Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Cyber-threat perception and risk management in the Swedish financial sector

Stefan Varga[a,b,*], Joel Brynielsson[a,c], Ulrik Franke[a,d]

[a] KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[b] Swedish Armed Forces Headquarters, SE-107 85 Stockholm, Sweden
[c] FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden
[d] RISE Research Institutes of Sweden, SE-164 29 Kista, Sweden

ARTICLE INFO

Article history:
Received 17 September 2020
Revised 20 January 2021
Accepted 16 February 2021
Available online 20 February 2021

Keywords:
Situation awareness
Common operational picture
Cyber security
Information assurance
Risk management
Financial sector

ABSTRACT

The financial sector relies heavily on information systems for business. This study sets out to investigate cyber situation awareness in the financial sector in Sweden, by examining what information elements that are needed for a common operational picture, and exploring how key actors perceive cyber-threats.

Data was collected through a survey and a series of interviews with key actors in the sector in conjunction with a national level crisis management exercise. The data was then analyzed and contrasted to theory. Conclusions were drawn and results discussed. Finally, possible mitigation actions were suggested.

It was found that actors in the Swedish financial sector have a well developed crisis management working concept. However, information about rational adversaries that cause prolonged disturbances is possibly not collected, analyzed and utilized systematically. Much effort is put into ensuring that timely and relevant information from organizations is shared in an efficient manner. The sector perceives cyber-threats against the underlying financial infrastructure, as well as against IT service availability and data confidentiality, besides financial theft. The sector has particular concerns for the potential of reputational loss due to cyberattacks. There are also special concerns about the insider threat.

Respondents agree that risk management has to account for cyber risk. A possible route to enhance risk management practices is to ensure that cyber personnel is integrated in crisis management teams.

1. Introduction

The financial business is heavily reliant on technology (Shin, 2001). The sheer amount of transactions in modern days makes the functioning of the financial sector infeasible without automated networking, information processing, and telecommunication services. As predicted already in 1984 by the U.S. Congress (1984), the financial industry would become increasingly dependent on technology. New information technology in combination with its careful implementation in organizations, can bring improved net profit for the financial institutions (Shin, 2001). Increased availability of information and enhanced data processing capabilities have increased

* Corresponding author at: KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden.
E-mail addresses: svarga@kth.se (S. Varga), joel@kth.se (J. Brynielsson), ulrik.franke@ri.se (U. Franke).
https://doi.org/10.1016/j.cose.2021.102239

competition, and thus resulted in a more effective marketplace for the benefit of the customers too (Hauswald and Marquez, 2003). In addition, the recent emergence and ubiquitous presence of mobile payment devices, e.g., mobile phones with remote connectivity and contactless payment capabilities, has further reduced the need for banks and other financial institutions to have physical offices. Some of the work is increasingly pushed out to end-customers.

Although extensive use of information technology allows for ever more efficient conduct of business, it also introduces a set of new vulnerabilities. These are specifically attached to the technical systems (U.S. Congress, 1984). Moreover, it has been shown, unsurprisingly, that financial incentives are a powerful motivator for criminals (Bhasin, 2007; European Central Bank, 2018). The financial sector's heavy reliance on information as a vehicle for conducting business, combined with the myriad of threats to IT systems, has introduced a set of associated cyber-related risks, i.e., malicious actors are ready to probe and take advantage of potential vulnerabilities simply because the IT systems provide access to money (Kopp et al., 2017). In sum, it can be concluded that cyber-related activities, including cyber-crime, poses a non-neglible risk to the banking industry (Bhasin, 2007; European Central Bank, 2018).

The full range of cyber-threats encompasses everything from natural disasters, to threats where humans are involved. Cebula and Young (2010) divide actions that people can take to compromise IT systems into three classes: people can either (i) take inadvertent unintentional actions, without having a malicious or harmful intent, e.g., by doing mistakes, errors and omissions, (ii) fail to take action in a given situation, where actions otherwise would have prevented an undesired outcome, or (iii) act deliberately with the intent to do harm, e.g., by acts of fraud, sabotage, theft and vandalism. The present study mainly deals with the latter class; threats posed by malicious actors.

The *extent* of cyber-threats directed at various actors is hard to determine. There is no consensus about exactly what types of incidents entail cyber-threats, and whether or not certain actions raise to the level of criminality (Johnson, 2015). Even the volume of cyberattacks against any sector, including the financial sector, is notoriously hard to determine. The conventional assertion is that organizations tend to underreport cyber-threat related incidents to avoid embarrassment and loss of reputation (Britz, 2013, pp. 10–11). There are, however, some market actors that are in the business of following the cyber-threat landscape. Typically, companies that possess good data sources are in a position to have a fair view of the range of threats. Such companies include anti-virus software vendors and dedicated cyber intelligence companies. It should be kept in mind though, that some companies in the cyber security business may have incentives to project an exaggerated threat. Moreover, the data processing methods that they use, are not always fully transparent. Furthermore, threat intelligence products can be too generic, and not applicable to an individual organization.

The commercial company Intsights reports that the proportion of attacks directed against the financial sector, compared to other industries, is large (Rosenberg, 2019). Organizations are not only the subject for attacks against ATMs and mobile banking apps, but also for attacks with tailored malware, ransomware and phishing campaigns directed at other assets. The sector is certainly not immune to insider threats either (Randazzo et al., 2005). SWIFT and BAE Systems (BAE, 2018) note that cyber-threats in the sector appear to be directed at two main targets, namely the market's (technical) infrastructure, and its participants in the form of organizations and individuals. There has been an evolution of threats since 2006 with banking trojans such as `ZeuS`, `Dridex` and `Shylock`, through attacks on the banking networks themselves (`Carbanac`), and the SWIFT financial information messaging service (`Lazarus`) (BAE, 2018). To exemplify the characteristics of some of these historical examples; the `Shylock` trojan appears to be the work by a well resourced group that was active for several years, predominantely targeting U.K. banks. The trojan performs credential theft enabled by browser vulnerabilities.[1] `Dridex`, another trojan, uses phishing. Once a PC is infected, online banking credentials are stolen through the use of web injections and redirections to fake web pages.[2] Other pieces of malware perform in a similar manner.

When assessing cyber-threats, yet another factor to take into account is the sophistication and competence of the various threat actors (Bernier, 2013; Rosenquist, 2009). Threat actors can range from highly resourced state actors, e.g., the North Korean (DPRK) government, resourceful criminal groups, e.g., the Lazarus campaign, to less dangerous and skillful constellations of groups or individuals. Another serious threat actor category is the *insiders*, i.e., personnel with legitimate immediate physical, or indirect, access to the physical target systems.

In sum, it is no easy task to grasp the cyber-threat landscape in general, and especially the threat level for one's own organization. More precisely, we are referring to the difficulties of obtaining situation awareness, SA (Endsley, 1995; Patrick and Morgan, 2010; Salmon et al., 2008). SA is a concept that in essence tries to capture an individual's ability to interpret relevant aspects of the surrounding milieu, and grasp of a situation, oftentimes for the purpose of solving some task. Good SA implies that a person's inner mental model of the situation corresponds to some objective external reality. Research has shown that good SA may contribute to rational decisions and effective actions (Klein, 2000). Hence, it is of great importance to have good SA to perform well. In order to investigate SA it is therefore important to measure the actual level of SA. Several measurement techniques typically constructed to align with a specific SA model and suit a specific domain are available (Brynielsson et al., 2016). Some main groups of techniques include self-ratings, probes, ratings by observers and measurements of performance metrics (Salmon et al., 2006).

There are several theoretical models that seek to frame situation awareness (Salmon et al., 2008). An intuitively understandable and widely spread SA model is Mica Endsley's three tier model (Endsley, 1995). Simply put, the model presumes an actor with SA to have the capabilities of gath-

[1] https://www.computerworld.com/article/2489819/international-police-operation-disrupts-shylock-banking-trojan.html

[2] https://www.bankinfosecurity.com/dridex-banking-trojan-makes-resurgence-targets-us-a-9079

ering relevant information, to make sense of that information, and foresee some of its implications for the near future. Hence, in Endsley's terms, to *perceive*, *comprehend*, and *project* (Endsley, 1995). The original SA construct (Endsley, 1995) was intended to model how an *individual* acquires a level of situation awareness.

Cyber situation awareness, CSA, is about SA for the cyber domain. It can be seen as a special case of the general SA-concept described above (Franke and Brynielsson, 2014). The characteristics of cyberspace differ from other domains, which in turn makes it hard to define a "situation". Two differing factors to consider, for example, are physical space and temporal dynamics. First, the Internet with its vast network of interconnected networks is global. This means that threats against a specific network can be conveyed from anywhere. Second, multiple temporal scales must be considered simultaneously (Brynielsson et al., 2016). Cyberattacks, for example, take place at "computational speed", i.e., almost instantly, while their traces (Branlat, 2011) or effects can only be observed afterwards (Brynielsson et al., 2016). The complexities of the cyber domain have rasised a diverse set of CSA research questions which have created a heterogeneous academic field (Franke and Brynielsson, 2014).

A concept which becomes interesting in conjunction with research about SA is the common operational picture, COP. The idea of a COP originates from the military domain where it was to provide commanders, staffs and their warfighters with a "common picture" of the battlefield (Hager, 1997). A COP can form the basis for SA for both individuals and teams, but is mainly intended to help teams perform better. McNeese et al. (2006) found that a large information display screen could help a team in a military command post to gain shared awareness of a situation. Such shared awareness provides teams with a common base from which they then can solve problems collaboratively. The COP, in other words, serves as a vehicle that both enables and enhances individual work as well as teamwork. It can be seen as an artefact that stores and distributes useful information necessary for gaining SA, e.g., an "information warehouse" (Copeland, 2008). It can also be viewed as a process (Wolbers and Boersma, 2013), where the meaning of the information is actively negotiated in social interactions, hence a "trading zone"-metaphor (Wolbers and Boersma, 2013).

Regardless whether SA (CSA) or COPs are examined, the initial steps of selecting and including relevant information elements for further processing are equally important. It has been shown that if a COP is put together without deliberate and sensible design choices it risks to impede rather than improve collaborative work (McNeese et al., 2006, p. 468). The questions of information selection and processing here, also relate to an emerging research field about cyber-threat intelligence, CTI, and associated information sharing (Mavroeidis and Bromander, 2017; Shin and Lowry, 2020; Tounsi and Rais, 2018; Wagner et al., 2019). CTI at large aims to design information processing capabilities that ultimately help decision-makers make sensible cyber defense-related decisions.

There is to our knowledge no prior research that examines the collective cyber-threat information requirements of an industrial sector, despite that the literature indicates the presence of such government-private information-sharing constellations (Wagner et al., 2019, p. 4), and both European and American regulations within the sphere of cyber security strive for such enhanced cooperation (Skopik et al., 2016, p. 171). Neither is there, to our knowledge, prior research of how representatives covering large parts of an industrial (financial) sector on the national level perceive cyber-threats against it. This study seeks to partially bridge these research gaps.

