another aspect of the organization is information elements regarding the exposure of the authority and their employees, and what level of risk that might bring. There are also hindrances to CSA stemming from the organization when required information elements are not disseminated between different departments. The compliance subtheme deals with compliance-related information elements that stem from assessing the authority's adherence to ISO 27001 and MSB regulations. Compliance with these is seen as an aspirational goal, and measuring the organization's performance against these standards can form a COP to support the decision-making progress regarding what actions to take next.

Incident experience: Incident experience is explored in two subthemes: incidents at the authority and COVID-19 as incident. Exploring incident experience proved challenging due to a general reluctance to discuss specific incidents occurring at the administrative authorities that could stem from secrecy issues or not to implicate oneself professionally. Nevertheless, incidents resulting from human error were discussed more openly. These included common occurrences such as emails to the wrong addressee or falling victim to phishing attempts, which were widespread. The COVID-19 pandemic was in itself experienced as an incident, bringing risks to cybersecurity through the use of new, or uptake of existing, digital tools, employees outside the perimeter, and working from shared wireless networks.

5 Discussion

The purpose of this study has been to characterize the conditions for cybersecurity work at Swedish administrative authorities. This was explored by investigating organizational conditions, information elements for CSA, and incident experience. Empirical material from semi-structured interviews with 17 respondents from Swedish administrative authorities provides a foundation for the discussion and conclusions.

When the empirical material was analyzed, it was clear that the conditions for cybersecurity work differed considerably among the respondents. As can be seen in Sect. 4, it varies at the individual, authority, and national levels. The results show that there are differences in capabilities between the smaller and larger authorities. A small authority can have a single jack-of-all-trades IT person, dealing with all things related to IT, including cybersecurity, on a small budget, whereas a large authority can have an entire IT department, different cybersecurity specialists, and larger resources. Is it possible for staff working with cybersecurity at administrative authorities to achieve the CSA they require under these conditions?

Cyber situation awareness among operators in the context of a SOC has been the subject of several studies (see, e.g., Ofte and Katsikas 2023). CSA in the wider context of an organization has not been given the same attention. However, it is reasonable to assume that the relevant information depends on the role of the respondent—someone working with incident triage needs another kind of CSA than someone working with legal compliance (see, e.g., McKenna et al. 2015; Gutzwiller et al. 2020). Thus, the respondents require information stemming from a broader context than can be had from internal monitoring of the organizational network. This is in line with the organizational perspective on CSA suggested by Franke et al. (2022, Section 4). In the present study it is found that the information elements needed by respondents are, in several cases, not available to them. As the results show, information relevant to respondents' CSA can reside at another department in the organization, with another authority in the case of shared systems, with third-party providers in the case of outsourced IT operations; required intelligence gathering might not be given the attention needed to operationalize it (Ainslie et al. 2023), or information about threat actors targeting Swedish national interests might remain within the national intelligence community.

When looking at national-level support offered to the administrative authorities, the respondents brought up different government support aspects that do not meet their perceived needs. These needs vary in nature, ranging from assistance with how to comply with national regulations, to the need for more advanced security intelligence reports about potential threat actors. This suggests that the administrative authorities' cybersecurity staff would benefit from diversified support that takes the varying conditions into account. The competent authorities, like MSB, might ought to tailor information about regulations so that different audiences can quickly and easily find what is most relevant to their particular circumstances.

In addition, the competent authorities responsible for information security and protective security, respectively, have the opportunity to identify where their areas overlap and point out these in their respective guidelines, thus avoiding different security "stovepipes" and leveraging synergies where possible and appropriate. Today, this is not working smoothly for all concerned authorities. As mentioned above, more collaboration between the competent authorities might ease this intra-authority collaboration. The established National Cyber Security Centre (NCSC) is an effort to gather the authorities involved in cybersecurity at the national level, to work together to provide advice and support concerning threats, vulnerabilities, and risks.[9] This provides an opportunity for the NCSC to be able to provide a more holistic take on national cybersecurity.

