

On the Collaborative Practices of Cyber Threat Intelligence Analysts to Develop and Utilize Tacit Threat and Defence Knowledge

On Existing Practices, Shortcomings, System Circumventions and Implications for Design

Jan M. Ahrend

Department of Computer Science
University of Oxford
Oxford, England
ahrend@cs.ox.ac.uk

Marina Jirotko

Department of Computer Science
University of Oxford
Oxford, England
marina.jirotko@cs.ox.ac.uk

Kevin Jones

Airbus Group Innovations
Newport, England
kevin.jones@airbus.com

Abstract— While the need for empirical investigations of cybersecurity analysts' collaborative work practices is widely acknowledged, research efforts are fairly limited. This paper aims to provide empirical evidence to support a deeper consideration for the seemingly intangible collaborative practices that situational awareness in cybersecurity relies on and add to our understanding of what it means to “do” threat intelligence. In particular, it aims to unpack the informal forms of collaboration and coordination at work that build tacit knowledge about threat actors and defenders and that span across time, people and tools to inform the translation of threat information into actionable threat intelligence. In-depth semi-structured interviews and diary studies are conducted at three cyber threat intelligence service providers (N=5) and analyzed using thematic analysis. This paper introduces the concept of Threat and Defence Knowledge, tacit knowledge that analysts within an organization form over time and utilize through informal ways of becoming aware of this knowledge, making it available and correlating it.

We find that a lack of accessibility to knowledge about relevant threat and defence factors can reduce analysts' effectiveness at arriving at actionable threat intelligence and hence reduce the ability to be alerted in advance about cyber threats, to contain damage and obtain situational awareness. Perceived and potential shortcomings of the existing processes and tools are presented, and practices to circumvent the existing systems investigated and implications for design are considered.

Keywords—*cyber situational awareness; collaborative situation awareness for decision making; team and group SA*

I. INTRODUCTION

The increasing connectivity of IT infrastructure has rendered actors more vulnerable to both directed and undirected cyberattacks. Their effects may range from threatening the foundation of modern information society by paralyzing the national-wide network and obstructing e-commerce, to causing catastrophic failure of nation-wide information infrastructure which most developed nations now rely upon to govern and run a country. These risks are not only theoretical; serious effects can be observed in industry and governance that demonstrate the need to advance our nations' and organizations' cyberdefences [1]. Global implications will rise, as

technologies will continue to penetrate further and further into governments', enterprises' and citizens' everyday lives. Due to these potentially severe effects, attention and effort has been appointed to the ability to be alerted in advance about cyber threats and contain damage. To advance this ability, the majority of literature investigates how to add to the quantity and quality of threat information that is distributed by considering the design of sharing mechanisms. The existing literature, however, is only high-level, understands the transformation of threat information into actionable threat intelligence (TI) as a practice of an isolated user or is part of technology-oriented approaches. To date, little is known about the local practices of threat analysts from a collaborative perspective. Further, an understanding of practitioners' actual work practices, the current models with which they work, and potential shortcomings of the current technology they use to perform these activities is largely missing. Building upon empirical data may help to reduce the discrepancy between what security practitioners actually want and what we as researchers perceive as what they want [2]. Recent reviews of the literature on Situational Awareness (SA) have emphasized the need for empirical data of practitioners' collaboration [3]. This understanding can help designers develop systems that support their practices as cyberdefence becomes increasingly complex. Given these limitations, the research question addressed by this paper can be framed as: How do cyber threat analysts internally collaborate to manage TI and what are some of the challenges and opportunities they are facing when working together?

TI service providers fight on the frontiers of cyberspace to prevent cyberattacks against our financial banks, energy suppliers and governments. These highly specialized organizations transform large amounts of threat information into custom intelligence reports for their clients. This research takes the unique approach of studying the collaborative practices that analysts of TI service providers already employ and so heavily rely on to transform threat information into actionable TI reports for their clients.

We conduct semi-structured interviews and user diary studies to explore threat analysts' day-to-day practices and unpack their collaborative practices. We find that analysts

develop and rely on knowledge about threats and the environment they defend when transforming threat information into actionable TI. Such knowledge is developed throughout time and becomes tacit by analysts. We also find that analysts follow formal and informal practices to uncover and utilize tacit knowledge from their colleagues. In the light of these practices, shortcomings in existing practices were identified, participants' practices to circumvent locally present solutions explored and lastly implications for design introduced.