The first research question targeted by the present study, concerns what *information elements are needed in a financial sector COP to achieve CSA*. The second research question concerns the *cyber-threats perceived by financial sector actors in Sweden*. Here we examine informant perception of the cyber-threat against the financial sector and their organizations in general, and the most common and the most serious threat types in particular.

The remainder of this paper is structured as follows. Section 2 discusses relevant related work and positions the contribution. Section 3 provides background on cyber risk in the financial sector in general, contextual information regarding the Swedish financial sector and the exercise studied, and concludes with a brief discussion regarding relevant related work. Section 4 explains the adopted methodology, including the construction of the questionnaire used, the choice of informants, and the conduct of interviews. This is followed by Section 5, which contains the results from the survey and the interviews. In Section 6, these results are discussed in relation to the literature, along with limitations with the study. Finally, Section 7 concludes the paper and presents recommendations.

2. Related work

There are multiple perspectives when it comes to SA in *teams*. One is to see team-SA as the SA of individual team members, which can either be similar, or shared with other team members to varying degrees. Another perspective is to see team-SA as the combined SA of the whole team (Salmon et al., 2008). Salas et al. (1995a) propose that team-SA consists of both the individual's SA and team processes. Artman and Garbis (1998) further emphasize team-SA as an active interpretative process, e.g., "the active construction of a model of a situation partly shared and partly distributed between two or more agents..." (Artman and Garbis, 1998, p. 3), that is: the building of a common understanding through communication. Salas et al. (1995a) also found that there is a general consensus among scholars that communication is a crucial factor for developing team-SA. Research about team-SA (understanding) has been carried out in many diverse fields, among others: railroad operations (Roth et al., 2006), off-shore drilling (Haavik, 2011) and counter-terrorism operations (Valaker et al., 2018). However, we have found no previous investigation of team-SA in the financial sector. In particular, our analysis of information elements needed from and offered to other organizations, relates to this field.

When it comes to CSA, Paul and Whitley (2013) examines the information requirements of cyber defense analysts. They found that analysts ask themselves questions within two main categories: event detection and event orientation. These categories loosely correspond to Endsley's level one

(perceive) and two (comprehend). For detection (perception) there is a need to know the normal state of the network, deviations from this normal and the specifics of those deviations. Questions about the orientation (comprehension) category are about making sense of the detected events from the prior phase, and typically includes *what?, where?, who?, how?* and *why?* type of questions. In the orientation category there are also inquiries about the attack's impact on one's own mission and damage assessments, including cascading effects. In this work, notably, respondents do not explicitly indicate an interest for information that would enhance projections of future outcomes (according to Endsley level three) (Paul and Whitley, 2013). Tadda and Salerno (2010) use Endsley's model as a base for a proposed SA reference model. Information requirements are listed in a part of their model which corresponds to Endsley's first level: perception. Hence, they propose that information about activities that involve organizational groups and associated events should be collected. This information should then be linked to entities that are either physical objects or concepts. Endsley's second (comprehension) and third (projection) levels are also represented in the model. In the second-level part, they highlight the importance of knowledge of one's own system and an assessment of the impact (damage) that was caused by the previously observed activities. Their model also includes elements of projection (Endsley level three) of future states (Tadda and Salerno, 2010). We do not aspire, in this work, to make any theoretically novel contributions to the application of Endsley's model to the cyber domain. However, from a practical perspective, it brings some additional evidence on how the different levels work in practice when applied to the cyber domain.

As of the linkage between SA and COP, Harrald and Jefferson (2007) suggest that technological solutions must provide access to adequate information for decision-makers even if they are at different geographical locations in order to obtain a COP. Recipients, thus, must receive and perceive the same information. Second, they call for the necessity of common methods for information structuring and integration that contribute to a common understanding of the received information. To acquire team-SA, an additional third step is also necessary: critical decision-makers must share institutional, cultural and experiential backgrounds to ensure some measure of uniformity to the process of extracting knowledge out of the information, e.g., to make sense of it in roughly the same way. Sophronides et al. (2017) conclude that a COP facilitates the acquisition of SA and supports collaborative planning for multiple agencies across several levels of command. A COP promotes shared perspectives and common priorities for emergency operations. Likewise, Norri-Sederholm et al. (2017) find that COP-systems enable shared SA for public safety organizations. Steen-Tveit and Radianti (2019) gather that SA and COP are two important artifacts required when various emergency response stakeholders must cooperate to handle large crises. With respect to these areas, our work extends the literature both by its focus on the cyber domain, and by its setting in the financial sector, which we have not found represented in the extant literature.

The field of information security management, ISM, is risk management where the critical asset is information. ISM is ideally a structured process that leads to well balanced implementation of safeguards to protect ones' information. The initial steps in this process include identification and analysis of both asset value, vulnerabilities and safeguards already in place, as well as threats and threat scenarios (Fenz et al., 2014). Blakley et al., 2001 suggest that information security is about risk management with a wider scope than purely technical aspects and should account for other variables too. Webb et al. (2014) emphasize the importance of information and intelligence in ISM. In fact, they propose that the primary goal of the whole information security risk management process is to support the SA of the decision-maker (p. 10). Similarly Cooke et al. (2019) point out that CSA-models also should include elements beyond the "network", i.e., the technical parts of the cyber domain. More specifically they propose to expand the scope to include a wider view of the "cyber landscape" (p. 130), which among other things should include the behavior of end-users. Ahmad et al., 2020 also identify two main scopes of interest, but here in terms of organizational learning for cyber incident response. The first, that here corresponds to the "network" level, is single-loop learning. Such learning may result in corrective actions, such as patching vulnerabilities based on prior events. The second level, double-loop learning, can lead to more profound organizational changes, e.g., improvements in the overall security posture by the amendment of current security strategies, processes and workflows, etc., in order to remove or diminish existing vulnerabilities. In terms of the nomenclature in this study, single-loop learning corresponds to a limited level of CSA that enables organizations to metaphorically "stop the bleeding", e.g., to perform immediate acute actions that will improve the level of cyber/network security in the short term. Double-loop learning corresponds to the higher level of CSA that can be used to initiate and perform more profound organizational changes. Burger et al., 2014 propose a taxonomy for cyber-threat intelligence information exchange. It has five layers where the layers arguably contain information elements ranging from straightforward to more complex. The layers are transport, session, indicators, intelligence and 5W1H. The lower-most transport-level involves information about the movement of bytes, e.g., data-streams that represent the cyber-threat intelligence between enterprises. The purpose of the uppermost 5W1H-layer, which is fed from the underlying layers, is to answer questions such as *who, what, when, where, why* and *how?* Hence, it seeks to answer the overarching question of attribution; Who or what organization was responsible for the threat? Here we offer an extension of the literature to include the financial sector, which is not explicitly addressed in the ISM literature cited above.

With regard to the specific circumstances within the financial sector, Leaver and Reader (2016) conclude that a significant portion of the underlying causes of critical errors committed by financial traders originated from insufficient situation awareness and deficiencies in teamwork processes, or both. Moreover, in a survey performed by the International Organization of Securities Commissions, IOSCO (Tendulkar, 2013), 46 exchanges reported that the two most common cyberattacks are perceived to be denial-of-service, DoS (by 55% of the respondents), followed by malicious software, e.g., viruses (52%). These attack types are at the same time also judged to be the most hazardous (75%

and 55%, respectively). Two other attacks are thought to be potentially hazardous, although not particularly common: data theft (45%) and insider information theft (34%). The two most disruptive attack types are judged to be malicious software at 45% and DoS at 38%. There are also empirical studies of cyber incidents in banks based on loss data from operational risk databases, such as Goldstein et al. (2011), Rachev et al. (2006), Ibrahimovic and Franke (2016), and Biener et al. (2015). These studies typically aim to use empirical insights to improve risk management practices such as the Basel framework which is briefly introduced in Section 3.1. All of these quantitative studies offer an interesting background to the more qualitative assessments made by the informants interviewed in our study. Conversely, these qualitative assessments make it easier to correctly interpret and contextualize figures such as those cited above.

Tounsi and Rais (2018) argue that the ever increasing sophistication of cyberattacks require defenders to collect and understand cyber-threat intelligence. They divide such threat information into four categories: strategic, operational, tactical and technical. Strategic intelligence is mainly intended to cater for risk management for decision-makers. Operational intelligence includes information about specific impending attacks, while the tactical category involves more detailed descriptions of *modus operandi* for attackers. The technical category, finally, consists of information about IOCs, e.g., detailed technical information such as IDS signatures, malicious domain-names and hash-sums of specific pieces of malware, etc. (Tounsi and Rais, 2018).

Another systematic analysis of what aspects to include in CSA was made by Barford et al. (2010). They propose that knowledge within seven areas is required for "full cyber situation awareness" for cyber defense. The seven requirements are awareness about: (i) the current situation (which may include network security and the wider cyber influence), (ii) impact of attacks, (iii) how situations evolve, (iv) adversary behavior, (v) why and how the current situation was caused, (vi) the quality and trustworthiness of the situation awareness information itself, and (vii) assessment of plausible futures of the current situation. These requirements also align with Endsley's SA-model. A very similar model can be found in Jajodia and Albanese (2017). In this study we chose to analyze our collected data, i.e., the respondent inputs, by using the Barford et al. (2010) model as a theoretical backdrop. The reason is that their model is generic and suitable for all categories of threat information, see Tounsi and Rais (2018), including the strategic level which relates to our main topic.

3. Background

The purpose of this section is to outline relevant concepts such as risks, and especially cyber-related risks, briefly describe the structure of the Swedish financial sector, and the sector exercise from which data was collected.

3.1. *Risks, operational risks, and cyber risks in the financial sector*

While risk management is a core business of the financial sector, it is important to distinguish between different types of risk. The most fundamental distinction is that between *financial* and *non-financial* risks. For example, Hull lists three broad types of risk for which banks are required to hold capital: credit risk (that counterparties default), market risk (that traded assets decline in value), and operational risk (that internal processes or systems fail or that adverse external events materialize) (Hull, 2015, pp. 41–42). The first two risks in this taxonomy are financial in origin whereas the last one, which includes cyber risks, is non-financial in origin. Regardless of origin, of course, all these risks entail costs.