When discussing incidents, it should be noted that the term "incident" was not defined during the interviews. The interviewer and the respondents might have different ideas about what constitutes an incident. In addition, there is the legal context of what constitutes an incident that should be reported to a competent authority—for a brief introduction to the complexity of incident reporting in the Swedish context, see, e.g., Andreasson and Fallen (2018) and the MSB annual report on IT incidents (MSB 2022). For a more thorough legal analysis, including possible conflicts between the different laws on mandatory incident reporting, see Naarttijärvi (2019). Which aspect of confidentiality, integrity, and availability (CIA) is affected, or how severely the authority is affected, are among the factors deciding whether an incident should be reported or not and to what competent authority. For example, if the availability of an essential service or digital service is affected for a certain time period and for a certain number of people, it constitutes a reportable incident according to the NIS Directive, and MSBFS 2020:7 (2020) requires an incident report if, for example, CIA of information in need of extended protection is affected, or if the incident has affected the authority's ability to perform its mission. Thus, sorting out what constitutes a reportable incident is nontrivial.

While it is widely accepted that one can learn from reviewing incidents, few respondents wanted to discuss specific incidents, as reflected on in Sect. 4.3. Also, it should be noted that only two respondents mentioned making use of white-hat hackers, or penetration testing, as a means to finding vulnerabilities, during the interviews. The unwillingness to discuss incidents could be due to a reluctance to expose the authority, or that incidents could reflect poorly on the respondent's competency. However, incidents originating from the user or ubiquitous events like phishing, were mentioned more freely.

It is worth mentioning, though, that, after system failures, user mistakes make up the second most frequently reported incident category, nearly twice as large as the third category, in MSB's annual incident report (MSB 2022). For MSB to provide an accurate common operational picture over incidents affecting Sweden, they need to have high-quality incident data reported to them. This is not always the case—see, e.g., the study by Franke et al. (2021) on the Swedish NIS reporting, which finds some aspects of reports to be incomplete, and concludes that operators may need to be trained to make the data more useful. The importance of sharing and receiving information from MSB for organizations' COPs is in line with the findings by Varga et al. (2018, Sections 5.1.5 and 5.1.7), where MSB is frequently mentioned as both source and recipient of information elements in cyber COPs. Also, as mentioned by one respondent in Sect. 4.2.4, the respondents generally feel that they have sufficient CSA when they have the information required to provide a COP to their management showing how they are doing in relation to the MSB regulations. From this strategic COP, they decide on future actions.

Some respondents work at administrative authorities where IT operations are outsourced. Having a supplier running IT operations could lead to improved cybersecurity. A supplier could have very good technical monitoring, enabling them to detect incidents, but there is also the aspect that CSA at the authority could decrease significantly. Also, without meticulous service level agreements, questions might arise about who really has the responsibility for the authority IT operations. While MSB regulations state that administrative authorities should conduct risk-based information security work in accordance with the ISO/IEC 27001:2017 standard, and outsourcing IT operations is one way of handling risk by sharing the risk, is the outsourcing of administrative authority IT operations compliant with the legal framework?

Administrative authorities share systems to varying degrees. This is one reason for administrative authorities to strive toward a high baseline level for cybersecurity. The results show that sharing systems carry some risk, especially when sharing authorities do not make the same assessment of the required level of protection for the information shared in the system. Sharing systems could also lead to questions about where responsibility lies. It is worth repeating that shared systems could also be detrimental to CSA when there are no functioning processes for information sharing in place.

6 Conclusions

This work highlights the complexities of achieving CSA in the cybersecurity efforts of Swedish administrative authorities. Through 17 semi-structured interviews, the study reveals the diverse methods employed by cybersecurity staff to gather relevant information from various sources during different timeframes, essential for understanding past, present, and future cyberthreats. A significant finding is that the necessary information elements are

[9] NCSC, https://www.ncsc.se/, comprises Swedish Defence Materiel Administration (FMV), National Defence Radio Establishment (FRA), Swedish Defence Research Agency (FOI), Swedish Armed Forces, Swedish Civil Contingencies Agency (MSB), Swedish Police, Swedish Post and Telecom Authority (PTS), and Swedish Security Service.

often inaccessible, impeding the staff's ability to attain the desired CSA.