II. BACKGROUND

Cybersecurity is a dynamic trade-off, a balancing act between attacker and defender [4]. Attackers are in the "position of the interior" [5], meaning they often have a first-mover advantage and are faster in incorporating new technologies where they only need to find one flaw that allows a way through the defences in increasingly more complicated and distributed technologies [6]. This stands in contrast to cybersecurity defenders who have a natural disadvantage through their constant position of responding, for example, through better intrusion detection rules [7]. This imbalance opens a gap which is often referred to as the "scope of defection" [4]. Defenders are trying to decrease the scope, adversaries to increase their window of opportunity. That scope of defection is never static but rather dynamic since attack vectors change every day, targets surface every week and values of what's at stake can change every second [8].

SA describes an individual's perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future [9]. As suggested by Endsley [9], the words perception, comprehension, and projection can be taken to describe the progressive awareness levels ranging from (i) basic perception of important data, (ii) interpretation and combination of data into knowledge, and (iii) ability to predict future events and their implications. As one advances through these levels, decision making capabilities are said to be improved [3]. Given the complexity of cyberdefence, resulting from the interconnectivity, dependencies and changing use of technology, no defending party can fully foresee what has to be done to keep the environment secure [7], [10]. As a result, it is impossible for defenders to access and utilize all relevant forms of information, resulting in a large degree of uncertainty. Taking the understanding of cyberdefenders' ability to make informed decisions, it becomes apparent that the role of information to reduce uncertainty is crucial at all stages of SA.

A. Threat information to reduce uncertainty and TI to provide actionable advice for defence

The uncertainty in real-time SA mostly arises from the invisibility of attackers in cyber space — it is hard to know who and where the attackers are, what intentions they have, and what tools and methods they use to carry out attacks. The existing attention in cyberdefence is largely focused on the data that is collected by internal sensors that can only detect activities that have already occurred locally (i.e. intrusion detection systems). Consequently, this could result in a disastrous warning failure against a variety of attacks that are unknown to local defenders [11]. As a result, the ability to be alerted in advance about threats by reducing uncertainty and increase SA through

externally originating threat information has taken on great interest and is evolving into an important field which need is generally understood among political [12]–[14], economics and security experts alike [15], [16].

One approach of cyberdefenders with which this is achieved is through the observation that cyberattackers often prey on similar types of organizations, so that an incident at one location can be a precursor to an attack at another similar location [17]. As a result, knowledge about a threat can be distributed across individual defenders. This leads to what is commonly referred to as TI, which can be defined as evidence-based knowledge including context, mechanisms, indicators, implications and actionable advice that can be used to inform decisions [18]. This TI encompasses the pooling of information about new threats, new vulnerabilities and insights on new defences against all kinds of attacks and requires the distributed information to be manually or automatically gathered from different locations on the Internet [14], [19]. Goodall et al. [20, p. 343] was one of the first to document the daily routines of operators scanning the Internet "for news of the latest attacks, vulnerabilities, and IDS signature updates". Such information may take the form of "unstructured reporting and third party data: RSS feeds, vendor reports, government intelligence reports, databases of cyber threat actors, social media streams, IP information, and domain reputation feeds" [21] and include threat information and tactics, techniques and procedures that support the local response [22].

Several benefits are associated with the practice of managing TI. Short-term, it (1) supplements the knowledge gained from local sensors and help to identify trends, particularly with regard to undirected malware (e.g., computer worms) that might not otherwise be recognized due to the noise of internal network traffic [16], [23], (2) helps to be on alert for similar attacks that took place elsewhere [14], (3) and helps to discover unknown incidents or accidents by detecting patterns in the activity on systems of different organizations [24, p. 458]. Further, it (4) supports the facilitation of appropriate local responses [19] to (5) prevent or mitigate as many accidents as possible [14] and (6) contain damage [17]. Thereby, it can (7) help to employ precautionary measures against consequences of attacks such as revoking user credentials like Facebook and Diapers did after 130 million Adobe passwords leaked [25]. Ultimately, TI can (8) help to gain a better a better view of global network attack activity [19], [23] and (9) ultimately increase cyber SA [3].