Other authors propose more fine-grained taxonomies. For example, Bessis lists seven types of financial risks (credit risk, liquidity risk: funding risk, interest rate risk, mismatch risk, market liquidity: market price risk, market risk, and foreign exchange risk) alongside the non-financial, operational risk (Bessis, 2010, p. 26). Traditionally, credit risk has been the greatest risk facing banks (Hull, 2015, p. 41). As the separation between commercial and investment banking has largely disappeared, and as large banks most often are involved in securities trading, the other financial risks have become more prominent. This is reflected in the literature on risk management in the financial sector, where financial risks receive by far the most coverage in textbooks as in the scientific literature. However, with increasing dependence on information technology, non-financial operational risks such as cyber risk have received more attention in the past few years, both by practitioners and academics. Hull remarks that it is much more difficult to quantify operational risk than credit or market risk, and whereas financial institutions consciously balance the upsides and downsides of credit and market risks as part of their core business, operational risks represent a downside only with regard to doing business at all (2015, p. 480).

The growing importance of operational risks is reflected in the Basel regulatory framework, the set of recommendations for regulations in the banking industry that is standard in the G20 and some other countries. In the initial version, Basel I (1988), operational risk was absent. It was first defined in Basel II (2006) as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (2006) with a definition that is retained in the latest version, Basel III (2017).

Following the introduction of operational risk in Basel II, a conceptually oriented strand of academic research has aimed to shed light on the relation between the Basel risk management practices on the one hand, and established IT (security) governance practices such as COBIT, ITIL, ISO27001, and ISO/IEC 15504 on the other hand. Contributions in this spirit include the work by Guldentops (2004); Nastase and Unchiasu (2013); Önal (2007); Rifaut and Feltus (2006). One relatively well-cited definition, based on Basel II, that is roughly adhered to throughout the rest of this study was provided by Cebula and Young (2010, emphasis in original, p. 1):

> *Operational cyber security risks* are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems. This report presents a taxonomy of operational cyber security risks that attempts to identify and organize the sources of operational cyber security risk into four *classes*: (1) actions of

people, (2) systems and technology failures, (3) failed internal processes, and (4) external events.

3.2. The Swedish financial sector

The Swedish financial sector forms a non-negligible part of the economy. In 2017, the financial industry accounted for 4.1 percent of the total output of Sweden (GDP). At the time more than 90,000 people, corresponding to about two percent of the total workforce, worked in the financial industry.[3]

Changed regulatory conditions and technological advances have led to a significant change in the structure of the sector. Many new financial companies, both Swedish and foreign, have established a presence on the Swedish market lately. As a result, probably due to an interplay between both increased competition and technological developments, branch offices have become less important for bank customers' daily services. Today normal bank services are to a large extent performed through computers, mobile phones, and tablets. Swedish customers were forerunners in adopting online banking and a similar trend can also be observed for the next generation of FinTech (Björn, 2018), including real-time payments between private individuals (e.g., Swish, a mobile phone payment system used in Sweden), e-invoices, etc. As a consequence, the use of cash has plummeted, with the share of electronic payments (by transaction value) reaching 98.3% in 2015 (Arvidsson, 2018). Thus, while the increasing dependence of the financial sector on IT services is a global phenomenon, the particular dependence of consumers and small merchants on IT services for everyday transactions is even larger in Sweden.

3.3. The Swedish financial sector exercise

The Swedish financial sector's private-public partnership (Swedish: *Finansiella Sektorns Privat-Offentliga Samverkansgrupp*, FSPOS), henceforth FSPOS, conducted a one day national level crisis management and cooperation exercise on 7 November 2018. The exercise was part of an ongoing series of exercises aiming to strengthen the ability of the sector as a whole to manage disturbances and interruptions. More specifically, the 2018 exercise aimed to train each organization in establishing a common operational picture, to share it, and cooperate with other relevant actors in the sector. The underlying aim for this, was to agree upon collective needs for actions and common unified messages for both external and internal communication.

Some 270 individuals representing a large part of the entire Swedish financial sector participated. Participants included (i) banks, including the five largest, (ii) insurance companies, (iii) securities dealers, and (iv) central players in the financial system such as the Riksbank (Sweden's central bank), the Swedish National Debt Office (the central government financial manager), Euroclear (the Swedish central securities depository), and Nasdaq (the stock exchange).

[3] https://www.swedishbankers.se/en-us/the-swedish-bankers-association-in-english/the-swedish-banking-market/the-swedish-financial-market/

1. Facts	2. Prognosis
• What has happened? • What actions have we taken?	• What do we think about the development? • What central assumptions have we made about the development? • What central assumptions have we made about the current state?
3. Strategic intent	**4. Actions**
• What is our strategy? • What do we want to achieve? • What is our desired end state? • What is the way forward? • What are our subgoals? • What are our messages?	• What prioritized general actions do we plan for?

Fig. 1 – "The quadrants" methodology for establishing and maintaining a common operational picture. Translated and adapted from FSPOS AG KON (2017, pp. 19–25) and exercise briefing.

The fictional scenario involved cyberattacks causing various disturbances throughout the financial system, paired with so called fake news and a generally chaotic media and information environment.

3.4. Methodology for the construction of a common operational picture

FSPOS has developed a *Guide to crisis management* (FSPOS AG KON, 2017). It contains a description of crisis management principles and methods that can be used within the financial sector in Sweden. These principles formed the basis for the training in the exercise. Among other things, the guide offers a methodology for establishing and maintaining a COP, colloquially known as "the quadrants" (Swedish: *fyrfältaren*), because of its visual appearance as illustrated in Fig. 1. The enumeration 1–4 shows the order in which the COP is created or updated. The quadrants should be continuously visualized in the situation room and be accessible to everyone working with crisis management. At each staff meeting, proposals for updates are discussed, and a new COP is decided upon. This is then valid until the next meeting. "The quadrants" is similar, but not identical, to other COP-templates described in Swedish literature on civilian staff work (Svensson, 2007, p. 160).

4. Method

This section seeks to outline the method used for this study. The study was based on two separate, but complementary, data collection methods: (i) a questionnaire distributed among participants of a national level incident management exercise within the financial sector, and (ii) in-depth interviews with the people who led cooperation conferences that were held within the same exercise. The two collected datasets were first analyzed separately, and then jointly. The results were contrasted to theory, and conclusions were drawn.

4.1. *Questionnaire*

The questionnaire was distributed to the informants in a dedicated session during the so-called "after-action-review". This meeting was held a few weeks after the actual exercise. Around 70 individuals participated at this meeting, that encompassed training sessions as well. All attendees, however, were not present at the time of the data collection for the study . The informants were briefed about the research purpose of the data collection. Then, printed questionnaires on paper were handed out, and completed in about 20 minutes. A total of 42 responses ($N = 42$) were received. However, all forms were not completely filled out. Towards the end of the allotted time slot, one of the authors gave a short lecture on COP and CSA research. Respondents were not paid or compensated in any way.

The questionnaire contained ten questions. The first seven were asked mainly to obtain answers to our first research question; about required information elements for a financial sector COP. These questions also sought to clarify intended recipients and the usage of the COP, as well as information sharing practices. The remaining three questions sought to contribute to the answer for our second research question; about specific cyber-threats. Here we examined whether and how systematic work with regard to constructing a cyber-COP was carried out.

The questions were the same ones that were used in previous COP/CSA research (Varga et al., 2018), thereby allowing for comparison with earlier results. Based on the experiences from the previous questionnaire, however, one question was dropped. The questions asked were (translated from Swedish):

1. What kind of information does a useful common operational picture need to contain?
2. What positions or roles in your organization is such a common operational picture intended for?
3. What type of decisions should be made based on the situation awareness that the common operational picture provides?
4. What kind of information may your organization contribute to others' common operational pictures?
5. What other organizations may benefit from information from your organization's common operational picture?
6. What kind of information from other organizations do you require for your own common operational picture?
7. From which other organizations do you require information for your own common operational picture analysis?
8. Do you work systematically with creating and upholding a cyber common operational picture?
9. Describe briefly how you are working with a cyber common operational picture!
10. How do you track cyber-related issues that may affect your organization?

No introductory remarks about the definitions of crucial terms, e.g., "cyber", and common operational picture, were given in conjunction with the completion of the questionnaire. The intent was to capture the variance of interpretations of these terms in the provided answers. An additional question about whether the informants were willing to participate in further research was also asked.

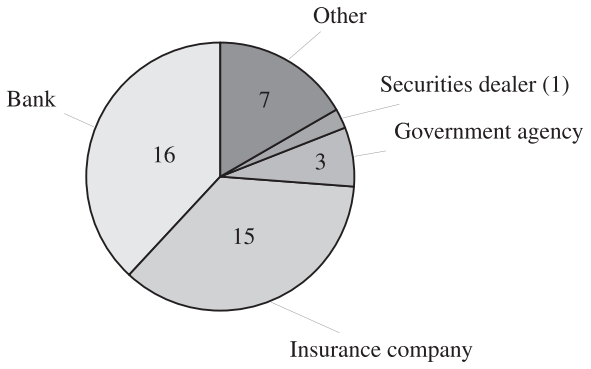

Fig. 2 – The distribution of the participating organizations ($N = 42$).

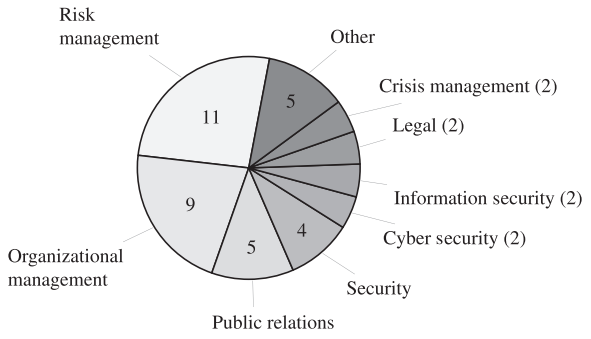

Fig. 3 – The distribution of the different roles of the participants ($N = 42$).

Respondent affiliations are shown in Fig. 2, and their organizational roles in Fig. 3. To properly interpret the meaning of these roles, two remarks are in order. First, the exercise was not a technical one, but a table-top: there were no (simulated) cyberattacks ongoing in order to train hands-on incident management by staff in Network-, or Security Operations Centers (NOCs/SOCs). Instead, the training audience was people at the management level. Therefore, it is reasonable to assume that the respondents mostly represent the strategic, as opposed to the operational, level. Second, the roles are self-identified. While some of the options used were prefilled on the questionnaire (Organizational management, Public relations, Cyber security, Legal), the majority of respondents ticked 'Other' and then supplied their own labels (Risk management, Crisis management, Security, Information security). Results should be interpreted in light of this. For example, the respondents who self-identified as Security or Information security rejected to self-identify as Cyber security, but it is not known how those who did self-identify as Cyber security would have answered if they had also been given the Security or Information security labels to choose form. What can be said with some certainty is that the largest group of respondents self-identify as risk management in the financial sector sense, as introduced in Section 3.1.