The research underscores the need for customized guidelines and threat intelligence tailored to specific roles and authorities, emphasizing that CSA requirements vary widely. Additionally, the study advocates for the development of situation-specific COPs and improved incident reporting systems to enhance information sharing at the national level. These recommendations aim to provide authorities with a more comprehensive understanding of their cybersecurity landscape, both locally and globally, thereby strengthening their overall CSA and response capabilities.

As mentioned in Sect. 1, this study served to answer the following overarching research question: what characterizes the conditions for cybersecurity work at Swedish administrative authorities? In the following, conclusions related to the study's three sub-questions are presented, recommendations for cybersecurity work are given, and, finally, future work is suggested. The first sub-question concerned the organizational conditions for cybersecurity work at the individual, authority, and national levels. The empirical material showed a large variety of conditions expressed by the respondents. At the individual level, different roles with differing mandates are involved in cybersecurity work. At the authority level, the respondents reported diverging management attitudes to cybersecurity, diverse abilities to discover incidents, and differing maturity in the organization of cybersecurity work. Finally, at the national level, respondents expressed that the national-level support could be improved in several ways. Based on the analysis, a few key recommendations can be made:

- guidelines for action and threat intelligence ought to be tailor-made to suit different roles and authorities, and
- incident reporting systems should facilitate reporting of the information elements relevant for contributing to a national COP.

The second sub-question concerned what cybersecurity staff do to acquire the CSA required for their role. The respondents gathered different types of information elements from different types of sources, within and outside the authority, that they deemed relevant for their role. The information elements required cover diverse timeframes, for understanding the past, present, and planning for the future. In some cases, the information elements they required were not available to them, meaning that they could not achieve the desired CSA. The following key recommendations can be made:

- different roles and agencies have different CSA requirements, and therefore situation-specific COPs ought to be constructed to fit those needs, and
- authorities should be able to put their situation in a global context, and therefore should be given access to relevant parts of a national COP.

The third sub-question concerned the incident experience of cybersecurity staff. While the respondents expressed having experienced incidents, the results show that there was a reluctance to discuss specific incidents other than commonplace events originating with human error. COVID-19 as incident was an experience all respondents shared, and the overall view was that the transition to working from home was easy. The main concern of the respondents was employees working outside the authority perimeter, where the respondents had little control over networks. A key recommendation is the following:

- cross-agency lessons-learned activities should be conducted in order to facilitate a learning culture.

The results clearly show the diversity among staff responsible for cybersecurity at Swedish administrative authorities. One direction for future research in order to highlight the diverse roles and needs could be to create personas (Cooper 2004) representative of the respondents at Swedish administrative authorities based on the extensive empirical material collected. The personas could be used as a communication tool by the competent authorities to create an understanding of the diverging needs of the cybersecurity employees, who are both at the receiving end of their regulations and guidelines, and providers of information for COPs. In addition, personas can also support the development of tailored systems for reporting, or be used to create tailored COPs.

Another possibility is to build on this study to investigate the conditions for cybersecurity at the county council and municipal level to expand the body of knowledge of the conditions at all levels of the Swedish public sector. As the cyberattacks targeting Swedish interests during recent times show, as discussed in Sect. 1, all levels of government are targeted and, hence, need a high level of cybersecurity in addition to employees with a high level of CSA.

A Interview guide

This interview guide is loosely structured so that the interviewer tried to ensure that when a question was asked, the respondent touched upon the areas outlined in the subsections. If the respondent did not address the areas of interest, the interviewer had the freedom to formulate a follow-up question or use the suggestion provided, depending on the context and time restrictions. The interview guide is translated from Swedish.