The significance and potential of TI has not only received growing attention in academia but industry as well. Various general purpose platforms exist that pool cyber TI, such as Norse Dark Intelligence [26], CERTStation [27] or Sicherheitstacho.eu [28]. Recently, more sophisticated and customizable platforms emerged. To name one example, in December 2015, EclecticIQ announced a platform for threat analysts that provides advanced intelligence gathering, analysis and real-time collaboration with internal and external partners [29].

B. From technological considerations to individuals and collaborations of individuals

The majority of the literature on SA draws on technology-oriented approaches [3], [30], [31] and while work in this area is generally believed to be existential to attain SA, it is built upon technical implementation challenges rather than individuals' practices and collaborations of individuals' needs and limitations that give these tools purpose. Technology-oriented approaches in SA, such as tool implementations, architectures, and algorithms [32]–[34], data fusions [35] and visualizations [36]–[38], prioritize computer-based information processing and technology-mediated communication over humans and their communicative collaboration [39]. It follows a functionalist paradigm, which approaches the subject from an objectivist point of view that aims to regulate and control all organizational affairs [30]. These approaches are targeted at closing-down technology-centred problems, rather than opening up a technology-supported system of human-activity for examination and change [40]. While expanding the powers of technology is a necessary activity, research results have shown that is rarely sufficient in itself [41]. In a sense, these research efforts seem to follow “top-down” approaches to studying and developing cyberdefence support that impose what is best for defenders whilst lacking empirical data. Empirical studies on the impact of new technology on actual practitioners, their collaboration and practices have revealed that new systems often have surprising consequences or even fail [2], [42] and their existing practices need to be taken into consideration when designing technology [41]. Franke and Brynielsson [3, p. 27] conclude their literature review on SA that “there is plenty of work dedicated to cyber SA in industrial control systems, or general work on algorithms and information fusion in intrusion detection systems”. In contrast, less research has been devoted to user centred approaches and that “overall, it seems that there is potential for making more empirically based research” [3, p. 27].

As approaches to bolster cybersecurity have evolved, an increasing amount of consideration [43]–[45] has been devoted to human users and supporting their interactions with systems in relation to information security technologies. In contrast to technology-oriented approaches, literature on the human side of SA concerns the human capacity of being able to “comprehend” the technical implications and draw conclusions in order to come up with informed decisions [3]. A smaller, but still significant body of literature follows a more traditional approach to studying and designing for the interactional factors in cyber SA and cyberdefence by drawing upon cognitive methods and approaches. For instance, researchers have investigated SA by trying to understand it as a cognitive process in the individual defender's mind. Reflecting trends within mainstream Human-Computer Interaction (HCI), methods inspired by Psychology, such as cognitive task analysis have been employed to refer to individuals' mental states [46]–[48]. Apart from work that directly focused on cyber SA, there is a large body of literature that is studying the perception and comprehension of risk information to understand how individuals' perception and interpretation of data may differ [49]–[53].

But even when we make the human the centre of attention, it is often not enough, and more sophisticated methods are needed to obtain a more holistic understanding of the needs and limitations of individuals who are acting, often in collaboration, within the complex socio-technical environment of cybersecurity. These cognitive accounts of SA aim to arrive at a quantitative measurement of SA and their data collection and analysis is mainly centred around network traffic, rather than the complexity of intra-organizational collaboration.

C. Organizational studies in cybersecurity

An alternative account of studying cyberdefence is presented by considering the social and organizational context, in what has become known as the “turn to the social” [54], [55]. According to Grudin [56], HCI is passing into a stage that focuses on the social context in which activities are embedded. The focus shifts from individual users and their interaction with technology to social contexts and work settings that work occurs in. With the goal to support social and organizational practices, the tools to study groups of end-users have adapted. Applied methodologies shifted from a basis in the cognitive sciences to more qualitative sociology and the social sciences and found increasing application in HCI.

A turn to the social can also be observed in the field of cybersecurity. Beznosov and Beznosova's [31] literature review on public research in computer security concludes that the highest potential for making progress in the attacker-defender game is to involve social and collaborative factors, organizational behavior and structure as well as social capital aspects that are currently not high on the computer security research agenda. They define the social aspects of security as activities that are exclusively due to interactions among more than one individual. Relatable back to the dynamics of the scope of defection, the authors conclude that “for research in computer security to sustain the arms race, it ought to explore the social dimension of the problem space” [31, p. 425]. The authors further conclude that competitive advantage can be gained for whoever side employs social factors better.