To analyze the responses, they were split among the three authors. Each author subjectively identified the frequency of occurring similar answers for each question, in three strata, e.g., if they were mentioned: (i) *many*, (ii) *some*, or (iii) *a few* times by the respondents. These results were documented. In some cases "outlier" answers that were only brought up by a single or a few respondents, but still deemed of interest, were also documented. The authors then convened and discussed each question, eventually reaching an agreement as of how to document the answers to that question. Multiple such meetings were held until a consensus emerged.

4.2. *Interviews*

During the single-day exercise, cooperation conferences for organizations in the participating branches were held twice; once at the beginning of the day and once at the end. Five such fora, based on branch affiliation, were established: (i) for the members of the Swedish Bankers' Association (henceforth: the Bankers), (ii) for members of the Association of Savings Banks (henceforth: the Savings Banks), (iii) for the insurance companies that are members of the industry organization Insurance Sweden, (iv) for the securities dealers that are members of the Swedish Securities Dealers Association (henceforth: the Securities Dealers), and (v) for the central players in the financial system. All leaders of these five workshop fora were interviewed ($N = 5$) to gain a better understanding of the challenges in establishing a shared COP and CSA at the exercise. The interviews were the main source for answering the research question about perceived cyber-threats.

Each interview was booked and expected to take about 1–1.5 hours, and conducted by two of the authors in a semi-structured fashion. All interviews were carried out at the premises of the respondents. One interviewer was assigned the main responsibility for asking questions, and the other for taking notes. However, both did both tasks to some extent. After the interview, the notes were sent to the interviewee in order to verify the answers. The interviews were held in the weeks following the exercise; the first one the day after the exercise, and the rest in the following weeks. The last interview was completed on 11 January 2019.

All the questions from the aforementioned questionnaire were also asked in the interviews. The inclusion of these questions provided an opportunity to complement the broader data collection through the questionnaire, with more in-depth reasoning with respondents, if needed. An additional COP/CSA question was also added. This question was related to the decision-point from when to go from normal day-to-day operations, to crisis management mode. In addition to the COP/CSA questions, questions related to two adjacent areas were also asked, namely about (i) cyber-threats against the financial sector, and (ii) the respondents' experiences from the exercise as such. In one case, the chair of a cooperation forum declined to answer some questions about organizational cyber-threat perception. The respondent, who did not feel authorized to answer on behalf of the organization, referred to a colleague who had that responsibility. As a consequence, an additional interview with a colleague to the original informant was held. This new interview was focused on cyber-threats only.

Finally, the outcome of the interviews was discussed and merged with the results from the questionnaire, in additional meetings with the authors.

4.3. *Corroboration of results*

Once the first version of the article manuscript had been written, representatives from the five organizations interviewed were given the opportunity to read and correct any misrepresentations of their statements.

5. Results

This section presents the results of both the survey and the interviews. First, the results from the survey and the corresponding interview questions (see Section 4.1), are reported. These results relate to our first research question about information elements in a financial COP. Then, we account for the results regarding the cyber-threat perception in the financial sector, based on the interviews. These results correspond to our second research question.

5.1. *Information requirements on cyber COP/CSA*

Here the results of the survey and interviews are presented, structured per question. The number of survey respondents are in brackets. Unless otherwise indicated, the number of occurrences of survey responses that coincide are described using the taxonomy introduced in Section 4.1 where the wording (i) "a few", (ii) "some", and (iii) "many" refer to (i) 2–3, (ii) 4–5, and (iii) more than five respondents, respectively.

5.1.1. *What kind of information does a useful common operational picture need to contain? ($N = 42$)*

The most common (31 out of 42) answer was that the COP needs to contain reliable information that is based on verified sources. The information should include a description of events that have occurred. Many also pointed out that unverified information, such as rumors, is also of interest, but that it would be absolutely necessary to separate the two categories. Many (15 out of 42) expressed that current intermediate subgoals and strategies, within the crisis management context, should be explicitly stated. A few mentioned that it was important that such goals should align with and reflect the overall strategic (as opposed to operational) goals of the enterprise, which in turn should adhere to its core organizational values (*ethos*). Here, both the short-term and long-term time frame should be taken into account.

Another requirement by many (ten out of 42) was a communications plan that explicitly clarifies the existing information-sharing policy, e.g., precisely what pieces of information that should be kept within the organization, and what should be shared. In this vein, a list of approved messages for both external and internal audiences, was asked for. Besides keeping track of events that are unfolding, many also formulated a need to keep track of already taken, and planned, actions. Further, they wanted a list of stakeholders, as well as cooperating organizations. A single respondent called for the identification of triggers and indicators to proactively watch

out for. Such indicators would be used for getting a clear grip of an evolving situation. Many wanted access to prognoses, but also to information about anticipated possible actions, as well as their predicted consequences.

A few respondents interestingly suggested that several types of prognoses needed to be made, e.g., both for expected probable (normal) cases, but also for worst-case scenarios.

Interviews. The interviewees did not add any further insights with regard to this question beside the answers given by the survey respondents. They rather reiterated the basic idea behind having a COP, namely that it allows for dissemination of information about threats. This, in turn, can be used to clarify if others are experiencing the same problem(s). Such an insight could enhance cooperation with other parties, to solve common problems. The interviewees pointed out that the COP should focus on issues that are forward-looking, if possible. Most incidents affect the IT environment. If a rumor is set in motion and distrust is introduced in the general population, the propagation of negative sentiments might be hard to counter or stop. Another useful insight given by the informants, was a widespread view that rumors have to be rapidly handled through the communications department.

5.1.2. *What positions or roles in your organization is such a common operational picture intended for? (N = 42)*

The most common answer (29 out of 42) was that the crisis management function, that typically constitutes a crisis management team, should be the main recipient of the information contained in the COP. In larger organizations, such a team can consist of a central crisis management function, as well as regional equivalents. Many (28 out of 42) respondents also wanted to address the COP to senior management, e.g., the CEO and his/her second-in-command. Many mentioned incident management teams (first responders) and risk management teams as suitable recipients, as well. Again, many also singled out various other senior management executives as potential recipients, particularly the head of the public relations (PR)/communications department, but also, e.g., the chiefs of security, the chief information security officer, the chief financial officer, and the head of the legal department. Some respondents wanted to share the COP with everyone in the organization, and a few pointed out that the COP should be shared with decision-makers in other organizations as well.

Interviews. Again, the interview respondents did not add any substantial insights to the survey respondents'. It was pointed out that it is important to have an up-to-date roster with important contact information, to be able to reach the right people quickly. Further, it was stressed that it is important to inform external suppliers, who perhaps carry some of the outsourced functions in the enterprise. Another point that was made, was a call for the need to have distinctly formulated decision conditions coupled with, e.g., a point in time from which the organization formally can transition to a crisis-handling mode.

5.1.3. *What type of decisions should be made based on the situation awareness that the common operational picture provides? (N = 40)*

The most common response (23 out of 40) given, was that decisions within the field of communications and public relations are important. The respondents identified a need for approved messages for both external and internal audiences. Many mentioned decisions about whom to cooperate with, and whether the organization should coordinate and align its actions with other sector partners or not. Yet another common answer by many was that there is a need for decisions about the overarching strategic direction, that ideally is also aligned with organizational values (this is in line with the answer to Question 1, see Section 5.1.1). A third category of decisions, also mentioned by many, is the prioritization of actions and resources. This would be important especially if there is a scarcity of resources, or that such decisions are called upon for other reasons.

A few expressed the need for operational decisions connected to what services to uphold or terminate. Examples of such decisions include: whether or not to regroup personnel to other locations; whether or not to stop trading; routines for the physical handling of cash; as well as decisions about whether to take internet services off-line, or not. A single respondent, interestingly, called for forward-looking decisions about activities aimed at preparations for handling the aftermath of the crisis.

Interviews. The answers generally reflected that it is important for everyone to have well-defined roles if crises occur. It was pointed out that it is impossible to predict the exact characteristics of a crisis, which in turn makes it hard to prepare for responses to all kinds of situations. In other words, it was expressed that it is unfeasible to rely on rules to cover all possible scenarios. The respondents called for an operational mode, in which the foundation for decisions should rest on solid underlying principles, rather than on specific rules. A general view among the respondents' answers, was the importance of the PR/communications function. The respondents also expressed that they care about their customers. The customers, in any case, can also be seen as an information source that provides useful information about the state of the services that are offered.

It should be noted that the main types of decisions that were mentioned by the interviewees, pertain to IT services. The whole financial sector depends heavily on IT infrastructure, and decisions in times of crises are often about whether services (systems) should be shut down or not. In some situations, it was pointed out, a rational option can actually be to deliberately stay calm without intervening and let events unfold, just to see if things settle anyway.

5.1.4. *What kind of information may your organization contribute to others' common operational pictures? (N = 41)*

Respondents primarily pointed to (i) confirmed factual information regarding external phenomena, (ii) situational assessments, (iii) own resource status, (iv) measures taken, (v) different types of financial market and other domain knowledge, and (vi) different types of prognoses. Unsurprisingly, the responses can to a large extent be related to "the quadrants" COP model described in Fig. 1, which can be assumed to be well known by the respondents. In this regard it can be noted that the vast majority of the answers relate to the initial phases of this model, while the later phases that are more about describing the forward-looking strategic (as opposed to operational) perspective are hardly mentioned at all.

A few respondents also pointed out that, in their capacity as a coordinating body, they contribute with different types of strategic decisions regarding priorities at large, decisions concerning ways to communicate, and other measures taken for the purpose of coordination.

Interviews. Similar to some of the questionnaire responses, the interview respondents do not explicitly reason about the actual information but about the communication about it. There is clearly a blurred line between the information that is communicated, the communication itself, and the choice of communication path.

5.1.5. *What other organizations may benefit from information from your organization's common operational picture? (N = 42)* In the responses two major categories of organizations can be discerned: other actors in the financial sector, and other authorities not primarily related to the financial sector. Unsurprisingly, almost all (40 out of 42) respondents in some form point to other players in the financial sector. Specifically, Finansinspektionen (Sweden's financial supervisory authority), and the Riksbank are mentioned to no small extent. Furthermore, half (21 out of 42) of the respondents point implicitly or explicitly to three of the industry organizations central to the financial sector: Insurance Sweden, the Swedish Bankers' Association and/or the Swedish Securities Dealers Association (the Savings Banks are not mentioned explicitly albeit "other savings banks" are mentioned a few times).

Three-quarters of the respondents (32 out of 42) also mention other authorities that do not have the financial sector as their main area of interest. Specifically, the Swedish Civil Contingencies Agency, the police authorities, and the Government Offices are mentioned to no small extent.

Similar to previous studies (Varga et al., 2018), many respondents state that "everyone involved", "other players in the sector", "all financial players" and the like ought to be provided with information, which can be interpreted as a general need to be able to share information in a crisis situation.

Interviews. The interview responses confirm the bigger picture, but place a greater emphasis on central functions related to the payment system and securities trading in general. The interview respondents also emphasize "the media" as important information recipients.