A.1 Guide

1. Can you tell me a bit about your background and your work?
   - (a) Background
     - (i) Educational background
     - (ii) Previous experience
   - (b) Role
     - (i) Current role
     - (ii) Role entails
     - (iii) Time in role
   - (c) Cybersecurity connection
     - (i) Place in authority cybersecurity work
     - (ii) Part of full-time
     - (iii) View of cybersecurity
   - (d) Knowing what's going on
     - (i) How do you know what's going on?
2. Can you describe what you do at the authority level to "know what's going on"?
   - (a) Knowing what's going on
     - (i) What details are attended to
     - (ii) Reports from other authorities
     - (iii) Intelligence
     - (iv) Who partakes of intelligence
   - (b) Organization
     - (i) Organization of information security work
     - (ii) Clear mandates/authority
   - (c) Ability
     - (i) How would you describe the authority's ability to rapidly discover and assess situations and deviations?
     - (ii) If you have experienced a situation/deviation, how do you assess if it needs to be reported externally?
     - (iii) What departments/roles are involved?
   - (d) Respondent
     - (i) Do you have the authority to take drastic measures to influence a situation?
3. What details are you paying special attention to in order to know what's going on?
   - (a) Why these?
   - (b) How do you contextualize these details?
4. Can you tell me about a situation you have experienced at the authority?
   - (a) Discovery
     - (i) How did you discover the situation?
     - (ii) Who was involved?
     - (iii) When did you get involved?
   - (b) Assessment
     - (i) How did you assess the situation?
   - (c) Preparation
     - (i) Was this a situation you had prepared for?
     - (ii) Why had you prepared for a situation like this?
   - (d) Response
     - (i) How was the situation resolved?
   - (e) Lessons learned
     - (i) Did you follow up on the situation?
     - (ii) How?
     - (iii) Did it lead to any measures taken?
   - (f) Report
     - (i) Did you report the situation?
     - (ii) To whom?
5. If we were to try to define "what's going on" from your perspective, how would you describe it?
6. If you reflect on the COVID-19 pandemic, how have you handled risks/threats with working from home?
   - (a) Observations
7. Before we end this interview, is there anything else that you would like to add that you think would be useful for me to know?

B Codes and corresponding themes

See Table 2.

Table 2 This table contains the final themes and the codes related to those themes

Theme	Subtheme	Code	Respondents	Code freq.
Organizational conditions	Conditions of the respondent’s role	Role mandate	14	18
		Role entails	17	34
		Challenges in role	9	33
	Conditions at the administrative authority	Infosec clear responsibility	16	19
		Internal collaboration	5	13
		Authority ability to detect incidents	15	15
		Management attitude	11	16
		Outsourced IT	5	8
	Conditions of national-level support	National-level support	8	15
Information elements	Intelligence	CERT-SE	7	10
		Threat	5	12
		Threat actors	7	17
		Supplier intel	8	10
		Media	12	17
		Networking	10	17
		Intelligence gathering	15	33
		Reports	5	7
		Trends	3	8
	Technology	Deviations	5	11
		Dashboard	3	4
		Logging	3	3
		Technical protections	10	21
		Updates	6	8
	Organization	Incidents	9	19
		Information classification	8	10
		COP	4	6
		Supplier/SLA	8	31
		Employee training	10	20
		Risk awareness	7	14
		Steering documents	5	6
		Knowledge of the organization	15	57
	Compliance	ISO 27000	5	7
		MSB regulations	8	16
Incident experience	Incidents at the authority	Incident at authority	16	20
		Preparedness for incident	8	8
		Lessons learned	11	13
	COVID-19 as incident	Employees outside the perimeter	11	14
		New needs	9	11
		Increased use of digital services	3	3
		Increased risk	7	9
		Increased capacity need	4	5
		Adaptation to COVID-19	9	10
		Tool requests	6	7
		Reminding employees about secrecy	3	3
		Facilitating digitalization	3	3

The column *Respondents* contains the number of respondent interviews where the code occurs, and the column *Code freq.* contains the number of text extracts that have the code

Acknowledgements This work was supported by the Swedish Armed Forces. The authors thank Stefan Varga, KTH Royal Institute of Technology and the Swedish Armed Forces, for assistance in the interview guide development phase, as well as the respondents taking part in the survey.