A smaller body of literature has studied the social and organizational factors in cybersecurity by considering the collective of cyberdefenders and their collaboration. Researchers in the field of system administration are investigating the work routine of general system administration work, with some focus on security and network admins [57]–[61]. IT work was found to require a variety of skills, whereby collaboration among team members is of particular importance in the day-to-day operations [62], [63]. It has been found that existing tools often do not assist system administrators efficiently and effectively in their daily routines [58], [59], [64], [65]. For instance, Tahir and Brézillon [66] write that communication processes surrounding IT information usage through databases are often complex due to a variety of disciplines that actors come from and the context in which for instance security incident solving occurs may not be shared and understood in the same way by all users. Kandogan et al. [67] have written about communities of system administrators and find the broader communities that system administrators belong to, such as informal groups of people who share knowledge, tools and advice, of great importance. While system administrators' work is not particularly the same as for instance

TI analysts, they often involve tasks and processes to protect cyber assets. Comparing security and other IT work, Haber and Kandogan [57] found that security practitioners deal with a higher complexity in their work.

Similarly, literature in cybersecurity has focused on the collaborative aspects of cyberdefenders. Research [20], [61], [63], [68]–[72] emphasized the need to understand how practitioners use tools to support collaboration and information sharing between stakeholders within the organization. The practice of cyberdefence was found to be distributed across the organization and requires collaboration between practitioners [60], [61], [69], [71]. Casey [73] conducted a case study of an intrusion into a network and expressed the need for better means of collaboration between system administrators, incident handlers and forensic examiners. Similarly, Werlinger et al. [74] conducted interviews with IT security practitioners on their security incident response practices and found the activity to be highly collaborative and reliant on tacit knowledge [75]. The authors find that the practices of cyberdefence are distributed across multiple employees from different organizational units or groups. Botta et al. [60], [76] conduct interviews to investigate the organizational practices of cyberdefenders and how they achieve distributed cognition [77] within the organization. Tyworth et al. [78] interviewed security analysts and similarly find that cyber SA is distributed across human operators and technological artifacts operating in four different functional areas: intrusion detection, threat landscape analysis, operations and policy and management. Each operational domain is separated by physical and virtual boundaries with individual communities of practice, which have distinct knowledge, terminologies, foci, understandings and practices and may even lie distributed outside the organization. The collaboration and sharing of information across the domains can be understood as ‘boundary objects’, which span the boundaries of the practices of communities that are commonly understood by all communities. Individuals working in the functional domains often customize the tools and operational purposes to access information in other domains.

Cyberdefence is a complex socio-technical environment that is by nature distributed among defenders, attackers and technologies, rather than an individual, isolated defender. This paper builds upon the notion of the “turn to the social” by considering the wider social context and including more complex and unexplored forms of collaboration through which tacit knowledge is utilized. We are interested in the under-explored practices of tacit knowledge that analysts build over time when working on incidents and that they rely on in their day-to-day work to form SA and contain damage.

III. METHOD

Since this study aims to explore what it means to “do security” at cyber TI service providers, we are interested in uncovering manifestations of the day-to-day practices of TI analysts. We aim to uncover how analysts’ practices when transforming threat information into actionable intelligence are mediated through artefacts in the environment such as technologies, information and team members.

For this study, a collaboration and non-disclosure agreement was signed with a TI affiliated organization. The

collaborating organization is a software company offering an online platform for collecting, analyzing and collaborating on cyber threat information. Users of its platform are Security Operation centres and managed security service providers for TI. TI service providers that the organization has previously established contact and trust with were invited by email to participate in the study. The invitation was sent by the Chief Technical Officer, the Head of User Experience and the principal researcher of this paper who was introduced as “a PhD researcher at the University of Oxford”. The research participation invitation followed ethical approval from the University.