5.1.6. *What kind of information from other organizations do you require for your own common operational picture? (N = 42)* The responses largely mirror the answers given to Question 4 (see Section 5.1.4), i.e., the information needed for one's own COP is similar to the information identified to be of value to others, and consists primarily of (i) confirmed factual information regarding external phenomena, (ii) other organizations' situational assessments, (iii) status of other organizations with regard to resources and systems, (iv) measures taken by other parties, (v) different types of prognoses, and (vi) strategic (as opposed to operational) decisions regarding priorities at large. Many respondents also explicitly mention that the sought for information is the same as the information that can be provided to others, by referring back to the answer given to Question 4. In comparison to Question 4, however, two differences can be discerned: (i) factual information is something that is to a larger extent requested from others than it is mentioned as something that can be offered, whilst (ii) different types of financial market and other domain knowledge is to a large extent considered as valuable information for others' COPs while it is hardly requested at all in regard to one's own COP.

Interviews. The interview respondents confirmed the answers given by the questionnaire respondents, emphasizing the overall need for different types of factual information, and provided examples related to payment system disturbances, IT attacks, fraud statistics, impending power outages, and critical infrastructure disturbances at large. In addition, information regarding status of other organizations in terms of resources and systems, was mentioned.

5.1.7. *From which other organizations do you require information for your own common operational picture analysis? (N = 41)* Responses can broadly be sorted into three categories: (i) various government agencies, (ii) the industry organizations (the Bankers, the Savings Banks, Insurance Sweden, and the Securities Dealers), and (iii) other (central) players in the financial system. Of the non-financial government agencies, the Swedish Civil Contingencies Agency (mentioned 15 times), the Security Service (mentioned eight times) and the police, including the financial supervisory authority (mentioned seven times), were the most common. Some respondents mentioned other agencies, e.g., the intelligence services and the The Swedish Data Protection Authority (renamed the Swedish Authority for Privacy Protection from January 2021).

Of the central players in the financial system, the financial supervisory authority (mentioned six times), Euroclear and central counterparty clearing houses (mentioned four times) were the most common. Additionally, the Riksbank (mentioned twice), the Swedish National Debt Office (mentioned twice), and the Nasdaq stock exchange (mentioned twice) were brought up by a few. Aside from these major clusters of responses, some other actors were mentioned, e.g., service providers (mentioned five times), rescue services (mentioned once), cash transportation services (mentioned once), and the general government and parliament (mentioned twice). Some also mentioned particular banks.

A common (nine out of 41) remark was that the answer depends on the situation at hand, i.e., different situations entail different information requirements. It is also noteworthy that many respondents referred back to their answers to Questions 5 and 6 (see Sections 5.1.5 and 5.1.6), which have been included in the analysis above. References to Question 5 could indicate bidirectional information flows.

Interviews. The interviews broadly confirmed the answers gathered from the survey. In particular, the importance of the financial supervisory authority, the Riksbank, Euroclear, and the Swedish Civil Contingencies Agency was confirmed by several informants. The informants also confirmed that different situations entail different information requirements and that it is important to involve different stakeholders in different kinds of crises. It is also noteworthy that the different roles of the informants are reflected in their answers. Hence, differences between governmental agencies, the various indus-

try organizations, and other organizations that perform other functions in-between, can be discerned.

5.1.8. *Do you work systematically with creating and upholding a cyber common operational picture? (N = 38)*
29 respondents did, nine did not. The remaining four respondents remarked either that they did not know the answer, that they did not know whether their work was systematic, or that the question could not be answered without a definition of a cyber COP.

5.1.9. *Describe briefly how you are working with a cyber common operational picture! (N = 29)*
Responses to this question included references to technical means, internal organizational groups (who performed the actual work), external fora for information exchange, processes, or individuals. Many respondents mentioned several of these. The technical means that were brought up included monitoring systems and penetration tests. Internal organizational parts that were reported to work with cyber COPs included security departments (e.g., security incident response teams, information security departments, cyber defense departments, etc.), the financial instruments department, group IT, group risk, and cross-functional teams (IT, communications, human resources, etc.).

Among the external fora for information exchange, the forum for information exchange about information security in the financial sector (FIDI-FINANS) run by the Swedish Civil Contingencies Agency and the Nordic Financial CERT (NFCERT), were named specifically by a few.

The informants who answered in terms of processes, referred to the specific "quadrants" model described in Section 3.4 (mentioned four times), the incident management (mentioned once), crisis management (mentioned once), regular common operational picture (mentioned once), unspecified competitive intelligence (mentioned once), and exercises (mentioned once). Additionally, a few respondents pointed to individuals.

Interviews. The interviews complemented the picture given in the survey. The responses also gave some insight into how the division of labor works in the sector, which is further described in Section 5.2 below.

5.1.10. *How do you track cyber-related issues that may affect your organization? (N = 41)*
Responses to this question were similar to the previous one, and included references to internal organizational groups, other companies, external fora for information exchange, government agencies, and the industry organizations (the Bankers, the Savings Banks, Insurance Sweden, and the Securities Dealers).

Mentioned internal organizational groups include security departments (e.g., security incident response teams, chief information security officer, cyber defense, etc.), risk management, IT operations, the financial instruments department, and cross-functional teams. Mentioned companies include IT vendors, consultants, the media, and parent companies.

External fora for information exchange include FIDI-FINANS, FSPOS, NFCERT, and a constellation of security incident response teams. Government agencies mentioned include the Swedish Civil Contingencies Agency, the Riksbank, the financial supervisory authority, and Europol. It is also noteworthy that many respondents refer back to their answers to Question 9 (see Section 5.1.9), which have been included in the analysis above.

Interviews. The interviews confirm the plethora of methods used to track cyber-related issues. The informants typically participate in various fora for information exchange and have dedicated personnel (full or part-time) for cyber-related issues.

5.2. *Perceived cyber-threats—interview results*

When given an open question on *threats to the financial sector in general*, informants generally identify cyber-threats as being important, in line with the literature (BCBS, 2018; Hull, 2015, pp. 479–480). Cyber risks mentioned include both (i) continuity issues and (ii) data breaches which might affect public trust. Insurance Sweden also mentions that the cyber-threat has a dual nature for insurers: (i) as for everyone else, they themselves need dependable IT systems, but as cyber insurers, they also (ii) carry the cyber risks of their insured customers, within the indemnity limits contracted. This is conceptually interesting in light of the financial sector risk taxonomy introduced in Section 3.1, because (i) the cyber risks of insurers' IT systems are non-financial operational risks assumed by insurers as a cost of doing business, whereas (ii) the cyber risks of insureds' IT systems are financial risks deliberately assumed by insurers as their core business.

When asked about *the most serious threat*, informants identify different aspects. A couple mention threats against the financial infrastructure as the most serious threat, while another identifies the practice of social engineering as the most serious threat, arguing that it is very serious because consumers are tricked to use their credentials against their own interests, which in turn can erode trust in the whole sector. Several informants identified such public trust as a key issue at stake.

There is some agreement that *the most common threat* is various kinds of consumer fraud, i.e., social engineering to obtain credentials, and credit card fraud. Human factors are identified as playing an important role in threats to non-consumer-facing activities, such as larger scale securities dealing. In general, there is agreement that humans, including consumers, are often the proverbial "weakest link", as there has been a dramatic shift towards self-service in the financial sector, with consumers themselves managing their electronic accounts.

Addressing different kinds of *threat actors and their capabilities*, there was agreement about the importance of (i) financially motivated actors who use digital means to commit theft and fraud. In contrast to financially motivated actors, it was speculated that (ii) activists who hold a grudge against the financial sector might have more limited capabilities. As a consequence of the importance of human factors, (iii) insiders were also identified as key threats, and background checks on staff were mentioned as an important precaution. Finally, (iv) states and state-sponsored actors were also discussed as an important matter of principle, though not

practice. In particular, the importance of adequate intelligence sharing within the industries and with relevant government agencies was discussed in this context. The respondents do not themselves collect intelligence about particular threat actors in order to identify them or their modi operandi—if such information is found, it is rather handed to the police. Similarly, most interviewees remark that they do not perform real-time intrusion detection, but that this is rather the business of their member firms (individual banks, securities dealers, insurers, etc.), in collaboration with relevant government agencies.

Turning to *the consequences of cyber incidents* (antagonistic and non-antagonistic alike), informants agree that these are potentially very large and difficult to assess, because (i) everything in the financial sector now depends upon available IT services, and (ii) people are very dependent on financial services in their daily lives. The availability of electronic payment systems was mentioned by several informants as being particularly important. One respondent reasoned instructively about prioritizations, remarking that if banks have the opportunity to prioritize, payment systems are probably the last service being closed down, whereas systems for mortgages and other credits are probably first to go. The aim is to avoid rollbacks of transactions as well as long restoration times, in line with the literature on IT service restoration times in financial services (Franke, 2012). Of course, it is far from certain that such prioritizations can be made in practice. The same respondent remarked that the cyber-threat landscape is growing ever more complex, with interaction effects between phishing, trojans, social engineering, denial-of-service attacks, data breaches, power outages, etc.

The Securities Dealers also mention that new regulations which must be implemented on a tight schedule can be problematic, because hurried change projects in IT environments are likely to introduce new bugs as an unintended side effect. This remark is not surprising from the perspective of the literature on success and failure in IT projects, see, e.g., Alami (2016); Bloch et al. (2012); Wateridge (1998).

6. Discussion

In this section we first reiterate the outline of our methodological approach, and discuss our findings contrasted to the backdrop of existing relevant theory. Second, we highlight possible limitations to our approach, as well as questions concerning validity and reliability.

The purpose of this study is to shed light on questions about cyber risk management in the financial sector. The main questions concern the information elements needed in a common operational picture, and cyber-threat perception. Data from surveys and a series of interviews with key actors within the Swedish financial sector form the basis for the conclusions. Data was collected in conjunction with a multi-stakeholder crisis management exercise.

Although the ever ongoing digitalization of society could not come as a surprise to anyone, the seriousness of cyber-related risks does not seem to have been fully understood until recently. According to the World Economic Forum, common cyber risk awareness, risk management practices and information exchange mechanisms in general, appear to be lacking throughout the financial sector.[4] These deficiencies have the potential to cause unwanted consequences.

As noted by Hull (2015) (see Section 3.1), these kinds of operational risks are much more difficult to quantify than credit or market risks. This is particularly true of cyber-related risks, where the literature contains some spurious results and different studies sometimes point in different directions (Woods and Böhme, 2021). To further complicate risk management, negative outcomes due to cyberattacks may come in many different forms, e.g., as physical or digital, economic, psychological, reputational and social effects (Agrafiotis et al., 2018). To have a unified framework, to quantify, and to determine the monetary value of these kinds of adverse "soft" factor effects with accuracy, is therefore extremely hard.