Author contributions Conceptualization: A.A., H.A., J.B., and U.F. Methodology: A.A., H.A., J.B., and U.F. Formal analysis: AA., H.A., J.B., and U.F. Investigation: A.A. Data curation: A.A. Writing - original draft: A.A., H.A., J.B., and U.F. All authors approved the final version of the manuscript.

Funding Open access funding provided by Royal Institute of Technology.

Data availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper. The empirical material analyzed in the current study is not publicly available in order to protect participant anonymity. All participants in this study gave informed consent in accordance with Swedish law.

References

Ainslie S, Thompson D, Maynard S et al (2023) Cyber-threat intelligence for security decision-making: a review and research agenda for practice. Comput Secur 132:103352. https://doi.org/10.1016/j.cose.2023.103352

Amankwah-Amoah J, Khan Z, Wood G et al (2021) COVID-19 and digitalization: the great acceleration. J Bus Res 136:602–611. https://doi.org/10.1016/j.jbusres.2021.08.011

Andreasson A, Fallen N (2018) External cybersecurity incident reporting for resilience. In: Zdravkovic J, Grabis J, Nurcan S et al (eds) Perspectives in business informatics research. Lecture notes in business information processing. Springer, Cham, pp 3–17. https://doi.org/10.1007/978-3-319-99951-7_1

Andreasson A, Artman H, Brynielsson J et al (2020) A census of Swedish government administrative authority employee communications on cybersecurity during the COVID-19 pandemic. In: Proceedings of the 2020 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM 2020). IEEE, Piscataway, NJ, pp 727–733. https://doi.org/10.1109/ASONAM49781.2020.9381324

Andreasson A, Artman H, Brynielsson J et al (2021) A census of Swedish public sector employee communication on cybersecurity during the COVID-19 pandemic. In: 2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, Piscataway, NJ, pp 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478241

Artman H, Wærn Y (1999) Distributed cognition in an emergency co-ordination center. Cogn Technol Work 1(4):237–246. https://doi.org/10.1007/s101110050020

Ask TF, Kullman K, Sütterlin S et al (2023) A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. Front Big Data. https://doi.org/10.3389/fdata.2023.1042783

Atzeni A, Cameroni C, Faily S et al (2011) Here's Johnny: a methodology for developing attacker personas. In: 2011 sixth international conference on availability, reliability and security (ARES 2011), pp 722–727. https://doi.org/10.1109/ARES.2011.115

Baumard P (2017) Cybersecurity in France. SpringerBriefs in cybersecurity. Springer, Cham. https://doi.org/10.1007/978-3-319-54308-6

Boeke S (2018) National cyber crisis management: different European approaches. Governance 31(3):449–464. https://doi.org/10.1111/gove.12309

Braun V, Clarke V (2006) Using thematic analysis in psychology. Qual Res Psychol 3(2):77–101. https://doi.org/10.1191/1478088706qp063oa

Brynielsson J, Franke U, Tariq MA et al (2016a) Using cyber defense exercises to obtain additional data for attacker profiling. In: Proceedings of the 14th IEEE international conference on intelligence and security informatics (ISI 2016). IEEE, Piscataway, NJ, pp 37–42. https://doi.org/10.1109/ISI.2016.7745440

Brynielsson J, Franke U, Varga S (2016b) Cyber situational awareness testing. In: Akhgar B, Brewster B (eds) Combatting cybercrime and cyberterrorism: challenges, trends and priorities. Advanced sciences and technologies for security applications. Springer, Cham, chap 12, pp 209–233. https://doi.org/10.1007/978-3-319-38930-1_12