Due to the fairly new establishment of the field of TI and the paucity of empirical accounts of their collaborative practices, our study followed an explorative approach by collecting qualitative data through semi-structured interviews (N = 5; 1 female, 4 male). Two rounds of interviews were conducted, resulting in a total of 10 interviews across three companies, as outlined in Table 1. The average age of the studied organizations was 12 years and the average employee size was 129. All participants had a technical background. Each interview lasted 60 minutes and was conducted via Skype. Individuals willing to participate gave consent to the conditions of the interviews, were briefed prior to the interviews and reminded to not disclose client-sensitive information. Participants did not receive any form of monetary reward for their participation. The first interview round’s aim was to uncover the (1) background and context of the individuals’ roles and responsibilities within the team and the company, (2) TI perception, attitude and culture, and (3) daily routines, work processes, local language and how practices are embedded in everyday local activities. The second interview round questioned individuals’ internal and external collaboration, how work practices unfold and stretch into other members’ everyday practices and the interaction with technology. Participants were asked 12 main questions with additional probes:

- ☐ Can you tell me what your organization does?
- ☐ Can you describe your role and responsibility at your organization?
- ☐ Can you walk me through your workday yesterday?
- ☐ Tell me about the TI you were dealing with yesterday.
- ☐ Can you walk me through how you managed TI yesterday?
- ☐ What do you do after you gathered a specific threat information?
- ☐ Please tell me with whom you were in contact with within your organization yesterday.
- ☐ How/do you collaborate with external parties on TI?
- ☐ How does your organization publish TI and disseminate to customers?
- ☐ What technologies did you use during your work yesterday?

- ☐ Which tasks took the most of your time yesterday?
- ☐ Can you walk me through difficulties in managing TI you encountered yesterday?

The questions allowed us to probe the individual's perceived ways of collaboration and coordination and the practices' context. The interviews were transcribed and subsequently analyzed using thematic analysis [79].

TABLE I. PARTICIPANTS AND THEIR ORGANIZATIONAL ROLES

Interviewed company	Participant	Role
C1	P1: male	Senior TI Analyst
	P2: male	TI Collection Manager
C2	P3: male	Director of TI
C3	P4: male	Junior TI Analyst
	P5: female	Head of TI

During the first interview round, P4 faced difficulties recalling his work from the previous days and answer the interview questions. As a result, he and P5 were asked to document their work for five work days in a diary that was provided to them. It took the form of an Excel spreadsheet which asked for: a description of the tasks, task priority, task assignee, expected outcome or deliverable, information that was provided alongside the task, steps taken to complete the task, if and how they collaborated or communicated with anyone about the task, task completion time and satisfaction about the task outcome. The work diary was used in the second interview rounds as a reference for both interviewer and interviewee to ask and answer the questions.

IV. FINDINGS

In the following, tacit knowledge will be unpacked through empirical accounts of interviewees' day-to-day practices, beginning with a description of the organizational context in which they work and the TI reports that present an important work deliverable. Subsequently, the role tacit knowledge plays to generate these reports will be considered, and more specifically analysts' awareness, availability and correlation practices to utilize knowledge unpacked. Lastly, perceived and potential shortcomings will be discussed, practices to circumvent the existing tools presented and implications for design considered.

A. The context: TI service providers and TI reports as a deliverable

While the studied TI service providers' main service is to provide TI, they also provide other cyberdefence services, including forensics, cyber crime investigations, IT audits and security products. All organizations are within one locale and each department can have several teams of normally five to twelve team members. The TI teams follow open-source data and information to investigate their meaning for their clients and produce TI reports that they deliver to their clients. To transform threat information into actionable intelligence,

analysts enrich the information with relevant external information (e.g. DNS lookups) and internal information (i.e. documented and undocumented knowledge inside the organization) and subsequently triage the information to determine the probability of occurrence, the probable impact and means for mitigation or prevention for a client. The reports' aim is to support clients' (1) identification of a threat, (2) understanding of the threat, (3) decision whether to mitigate or not, and (4) provide actionable advice on how to mitigate the threat. Doing so, they provide clients with information about who is responsible for a threat, "including real names, locations and activities" (P3) and compile a threat profile. In addition, they provide guidance on how to technically respond to the threat under investigation. The TI analysts working on client incidents are also referred to "as staff augmentation" (P5) for their clients. TI service providers communicate with their client by email, over phone and via dedicated online platforms they provide their clients access to. The majority of clients are within the financial and energy sector. Naturally, the work and deliverables are of time critical nature. TI reports that the teams produce may thereby be relevant to all clients, specific to an industry sector or only applicable to an individual client. A TI report represents the result of an investigation from a cyber threat that the teams come across and decide to further investigate in the interest of their clients.