6.1. *Cyber situation awareness*

To put the collected data, i.e., the respondent inputs, in context, it is useful to have a theoretical backdrop. Here we analyze the data according to the seven requirements for having "full cyber situation awareness" for cyber defense put forth by Barford et al. (2010). As mentioned previously, this same framework was used in a similar fashion in a previous paper that sought to investigate the same questions, but for other than financial businesses (Varga et al., 2018). According to Barford et al. (2010), the seven requirements for having CSA are (to have):

1. awareness of the current situation (which may include network security and the wider cyber influence),
2. awareness of the impact of the attack,
3. awareness of how situations evolve,
4. awareness of adversary behavior,
5. awareness of why and how the current situation is caused,
6. awareness of the quality and trustworthiness of the situation awareness information, and
7. assessment of plausible futures of the current situation.

After having analyzed the responses, it turned out that respondents asked for information largely aligning with Barford et al.'s requirements with some exceptions, in their efforts to create a COP. Respondents specifically sought information in line with Requirements 1 (see Section 5.1.1), 2 (Sections 5.1.1 and 5.1.3), 3 (5.1.1), 6 (5.1.4 and 5.1.6), and 7 (5.1.1). It was hard to discern any information requirements relating to adversary behavior (Requirement 4), and how, and particularly *why*, the current situation came to be (Requirement 5). These results are consistent with Varga et al. (2018).

Reflected in Section 5.1.9, there is a strong focus on technical means such as system monitoring and penetration testing to achieve cyber situation awareness. But CSA also involves having a higher order understanding of the potential implications of cyber-threats, e.g., the *meaning* of "system events", and other relevant threat information. The respondents point

[4] https://www.weforum.org/agenda/2020/02/cyber-risk-should-take-centre-stage-in-financial-services/

to the practice of relying on external fora for information exchange, and sometimes even on particular individuals. Judging by these answers, it is questionable whether there is a widespread practice to systematically collect, analyze and extract higher order knowledge from one's own technical "system events", that in turn can be used to inform risk management processes.

It is noteworthy that much effort seems to be made to ensure that truthful messages that reflect the state of the situation as perceived by the parties, are communicated to external audiences as an integral part of crisis management (see Section 5.1.4). This probably suggests that there is a widespread insight that the functioning of the financial sector *as a whole*, is highly dependent on the trust placed in it by its customers.

Very few ask for information about adversaries and/or question underlying root causes for the present situation. A possible explanation is that civilian crisis management is primarily tuned to handle non man-made, e.g., natural disasters, or isolated man-made incidents. The FSPOS scenario, by contrast, involved a sustained cyberattack campaign that was designed by rational adversaries (i.e., a game as opposed to a decision problem). Financial sector actors possibly do not think about sustained threats from intelligent purposeful adversaries on a daily basis—at least not on this scale. There is a value, however, in having knowledge about adversaries. It has been shown that game-theoretical models provide a feasible approach to capture the *interplay* between cyberattackers and defenders (Manshaei et al., 2013). Prognoses that fail to incorporate information about adversarial strategy, intentions and capabilities, risk being erroneous. Borum et al. (2015) argue that such cyber intelligence, which they call *strategic* (concerning the adversary), is indeed important for making high-quality risk-informed decisions.

There was an emphasis and a desire for sharing information with other stakeholders, but also to communicate to mass media. In the literature it has been shown that trust which is put into a complex system that is not fully understood—like the financial system—can be frail. When such trust is impugned, there is a possibility for a faster system collapse (Goldin and Vogel, 2010). Two dichotomies point to the importance of preserving trust in the system; First, it has been argued that attempts to eliminate the influence of trust by introducing impersonal rule systems, rather than relying on more direct interpersonal trust, create trust that is more "distant" and lack the safeguards of interpersonal trust. In short, complex technical systems may increase, rather than reduce, the risk they pose to systemic stability (Kroeger, 2015). Second, Earle (2009), in his analysis of the 2008 financial crisis, distinguishes social and relational *trust* from instrumental and calculative *confidence*. While trust is resilient, confidence is fragile: in the face of turmoil, a trusting party may interpret events charitably, whereas a party with mere confidence may withdraw this confidence at the first sign of performance criteria not being met. While we will not uphold Earle's distinctive terminology in the following, his analysis is thought-provoking also in the context of cyber incidents.

Consequently, when cyberattacks probe and overcome the defenses of cyber systems and the adverse effects are put on display, general trust in those systems can erode quickly and escalate to pose systemic risks (Kroeger, 2015). Therefore it seems justified to put much effort into controlling and managing information, including the information communicated to the public at large, in any financial sector crisis.

6.2. *Cyber-threat perception*

The results of this study align well with the cyber-threats flagged by the commercial sector. Three out of five top-tier threats noted by the commercial sector were explicitly identified in this study as well. Accenture (2019) lists credential and identity theft of consumer data, as well as data theft and manipulation, as major cyber-threats that are affecting the financial sector today. As for threats against the financial infrastructure, the Accenture report also puts forth the risks posed by destructive and disruptive malware. Two more general threats mentioned by Accenture (2019), (attackers') utilization of novel emerging technologies that are unproven and perhaps riddled with vulnerabilities, and the propagation and use of disinformation in a more general sense, were, however, not mentioned by the respondents in the present study.

The handling of cyber risk, and cyber issues in general, seems to be looked at in a different way than the management of other types of risks. It was indicated that neither the respondents, and sometimes nor their organizations themselves, perform the actual work that is associated with cyber risk management. More specifically, the respondents do not themselves collect intelligence about particular threats and threat actors in order to identify them or their modi operandi; such tasks are rather trusted to someone else, e.g., the police or other companies. Similarly, most interviewees remark that they, as industry organizations, do not perform real-time intrusion detection, but that this task is rather the business of their member firms (individual banks, securities dealers, insurers, etc.), in collaboration with relevant government agencies.

6.3. *Limitations*

The respondents in this study were all working for companies and institutions within the financial sector in Sweden. The exercise from which data was collected, was an integral part of the joint efforts within the sector to train for crisis management situations. All actors have a stake in that the sector continuously functions. Both governmental institutions and private companies alike, find it crucial to preserve public trust in the sector, and at the same time maintaining their good name.

The respondents in this study, again, made out a comprehensive cross-section of relevant actors within the Swedish financial system, even though some individual organizations and companies were not represented. The participating industry organizations voiced the opinions of their respective members, including those who were absent. This is to say that the study covered the span of relevant actors in terms of completeness.

The mission of FSPOS, and the crisis management exercise described in this study, suggests that the data collection phase of the study had a strong crisis management focus. The involved personnel were sharply focused on solving the various problems that arouse within the framework of the exercise.

Thus, the answers, in general, can be expected to be colored by the exercise context, rather than reflecting generic risk management practices.

Other threats to the validity of the conclusions may be derived from the specific circumstances in Sweden, that are not necessarily present elsewhere. The Swedish financial sector consists of a limited number of actors, and the overall health and well-being of the sector is in the interest for all involved parties. There is obviously competition for market shares, but a common set of ground-rules and behavioral standards is mutually beneficial for all involved parties, as manifested by, e.g., the FSPOS partnership. Another example is the practice of exchanging cyber-threat information, which to some extent is carried out even between competitors.

The involved parties in the financial sector have deliberately been using a common crisis management approach including an information handling model colloquially known as "the quadrants" (described in Section 3.4) for quite some time. The FSPOS partnership was initially conceived following an initiative by the Swedish financial supervisory authority in 2005.[5] The parties know the model well, and have been training crisis management with it for some time. It is likely that the personnel involved, mainly risk managers, have a common perspective on the problem set, which probably is a positive effect. Another possible consequence of the widespread use of the model is that it possibly constrains the thinking about crisis management, e.g., by fitting events and other information to the given categories of the model (this was also indicated in the answers to Question 4).

In sum, the study can be expected to have a good measure of *ecological validity* (Bronfenbrenner, 1977). As have been mentioned previously in this section, the participating personnel comprise a representative cross-section of the financial sector in Sweden. In addition, they were to a large extent performing according to their ordinary work roles, although in an artificial (exercise) milieu.

7. Conclusions and recommendations

In this section conclusions related to the study's two research questions are drawn, and a few recommendations related to cyber security and risk management work in the financial sector are made.

7.1. *Information elements*

The first research question concerned information elements needed in a financial sector COP to achieve CSA. The collected data displayed a large variety of interesting insights from the respondents. After having analyzed the responses by comparing the stated information requirements with Barford et al.'s (2010) requirements for CSA for cyber defense, it was found that respondents asked for information largely consistent with Barford et al. (2010), e.g., about impact of attacks, how situations evolve, plausible futures due to the current situation and also about the quality of the underlying information (see Section 6.1). However, a few other key results can also be highlighted:

- First, respondents showed limited interest in obtaining information about the behavior of adversaries, as well as for causal links between (prior) events and their effects, similar to the results of Paul and Whitley (2013), but contrary to the requirements of Barford et al. (2010). The lack of these pieces of information obstruct the potential to gain a deeper and clearer understanding of the current situation, which in turn also diminishes the ability to predict future events where adversaries who are thinking strategically form (part of) the threat. This result is consistent with Varga et al. (2018).
- Second, there was a strong focus on emphasizing technical aspects of cyber-threats, even on the higher managerial level. Here it would be more appropriate to consider the upper-tier information types, e.g., according to the Burger et al. (2014) model as cited earlier. Management should ponder questions such as *who, what, when, where, why* and *how?*, rather than concentrate on technical details better left to the operational level.
- Third, there was also a strong focus on information management. Respondents clearly appreciated a systematic approach to information handling, e.g., what to communicate to whom, in a structured fashion. This is probably related to the fact that the financial sector is highly dependent on trust, and thus needs to think carefully about how to communicate in a manner that inspires confidence, both in the short and the long term.

7.2. *Cyber-threat perception*

Our second research question concerned cyber-threats perceived by financial sector actors in Sweden. There is a general consensus among interviewees that cyber-threats are important to consider in risk management. The main assets at stake with regard to these threats are perceived to be the availability of IT-related services (continuity issues), and threats to information confidentiality (data breaches), both of which may lead to diminished public trust for specific companies and organizations, or indeed for the financial sector as a whole. The view on cyber-threats differ between insurance and other sectors, as insurers who underwrite cyber risk face cyber-threats twice: once against themselves (as everyone does), and once more against their customers, whose risks they insure.

When asked about the most serious threats, the respondents express that attacks against the financial infrastructure are seen as very serious. The most dangerous *attack vector* is reported to be social engineering, e.g., that attackers are manipulating humans to gain access to systems. The most severe consequence of attacks is seen as the erosion of public trust in the financial system as a whole. The most common threats are thought to be theft and fraud, committed by actors who employ social engineering techniques. Respondents also note that *insiders*, e.g., trusted persons with legitimate access to systems who are performing unauthorized activities, pose a significant threat. Moreover, when it comes to threat actors, those are consequently perceived to be crimi-

[5] https://www.fi.se/sv/om-fi/verksamhet/krisberedskap/

nals, but sometimes also ideologically or politically motivated activists.