Caruson K, MacManus SA, McPhee BD (2012) Cybersecurity policy-making at the local government level: an analysis of threats, preparedness, and bureaucratic roadblocks to success. J Homel Secur Emerg Manag. https://doi.org/10.1515/jhsem-2012-0003

Cavelty MD (2014) Cybersecurity in Switzerland. SpringerBriefs in cybersecurity. Springer, Cham. https://doi.org/10.1007/978-3-319-10620-5

Chałubińska-Jentkiewicz K (2022) Cybersecurity as a public task in administration. Springer, Cham, pp 191–208. https://doi.org/10.1007/978-3-030-78551-2_13

Comfort LK (2007) Crisis management in hindsight: cognition, communication, coordination, and control. Public Admin Rev 67(1):189–197. https://doi.org/10.1111/j.1540-6210.2007.00827.x

Conti G, Nelson J, Raymond D (2013) Towards a cyber common operating picture. In: 2013 5th international conference on cyber conflict (CYCON 2013). IEEE, Piscataway, NJ, pp 1–17

Cooper A (2004) The inmates are running the asylum: why high-tech products drive us crazy and how to restore the sanity, 2nd edn. Sams Publishing, Indianapolis

Council of the European Union (2016) Council regulation (EU) no 679/2016 (GDPR). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679

Dayaratne TT, Jaigirdar FT, Dasgupta R et al (2023) Improving cybersecurity situational awareness in smart grid environments. In: Haes Alhelou H, Hatziargyriou N, Dong ZY (eds) Power systems cybersecurity: methods, concepts, and best practices. Springer, Cham, pp 115–134. https://doi.org/10.1007/978-3-031-20360-2_5

Department for Digital, Culture, Media and Sport (2022) UK digital strategy. Policy paper, Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1089103/UK_Digital_Strategy_web_accessible.pdf

Endsley MR (1995) Toward a theory of situation awareness in dynamic systems. Hum Fact 37(1):32–64. https://doi.org/10.1518/001872095779049543

Endsley MR (2015) Situation awareness misconceptions and misunderstandings. J Cogn Eng Decis Mak 9(1):4–32. https://doi.org/10.1177/1555343415572631

European Commission (2021) EU countries commit to leading the green digital transformation | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/news/eu-countries-commit-leading-green-digital-transformation

European Commission (2022) Digital Economy and Society Index (DESI) (2022). https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022

Frandell A, Feeney M (2022) Cybersecurity threats in local government: a sociotechnical perspective. Am Rev Public Admin 52(8):558–572. https://doi.org/10.1177/02750740221125432

Franke U, Brynielsson J (2014) Cyber situational awareness: a systematic review of the literature. Comput Secur 46:18–31. https://doi.org/10.1016/j.cose.2014.06.008

Franke U, Turell J, Johansson I (2021) The cost of incidents in essential services—data from Swedish NIS reporting. In: 16th international conference on critical information infrastructures security (CRITIS 2021). Springer, Cham, pp 116–129. https://doi.org/10.1007/978-3-030-93200-8_7

Franke U, Andreasson A, Artman H et al (2022) Cyber situational awareness issues and challenges. In: Moustafa AA (ed) Cybersecurity and cognitive science. Academic Press, pp 235–265. https://doi.org/10.1016/B978-0-323-90570-1.00015-2

Government Offices of Sweden (2017) A national cyber security strategy. Tech. Rep. Skr. 2016/17:2013, Regeringskansliet. https://www.government.se/legal-documents/2017/11/skr.-201617213/

Gutzwiller RS, Dykstra J, Payne B (2020) Gaps and opportunities in situational awareness for cybersecurity. Dig Threats Res Pract 1(3):1–6. https://doi.org/10.1145/3384471

Hatcher W, Meares WL, Heslen J (2020) The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. J Cyber Policy 5(2):302–325. https://doi.org/10.1080/23738871.2020.1792956