A TI team consists of a team leader, analysts and sometimes account representatives. The team leader is responsible for allocating and prioritizing incidents and tasks, overseeing the work and work outputs of the analysts, and often also perform the work that analysts do. Analysts are responsible for proactively identifying potential threats, responding to threat alerts that internal systems are triggering and analyzing threats by contextualizing a threat in terms of the originator of the threat (i.e. the threat actor), the likelihood of occurrence and the implications of an occurrence. Clients may have an account executive, who is the person inside the organization who is responsible for communicating with the client and is overseeing and collaborating when producing a TI report. One to four analysts are normally investigating a single incident and are usually involved in two to four active incidents at a time.

B. Development of threat and defence knowledge

In the course of an investigation, threat information and data is analyzed by considering its relevance and meaning for the defence context the service providers are producing TI reports for. Since the TI service providers are working with a variety of clients in various industries, multiple contexts exist that analysts need to consider in the analysis. Practitioners are translating threat information into intelligence by contextualizing attackers' intentions, methods and tools with their meaning for the defence context, including the defender's tools, infrastructure, methods and processes. Doing so, teams build tacit knowledge about the threat space and the defence space.

Defence knowledge: When working on incidents, analysts communicate through email and phone calls with clients and expand their knowledge of what TI is purposeful for individual clients. They learn more about the infrastructure, processes and tools in place and their needs and wants in regard to TI. While first knowledge is created and documented during onboarding

procedures of new clients, individuals increase their tacit knowledge through ongoing communication with clients centred around TI reports.

Threat knowledge: As analysts are transforming information into actionable intelligence, they are building a knowledge base about threat actors and their context, including characteristics such as their motivations, team size, nationality and their tools and methods, and more importantly the implications for the parties they intend to protect. As described by participants, this knowledge base is dynamic and not static. With more information that is associated with a threat, knowledge is expanded over time. Since the knowledge is specific to a threat information's application in a local context, the interpretation of threats can be different from one client to another.

By working on numerous threat incidents throughout time, analysts continuously expand their tacit knowledge about the defence and threat context.

C. Utilizing threat and defence knowledge

When producing TI reports, analysts do not only make use of the new threat information that was introduced by an investigation and build knowledge, but also rely on threat and defence knowledge (TDK) that has been acquired through previous cases, as previously outlined. This knowledge could present attack or defence-specific knowledge and be of direct relevance to the active investigation. As a result, analysts are constantly trying to connect new information with what is known about a threat and its implications for the defenders. To utilize threat and defence knowledge, analysts form a relationship between the information that is introduced in the active investigation (hereafter referred to as *seed information*) and existing tacit knowledge. Forming this relationship is, however, not trivial. To build upon TDK, analysts firstly need to be aware that potentially relevant knowledge exists, then render the original information for further investigation available and lastly be able to correlate it with the seed information to understand its relevancy in aiding in the active investigation.

Doing so, analysts may draw back on their own work, in case TDK has been built through an investigation they personally have been involved in. In this case, analysts' awareness about existing TDK is achieved by "remembering" (P1) or "just knowing" (P5). To make TDK available, analysts revisit the original TDK artefact (i.e. information that aided in forming the knowledge) on their local work machines.

It becomes more complex when analysts utilize TDK that is distributed and has been built by other analysts in investigations they have not personally been involved in, as it is often the case.

"One head is good. But two heads are better. (...) It's like a collective mind." (P1)

Analysts perceive it to be more effective to collaborate in an investigation with other analysts due to the "plurality of views and experiences" that can lead to "more interesting findings" (P4). At times, teams engage in formal meetings for collaborative problem solving. More interestingly, this also results in a set of informal forms collaboration and coordination

to become aware of relevant tacit knowledge, make it available and utilize it, as we will unpack in the following.

TDK Awareness: An analyst first becomes aware that a certain context of a threat or defence exists that is potentially relevant to the seed information they are presented with during the investigation. For analysts, it can present a major challenge "to know that there is some context associated with a threat indicator and what that context is and what it means" (P3). When forming a connection between TDK and seed information, an individual must reportedly be aware that potentially relevant TDK exists. Building this TDK Awareness can take formal and informal forms. Analysts build TDK awareness in weekly team meeting, in which team members' work is discussed. Analysts also heavily rely on casual day-to-day interactions with their colleagues and informal monitoring and overhearing, inside as well as outside their team or department. When the existence of TDK is not known to an analyst, he or she may actively question its existence. Doing so, an analyst must know *who* to ask for relevant TDK. Building knowledge about TDK awareness *gatekeepers* again relies on informal overhearing of what departments', teams' and individuals' usually work on in regard to types of threats and clients and the stage in the investigation.