The first main contribution of this study was to empirically shed light on how a whole industrial (financial) sector on the national level determines its information requirements for a sector-wide common operational picture intended to facilitate cyber-related crisis management. The second main contribution was to present a unique and empirically-based picture of how key players in the sector perceive cyber-threats against it.

7.3. *Recommendations*

The results obtained in this study exemplify both good practices, and practices that call for improvements. In the judgement of the authors, hence, a few recommendations (not listed in any particular order) can be made.

- First, regular multi-stakeholder crisis management exercises allow parties that normally do not work closely together on a day-to-day basis, to get together and practice crisis management processes. This recommendation is consistent with the results of Nyre-Yu et al. (2019), who found that vertical and horizontal organizational communication, feedback and accountability emerged as a key requirement for successful incident response, awareness and learning. Exercises that unify work practices, use similar terminology and establish personal relations between personnel from various organizations, provide an advantage whenever a real crisis occurs.
- Second, a mindset where individuals think about the greater whole, and not exclusively their own organizations, fosters a collaborative spirit and mutual trust, that in turn leads to information-sharing that is for the benefit of all. Such a state of mind can be a result of exercises, but also of training efforts.
- Third, although these practices were not investigated in-depth in the present study, organizations should take the opportunity to complement existing information outlets by extracting information about cyber-related risks from sources within the organization itself, e.g., one's own computers and networks, more extensively. The collected information should be actively transformed to knowledge that can be used to inform the risk management process.
- Fourth, it is important to collect and use cyber-threat information that outline and describe opponents, e.g., the cyber-threat actors. Cyber defense efforts should not be seen as work that has to be carried out in a "static" scenario, but rather as an interplay between defenders and attackers in a dynamic setting. An understanding of the opponents' motives and rationale can improve cyber defense. This kind of deeper understanding, rather than the technical details of various attacks, should be a goal to strive for, especially for the higher managerial level.
- Finally, personnel with in-depth technical "cyber" competencies should be incorporated in cross-functional risk management groups, that are composed of personnel with multiple other specializations other than "cyber". These representatives of the "cyber" part of the business, should be able to leverage domain-specific insights into knowledge that are compatible with other risk dimension variables. This recommendation is consistent with the findings of Ahmad et al. (2020) and Bartnes et al. (2016).

7.4. *Future work*

Based on the results, a few areas of possible future research can be identified. This study sought to examine the properties of a COP as a basis for team-SA (team-CSA) for multiple stakeholders in an information/cyber security setting. We did not, and did not aspire to, measure the resultant level of CSA acquired by individuals or teams. There are, however, as already mentioned, multiple measuring techniques available to do so (Salmon et al., 2006). It would therefore be interesting to build upon the results in this study by measuring how various levels of CSA affect the outcome and effectiveness of cyber incident management practices. A number of possible studies within the realm of cyber defense exercises are suggested by Brynielsson et al. (2016).

Another possibility for follow-on research could involve the characteristics of multi-stakeholder and cross-sector cooperation practices. An obvious question would be to examine whether there exist other industrial sector-wide approaches for managing cyber-threats, and how they are constructed? If so—are there any differences between the approaches, and why? It might also prove useful to establish whether experiences and lessons-learned from the financial sector could be transferred to other industrial sectors that aim to establish a similar cyber-exercise regime.

Yet another direction for further research involves questions of effectiveness of training and exercise efforts. Do whole *industrial sectors*, such as the Swedish financial sector, that conduct sector-wide exercises fare better in the face of (large scale) cyber incidents than sectors that do not? Since the number of such incidents (luckily) is small, and the sheer scale of such efforts is massive, it may be impossible to evaluate this quantitatively, but case studies or natural experiments are possible. On a smaller scale it could also be worthwhile to evaluate whether individual *companies* that have participated in sector-wide exercises cope better with (small scale) cyber incidents than companies that have not. An obvious challenge here is the lack of cyber incident data, but it is possible that mandatory reporting regimes, such as the EU NIS directive, will provide sufficient data to econometrically evaluate the effectiveness of cyber security measures such as the exercise regime studied here.

The second main topic of this study was cyber-threat perception, where the views of respondents who represented the whole (national) financial sector expressed a homogeneous view of the threats facing it. To expand the body of knowledge here, it could be of value to examine the threat perception in other sectors and multi-stakeholder constellations, for comparative perspectives.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Stefan Varga: Conceptualization, Methodology, Investigation, Formal analysis, Data curation, Writing - original draft. **Joel Brynielsson:** Methodology, Investigation, Formal analysis, Data curation, Writing - original draft. **Ulrik Franke:** Methodology, Investigation, Formal analysis, Data curation, Writing - original draft.

Acknowledgments

This work was partially funded by the Swedish Armed Forces. We would like to thank the Swedish financial sector's private-public partnership, FSPOS, and Josefine Rosén, 4C Strategies, for assistance in conjunction with the data collection phase, as well as all the survey respondents and interviewees.

REFERENCES

Accenture. In: Technical Report. Future Cyber Threats - Extreme but Plausible Threat Scenarios in Financial Services; 2019.

Agrafiotis I, Nurse JRC, Goldsmith S, Creese S, Upton D. Defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 2018;4(1). doi:10.1093/cybsec/tyy006.

Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL. How integration of cyber security management and incident response enables organizational learning. J. Assoc. Inf. Sci. Technol. 2020;71(8):939–53. doi:10.1002/asi.24311.

Alami A. Why do information technology projects fail? Procedia Comput. Sci. 2016;100:62–71.

Artman H, Garbis C. Situation awareness as distributed cognition. In: Eds. Cognition and Cooperation. Proceedings of the 9th Conference of Cognitive Ergonomics; 1998. p. 151–6.

Arvidsson N. The payment landscape in Sweden. In: Teigland R, Siri S, Larsson A, Puertas AM, Bogusz CI, editors. In: The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond. Routledge; 2018. p. 238–52. doi:10.4324/9781351183628-14.

BAE. In: Technical Report. The Evolving Advanced Cyber Threat to Financial Markets. SWIFT and BAE Systems; 2018.

Barford P, Dacier M, Dietterich TG, Fredrikson M, Giffin J, Jajodia S, Jha S, Li J, Liu P, Ning P, Ou X, Song D, Strater L, Swarup V, Tadda G, Wang C, Yen J. Cyber SA: Situational awareness for cyber defense. In: Advances in Information Security, 46. Boston, MA: Springer; 2010. p. 3–14. doi:10.1007/978-1-4419-0140-8_1.

Bartnes M, Moe NB, Heegaard PE. The future of information security incident management training: a case study of electrical power companies. Comput. Secur. 2016;61:32–45. doi:10.1016/j.cose.2016.05.004.

BCBS. In: Technical Report. Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version. Bank for International Settlements; 2006.

BCBS. In: Technical Report. Basel III: Finalising Post-Crisis Reforms. Bank for International Settlements; 2017.

BCBS. In: Technical Report. Cyber-Resilience: Range of Practices. Bank for International Settlements; 2018.

Bernier M. In: Technical Report. Military Activities and Cyber Effects (MACE) Taxonomy. Defence R&D Canada; 2013.

Bessis J. Risk Management in Banking. third ed. John Wiley & Sons; 2010.

Bhasin M. Mitigating cyber threats to banking industry. Chart. Account. April 2007:1618–24.

Biener C, Eling M, Wirfs JH. Insurability of cyber risk: an empirical analysis. Geneva Pap. Risk Insurance-Issues Practice 2015;40(1):131–58.

Björn M. The adoption of online banking in Sweden. In: Teigland R, Siri S, Larsson A, Puertas AM, Bogusz CI, editors. In: The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond. Routledge; 2018. p. 99–108. doi:10.4324/9781351183628-6.

Blakley B, McDermott E, Geer D. Information security is information risk management. In: Proceedings of the 2001 workshop on New security paradigms (NSPW01). ACM Digital Library; 2001. p. 97–104.

Bloch M, Blumberg S, Laartz J. Delivering large-scale IT projects on time, on budget, and on value. McKinsey & Company Insights & Publications 2012:2–7.

Borum R, Felker J, Kern S, Dennesen K, Feye T. Strategic cyber intelligence. Inf. Comput. Secur. 2015;23(3):317–32. doi:10.1108/ICS-09-2014-0064.

Branlat M. Challenges to Adversarial Interplay Under High Uncertainty: Staged-World Study of a Cyber Security Event. Ohio State University; 2011.

Britz MT. Computer Forensics and Cyber Crime: An Introduction. third ed. London, United Kingdom: Pearson; 2013.

Bronfenbrenner U. Toward an experimental ecology of human development. Am. Psychol. 1977;32(7):513–31. doi:10.1037/0003-066X.32.7.513.

Brynielsson J, Franke U, Varga S . Cyber situational awareness testing. In: Advanced Sciences and Technologies for Security Applications. Cham, Switzerland: Springer; 2016. p. 209–33. doi:10.1007/978-3-319-38930-1_12.

Burger EW, Goodman MD, Kampanakis P, Zhu KA. Taxonomy model for cyber threat intelligence information exchange technologies. In: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS '14). ACM Digital Library; 2014. p. 51–60.

Cebula JL, Young LR. In: Technical Report. A Taxonomy of Operational cyber Security Risks. Carnegie Mellon University, Software Engineering Institute; 2010.

Cooke IA, Scott A, Sliwinska K, Wong N, Shah SV, Liu J, Schuster D. Toward robust models of cyber situation awareness. In: AHFE 2018, AISC 782. Springer International Publishing AG; 2019. p. 127–37. doi:10.1007/978-3-319-94782-2_13.

Copeland J. In: Strategy Research Project. Emergency Response: Unity of Effort Through a Common Operational Picture. Carlisle, PA: U.S. Army War College; 2008.

Earle TC. Trust, confidence, and the 2008 global financial crisis. Risk Anal. 2009;29(6):785–92.

Endsley MR. Toward a theory of situation awareness in dynamic systems. Hum. Factors 1995;37(1):32–64.

European Central Bank. In: Technical Report. TIBER-EU Framework - How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. European Central Bank; 2018.

Fenz S, Heurix J, Neubauer T, Pechstein F. Current challenges in information security risk management. Inf. Manag. Comput. Secur. 2014;22(5):410–30. doi:10.1108/IMCS-07-2013-0053.

Franke U. Optimal IT Service Availability: Shorter Outages, or Fewer? IEEE Trans. Netw. Serv. Manag. 2012;9(1):22–33. doi:10.1109/TNSM.2011.110811.110122.