HSLF-FS 2020:12 Folkhälsomyndighetens föreskrifter och allmänna råd om allas ansvar att förhindra smitta av covid-19 m.m. [Regulation and general guidelines on everyone's responsibility to prevent the spread of COVID-19, etc.] (2020). https://www.folkhalsomyndigheten.se/contentassets/0ac7c7d33c124428baa198728f813151/hslf-fs-2020-12u.pdf

Husák M, Bajtoš T, Kašpar J et al (2020) Predictive cyber situational awareness and personalized blacklisting: a sequential rule mining approach. ACM Trans Manag Inf Syst 11(4):19:1–19:16. https://doi.org/10.1145/3386250

ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems. Requirements, (2017) Standard. International Organization for Standardization, Geneva, Switzerland

ITU (2020) Global Cybersecurity Index (GCI) 2020. International Telecommunication Union, Geneva, Switzerland. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Jiang L, Jayatilaka A, Nasim M et al (2022) Systematic literature review on cyber situational awareness visualizations. IEEE Access 10:57525–57554. https://doi.org/10.1109/ACCESS.2022.3178195

Lindström K (2022) Invasionen i Ukraina satte cyberkriget i fokus—2022 ett dystert år för it-säkerheten [The invasion of Ukraine put cyber war in focus—2022 a gloomy year for IT security]. Computer Sweden. https://computersweden.idg.se/2.2683/1.774368/invasionen-i-ukraina-satte-cyberkriget-i-fokus

McKenna S, Staheli D, Meyer M (2015) Unlocking user-centered design methods for building cyber security visualizations. In: Proceedings of the 2015 IEEE symposium on visualization for cyber security (VizSec 2015). IEEE, Piscataway, NJ, pp 1–8. https://doi.org/10.1109/VIZSEC.2015.7312771

Ministry of Finance (2022) National Strategy for Digitalisation—together in the digital development. Tech. rep., Ministry of Finance, Denmark. https://en.digst.dk/media/27861/national-strategy-for-digitalisation-together-in-the-digital-development.pdf

Moore T (2010) The economics of cybersecurity: principles and policy options. Int J Crit Infrastruct Prot 3(3–4):103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

MSB (2022) En inblick i Sveriges cybersäkerhet –Årsrapport it-incidentrapportering 2021 [An insight into Sweden's cybersecurity – Annual report cyber incident reporting 2021]. Publ. MSB1913, Swedish Civil Contingencies Agency, Karlstad, Sweden

MSBFS 2020:6 Föreskrifter om informationssäkerhet för statliga myndigheter [Regulation on Information Security for Government Agencies] (2020) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf

MSBFS 2020:7 Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter [Regulation on Security Controls for Information Systems for Government Agencies] (2020) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-7-foreskrifter-om-sakerhetsatgarder-i-informationssystem-for-statliga-myndigheter.pdf

MSBFS 2020:8 Föreskrifter om rapportering av it-incidenter för statliga myndigheter [Regulation on Incident Reporting for Government Agencies] (2020) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-8-foreskrifter-om-rapportering-av-it-incidenter-for-statliga-myndigheter.pdf

Munsinger B, Beebe N, Richardson T (2023) Virtual reality for improving cyber situational awareness in security operations centers. Comput Secur 132:103368. https://doi.org/10.1016/j.cose.2023.103368

Naarttijärvi M (2019) Rapporteringskrav vid incidenter i myndigheters informationssystem: i spänningsfältet mellan krisberedskap och rättighetsskydd [Reporting requirements for incidents in government information systems: navigating the tension between crisis preparedness and rights protection]. Juridisk Tidskrift 2:405–431

Nafees MN, Saxena N, Cardenas A et al (2023) Smart grid cyber-physical situational awareness of complex operational technology attacks: a review. ACM Comput Surv 55(10):215:1–215:36. https://doi.org/10.1145/3565570