TDK Availability: Subsequently, analysts often require the artefact that resulted in TDK to understand if and how it is of actual importance and an aid to the active investigation. These artefacts may take the form of raw data, custom extracted information in txt or xml files, work notes, screenshots, SQL databases or final TI reports. To make TDK artefacts available, analysts either request access through one of the internal systems on which it may be stored, or, as it is more often the case, ask the TDK originator directly for the artefact. In return, the TDK originator may have to ask for access permission from his or her superior. To request access and deliver the artefact, analysts fall back on an exchange via email: "Give me please information about this Android program that you investigated last week" (P3).

TDK Correlation: Lastly, analysts correlate the seed information with the TDK artefacts, which may take the form of manual or automatic analysis. Thereby, analysts aim to understand if the identified TDK is of actual relevance for the investigation, and if so, how it is relevant for supporting the investigation.

"I try to group this information to try to find the source of the malware or identify the guys who are behind this malware. (...) It can be with a report or it can be some information that can be processed with some scripts." (P5)

To do so, analysts often require an understanding of the artefacts' context in which they were obtained and used in the first place. To learn about the context, analysts retrieve information about its relevance and role in the investigation for which it was originally obtained. Doing so, analysts consider the trace, how it was obtained and how it was further processed. Analysts also consider time factors, such as when certain data points were obtained, or sensor data was created. To obtain information about these contextual TDK artefact factors, analysts actively ask the TDK originator about it face-to-face or via instant messenger. Alternatively, analysts may infer from

the originator's work documentation, including text files, Wiki entries and mind maps.

D. Perceived and potential shortcomings

Perceived and potential shortcomings were identified that may result in issues when utilizing TDK. For one, TDK is largely tacit and not formally documented. As reported, TDK awareness relies on casual day-to-day interactions and informal monitoring and overhearing. Awareness about TDK is further limited to teams and departments the analyst is engaged in due to the passive overhearing's dependency on physical proximity. Another factor that may add to a decrease in TDK utilization is potential loss of tacit knowledge, stemming from an unavailability of TDK originators (e.g. change of team-, department- or organization-affiliation) or memory loss. TDK artefacts on the other hand are documented, but achieving their availability and obtaining the necessary access rights can be difficult. The participants perceive the current work practice to be tedious and see value in opening up access restrictions to save time for accessing information. TDK artefact's context is at times documented but again often restricted to the originator's personal machine. As a result, utilizing TDK can rely on manual queries of an analyst and the TDK originator's ability respond accurately and holistically. In particular, to obtain TDK awareness, an analyst needs to manually query if relevant TDK exists, and if not, a decision to actively question others in the organizations needs to be made, which requires a decision on *when* to ask *whom* for *what* information. The time investment, technical requirements and dependency on tacit knowledge about TDK, TDK originators and TDK gatekeepers make collaborative TDK utilization problematic and may limit analysts' effectiveness in producing TI.

E. System circumvention

Internal systems are in place that enable analysts to upload seed information, TDK artefacts and the final TI reports. They act "like a database" (P2), in which all incidents are listed with their date of initiation, status and associated documents. The systems are build in-house and have continuously evolved for the last five to 16 years. These systems are reportedly often circumvented. Instead of uploading seed information and TDK artefacts, analysts store seed information on their personal machines. The material is at times uploaded to the system by the TDK originator when he or she was asked to share it. But even the occasional reactive documentation is often circumvented through transmission of the material via email. This practice is reportedly preferred due to the perceived ease of use, speed and reliability compared to experiences made when using the internal systems. The system is particularly circumvented when only a single file needs to be shared which can reportedly be easier and quicker achieved if it is sent by email.