Franke U, Brynielsson J. Cyber situational awareness—A systematic review of the literature. Comput. Secur. 2014;46:18–31. doi:10.1016/j.cose.2014.06.008.

FSPOS AG KON. In: Technical Report. FSPOS Vägledning för Krishantering [FSPOS Guide to Crisis Management]. FSPOS; 2017.

Goldin I, Vogel T. Global governance and systemic risk in the 21st century: lessons from the financial crisis. Glob. Policy 2010;1(1). doi:10.1111/j.1758-5899.2009.00011.x.

Goldstein J, Chernobai A, Benaroch M. An event study analysis of the economic impact of IT operational risk and its subcategories. J. Assoc. Inf. Syst. 2011;12(9):1.
Guldentops E. The IT dimension of Basel II. Inf. Syst. Control J. 2004;6:17–20.
Haavik TK. Chasing shared understanding in drilling operations. Cogn. Technol. work 2011;13:281–94. doi:10.1007/s10111-010-0166-z.
Hager RS. In: Technical Report. Current and Future Efforts to Vary the Level of Detail for the Common Operational Picture; 1997.
Harrald J, Jefferson T. Shared situational awareness in emergency management mitigation and response. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07); 2007. p. 23. doi:10.1109/HICSS.2007.481.
Hauswald R, Marquez R. Information technology and financial services competition. Rev. Financ. Stud. 2003;16(3):921–48. doi:10.1093/rfs/hhg017.
Hull J. Risk Management and Financial Institutions. fourth ed. John Wiley & Sons; 2015.
Ibrahimovic S, Franke U. A probabilistic approach to IT risk management in the Basel regulatory framework: a case study. J. Financ. Regul. Compliance 2016;25:176–95. doi:10.1108/JFRC-06-2016-0050.
Jajodia S, Albanese M. An Integrated Framework for Cyber Situation Awareness. Springer Cham; 2017. p. 29–46.
Johnson KN. Cyber risks: emerging risk management concerns for financial institutions. Georgia Law Rev. 2015;50(1):131–42.
Klein G. Situation Awareness Analysis and Measurement. In: Endsley MR, Garland DJ, editors. Analysis of situation awareness from critical incident reports. Mahwah, NJ: Lawrence Erlbaum Associates, Inc.; 2000.
Kopp E, Kaffenberger C, Wilson C. In: IMF Working Paper. Cyber risk, market failures, and financial stability; 2017.
Kroeger F. The development, escalation and collapse of system trust: from the financial crisis to society at large. Eur. Manag. J. 2015;33(6):431–7. doi:10.1016/j.emj.2015.08.001.
Leaver M, Reader TW. Human factors in financial trading: an analysis of trading incidents. Hum. Factors 2016;58(6):814–32.
Manshaei MH, Zhy Q, Alpcan T, Ar TB, Hubaux J-P. Game theory meets network security and privacy. ACM Comput. Surv. 2013;45(3):1–39. doi:10.1145/2480741.2480742.
Mavroeidis V, Bromander S. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In: 2017 European Intelligence and Security Informatics Conference (EISIC); 2017. p. 91–8. doi:10.1109/EISIC.2017.20.
McNeese MD, Pfaff MS, Connors ES, Obieta JF, Terrell IS, Friedenberg MA. Multiple vantage points of the common operational picture: Supporting international teamwork. In: Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting - 2006; 2006. p. 467–71.
Nastase P, Unchiasu SF. Implications of the operational risk practices applied in the banking sector on the information systems area. Account. Manag. Inf. Syst. 2013;12(1):101.
Norri-Sederholm T, Joensuu M, Huhtinen A-M. Ensuring information flow and the situation picture in public safety organisations situation centres. In: Scanlon M, Le-Khac N-A, editors. In: Proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS 2017; 2017. p. 267–73.
Nyre-Yu M, Gutzwiller RS, Caldwell BS. Observing cyber security incident response: qualitative themes from field research. Proc. Hum. Factors Ergon. Soc. Annu. Meet. 2019;63(1):437–41. doi:10.1177/1071181319631016.
Önal MZ. An aggregated information technology checklist for operational risk management. J. BRSA Bank. Financ. Mark. 2007;1(2):49–76.
Patrick J, Morgan PL. Approaches to understanding, analysing and developing situation awareness. Theor. Issues Ergon. Sci. 2010;11(1–2):41–57. doi:10.1080/14639220903009946.
Paul CL, Whitley K. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In: Marinos L, Askoxylakis I, editors. In: Human Aspects of Information Security, Privacy, and Trust. Berlin, Heidelberg: Springer Verlag; 2013. p. 145–54.
Rachev ST, Chernobai A, Menn C. Empirical examination of operational loss distributions. In: Perspectives on Operations Research. Springer; 2006. p. 379–401.
Randazzo MR, Keeney M, Kowalski E, Cappelli DM, Moore AP. Insider threat study: illicit cyber activity in the banking and finance sector; 2005. doi:10.1184/R1/6574517.
Rifaut A, Feltus C. Improving operational risk management systems by formalizing the Basel II regulation with goal models and the ISO/IEC 15504 approach. Proceedings of the CAISE06 Workshop on Regulations Modelling and their Validation and Verification (ReMo2V), 2006.
Rosenberg H. In: Technical Report. Banking & Financial Services Cyber Threat Landscape report. Intsights; 2019.
Rosenquist, M., 2009. Whitepaper: Prioritizing information security risks with threat agent risk assessment.
Roth EM, Multer J, Raslear T. Shared situation awareness as a contributor to high reliability performance in railroad operations. Organ. Stud. 2006;27(7):967–87. doi:10.1177/0170840606065705.
Salas E, Prince C, Baker DP, Shrestha L. Situation awareness in team performance: implications for measurement and training. Hum. Factors 1995;37(1):123–36. doi:10.1518/001872095779049525.
Salmon PM, Stanton NA, Walker GH, Baber C, Jenkins DP, McMaster R, Young MS. What really is going on? Review of situation awareness models for individuals and teams. Theor. Issues Ergon. Sci. 2008;9(4):297–323. doi:10.1080/14639220701561775.
Salmon PM, Stanton NA, Walker GH, Green D. Situation awareness measurement: a review of applicability for C4I environments. Appl. Ergon. 2006;37(2):225–38.
Shin B, Lowry PB. A review and theoretical explanation of the 'cyberthreat-intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. Comput. Secur. 2020;92:1–16. doi:10.1016/j.cose.2020.101761.
Shin N. The impact of information technology on financial performance: the importance of strategic choice. Eur. J. Inf. Syst. 2001;10(4):227–36. doi:10.1057/palgrave.ejis.3000409.
Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur. 2016;60:154–76. doi:10.1016/j.cose.2016.04.003.
Sophronides P, Papadopoulou C-A, Giaoutzi M, Scholten HJ. A common operational picture in support of situational awareness for efficient emergency response operations. J. Future Internet 2017;2(1):10–35. doi:10.18488/journal.102.2017.21.10.35.
Steen-Tveit K, Radianti J. Analysis of common operational picture and situational awareness during multiple emergency response scenarios. In: Franco Z, Gonzlez JJ, Cans JH, editors. In: Proceedings of the 16th ISCRAM Conference; 2019. p. 199–208.
Svensson S. Staber och Stabsarbete vid Kriser, Risker och Olyckor [Staffs and Staff Work in Crises, Risks and Accidents]. Studentlitteratur; 2007.
Tadda GP, Salerno JS. Overview of Cyber Situation Awareness, 46. Springer, Boston, MA, Cyber Situational Awareness; 2010. p. 15–35.

Tendulkar R. In: Staff Working Paper. Cyber-Crime, Securities Markets and Systemic Risk. IOSCO Research Department and World Federation of Exchanges; 2013.
Tounsi W, Rais H. A survey of technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. 2018;72:212–33. doi:10.1016/j.cose.2017.09.001.
U.S. Congress. In: Technical Report. Effects of Information Technology on Financial Services Systems. Alexandria, VA, USA: U.S. Congress, Office of Technology Assessment; 1984.
Valaker S, Hrem T, Bakken B. Connecting the dots in counterterrorism: the consequences of communication setting for shared situation awareness and team performance. J. Conting. Crisis Manag. 2018;26(4):425–39. doi:10.1111/1468-5973.12217.
Varga S, Brynielsson J, Franke U. Information requirements for national level cyber situational awareness. In: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM); 2018. p. 774–81. doi:10.1109/ASONAM.2018.8508410.
Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Comput. Secur. 2019;87:1–13. doi:10.1016/j.cose.2019.101589.
Wateridge J. How can IS/IT projects be measured for success? Int. J. Proj. Manag. 1998;16(1):59–63.
Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Comput. Secur. 2014;44:1–15. doi:10.1016/j.cose.2014.04.005.
Wolbers J, Boersma K. The common operational picture as collective sensemaking. J. Conting. Crisis Manag. 2013;21(4):186–99. doi:10.1111/1468-5973.12027.
Woods DW, Böhme R. In: IEEE Symposium on Security & Privacy. Systematization of knowledge: Quantifying cyber risk; 2021. In press. Preprint accessed from https://informationsecurity.uibk.ac.at/pdfs/WB2020_sok_cyberrisk_snp.pdf.

Stefan Varga, Swedish Armed Forces, is a professional Ph.D. student (Computer Science) at the Royal Institute of Technology (KTH). Major (air force) Varga has worked in the military specialty fields of air surveillance, communications, and intelligence. He is an armed forces military specialist in command and control systems development. Stefan is a graduate from the Advanced Management Program at the Information Resources Management College of the U.S. National Defense University. He is a NATO cyber security professional trained by the U.S. Naval Post Graduate School and the NATO School Oberammergau, Germany. His research interests include cyber security, cyber situation awareness, and decision support.

Joel Brynielsson is a research director at the Swedish Defence Research Agency (FOI) and an associate professor at the Royal Institute of Technology (KTH). He previously worked as an assistant professor at the Swedish Defence University. Joel is Docent (Habilitation) in Computer Science (2015), and holds a Ph.D. in Computer Science (2006) and an M.Sc. in Computer Science and Engineering (2000) from KTH. His research interests include uncertainty management, information fusion, probabilistic expert systems, the theory and practice of decision-making, command and control, operations research, game theory, web mining, privacy-preserving data mining, cyber security, and computer security education. He is the author or coauthor of more than 150 papers and reports devoted to these subjects.

Ulrik Franke is a senior researcher at Research Institutes of Sweden (RISE). Prior to joining RISE, he was a senior scientist at the Swedish Defence Research Agency (FOI). His research interests include IT service availability, enterprise architecture, cyber insurance, and cyber situation awareness. He received his M.Sc. and Ph.D. degrees in 2007 and 2012, respectively, both from the Royal Institute of Technology (KTH) in Stockholm, Sweden.