Nederland Digitaal (2021) The Dutch Digitalization Strategy 2021. Tech. rep., Nederland Digitaal. https://www.nederlanddigitaal.nl/documenten/publicaties/2021/06/22/the-dutch-digitalisation-strategy-2021-eng

Norris DF, Mateczun L, Joshi A et al (2021) Managing cybersecurity at the grassroots: evidence from the first nationwide survey of local government cybersecurity. J Urb Aff 43(8):1173–1195. https://doi.org/10.1080/07352166.2020.1727295

Ofte HJ, Katsikas S (2023) Understanding situation awareness in SOCs, a systematic literature review. Comput Secur 126:103069. https://doi.org/10.1016/j.cose.2022.103069

Patton MQ (2002) Qualitative research & evaluation methods, 3rd edn. SAGE, London

Rampin R, Rampin V (2021) Taguette: open-source qualitative data analysis. J Open Source Softw 6(68):3522. https://doi.org/10.21105/joss.03522

Regeringskansliet (2017) För ett hållbart digitaliserat Sverige—en digitaliseringsstrategi [For a sustainable digitalized Sweden—a digitalization strategy]. Tech. rep., Statsrådsberedningen, https://www.regeringen.se/contentassets/c9bc0cd3a4374f9388e714ae7 fb1ec1d/for-ett-hallbart-digitaliserat-sverige-en-digitaliseringsstrategi.pdf

Salmon PM, Stanton NA, Walker GH et al (2008) What really is going on? Review of situation awareness models for individuals and teams. Theor Iss Ergon Sci 9(4):297–323. https://doi.org/10.1080/14639220701561775

Schallbruch M, Skierka I (2018) Cybersecurity in Germany. SpringerBriefs in cybersecurity. Springer, Cham. https://doi.org/10.1007/978-3-319-90014-8

SFS 2009:400 Offentlighets- och sekretesslag [Public Access to Information and Secrecy Act] (2009) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400

SFS 2015:1052 Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap [Ordinance on Crisis Preparedness and Supervisory Authorities' Actions at Heightened Alert] (2015) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052

SFS 2018:585 Säkerhetsskyddslag [Protective Security Act] (2018) https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585

Steen-Tveit K, Munkvold BE (2021) From common operational picture to common situational understanding: an analysis based on practitioner perspectives. Saf Sci 142:105381. https://doi.org/10.1016/j.ssci.2021.105381

Sterlini P, Massacci F, Kadenko N et al (2020) Governance challenges for European cybersecurity policies: stakeholder views. IEEE Secur Priv 18(1):46–54. https://doi.org/10.1109/MSEC.2019.2945309

Svantesson DJB (2023) Australia's cyber security reform—an update. Int Cybersecur Law Rev 4(3):347–350. https://doi.org/10.1365/s43439-023-00087-w

Tanaka S, Flores J (2023) Överbelastningsattacker mot flera svenska sajter [Distributed denial of service attacks on several Swedish sites]. https://www.dn.se/sverige/overbelastningsattacker-mot-flera-svenska-sajter/

Tariq MA, Brynielsson J, Artman H (2012) Framing the attacker in organized cybercrime. In: 2012 European intelligence and security informatics conference, IEEE, Piscataway, NJ, pp 30–37, https://doi.org/10.1109/EISIC.2012.48

Varga S, Brynielsson J, Franke U (2018) Information requirements for national level cyber situational awareness. In: 2018 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM). IEEE, Piscataway, NJ, pp 774–781. https://doi.org/10.1109/ASONAM.2018.8508410

Weber S (2017) Coercion in cybersecurity: what public health models reveal. J Cybersecur 3(3):173–183. https://doi.org/10.1093/cybsec/tyx005

Wirtz BW, Weyerer JC (2017) Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats. Int J Public Admin 40(13):1085–1100. https://doi.org/10.1080/01900692.2016.1242614

Wolbers J, Boersma K (2013) The common operational picture as collective sensemaking. J Conting Crisis Manag 21(4):186–199. https://doi.org/10.1111/1468-5973.12027