"(...) they can just ask me." (P4)

These circumventive practices are reportedly supported by the individuals' perception that their work is rather individualistic and not directly relevant to other analysts. Another factor that supports system circumvention is the data cleaning TDK originators engage in prior to uploading seed information to the internal systems. Uploading all data as they are is not useful due to the sheer amount of data and information

that is "trash" and "inconvenient" to go through (P5). Analysts fear to clutter the systems, making it hard to distinguish between relevant material that lead to the desired TI reports and material that turned out to be irrelevant for this investigation. While described as irrelevant, analysts still store all artefacts on their personal machine, because it "could provide useful later" (P1).

"If it (the data) will be necessary in the future, I can use it or send it to my colleague." (P2)

Another reason for not uploading artefacts is the assumption that the servers will not have enough storage. As a result, only finalized versions of TDK artefacts and TI reports are uploaded.

F. Implications for design

The identified reliance on in-house past experience and the resulting potential impact of staff turnover invites considerations for supporting expert systems. Further, one way to consider the outlined process and system shortcomings and circumvention practices is by regarding them as a result of the ways TDK becomes tacit and largely undocumented. Consequently, a central system that incentivizes the act of documenting gained TDK may be able to support the awareness, availability and correlation practices of analysts. In particular, the system may support the indexation of the outlined formal and informal TDK practices by building a TDK awareness database. The aim could be to augment and assist analysts' existing TDK awareness practices, by providing automated and passive processes rather than the current reliance on manual and active processes to identify potentially relevant TDK. This may take the form of automated suggestions for potentially relevant TDK when interfacing with seed information. Beyond supporting the passive awareness and automatic discovery of relevant TDK, the system may support the availability of TDK artefacts by centralizing its documentation and its access right management in a purposeful way without "cluttering" the system. When TDK artefacts are uploaded, it may also be purposeful to support human-driven and algorithmic ways to support their traceability and contextualization in regard to the underlying investigation. Lastly, the system may support the utilization by not only centralizing TDK artefacts, but also the discussed contextual factors to reduce the dependency of analysts on TDK originators. More crucially, ways to provide sufficient motivation for analysts to centralize TDK seed information and their context in the first place need to be investigated. Some first design values that may be purposeful have been identified, including the ease of use, reliability and task completion time.

V. DISCUSSIONS

While TI is perceived by practitioners to be fairly individualistic work, their practices are highly collaborative [61], [69]. Cyberdefence is achieved through formal and informal collaboration in the studied settings, which may take a delayed form, is produced for other people and is built over time [80], [81]. TDK is distributed internally among systems and people and their personal machines, which presents a challenge to make it aware, available and utilizable. We found, that when investigating threat incidents, analysts heavily build upon their and their colleagues' previous work. Incidents are

solved by building upon analysts' undocumented, tacit knowledge [74] about their colleagues' work and developed TDK. TDK is thereby distributed across practitioners and is shared across time and space. This means, that achieving cybersecurity monitoring, in this context, is dependent on the collaboration and coordination of individuals within the space, to become aware of relevant knowledge and be able to make it available and utilize it.

By building upon empirical data to shape this research, we aimed to arrive at findings that may help reduce the discrepancy between what security practitioners actually *do* and *need*, and what we as researchers perceive as what they want and how they want it. While the necessity for empirical accounts of work practices is generally understood in cybersecurity and SA [3], [30], gaining field access remains a challenge due to the sensitive nature of cybersecurity work. Data access for this study was achieved by building a relationship with a cybersecurity company who acted as a gatekeeper with established links in the industry.

This study provided a brief glance into how analysts perceive the creation and utilization of threat and defence specific knowledge that is distributed across analysts. As it is typical for interviews, the elicited accounts of individuals' practices are limited. The tacit nature of the practices can make it difficult to retrieve meaningful insights from second-hand or abstract accounts of interview answers about operators' actions [82]. Employing diary studies proved to be helpful in two situations where interviewees were having difficulties recalling their daily routines and may further be a manifestation of the practices' tacit nature. Hence, more naturalistic data may help to expand and deepen the findings by providing more holistic accounts of their local practices. We need to understand practitioners' actual work practices, the current models with which they work and the tools they use to perform their tasks to understand the actual needs of TI analysts. This may best be achieved through ethnographically informed approaches. Other possible areas of investigation can build upon these explorative studies in the future such as neural networks to explore possibilities of undesirable outcomes and quantitative evaluations of the practices' and tools' effectiveness through benchmark studies and hypothesis driven experiments to drive measurable work impact.

The contributions of this paper are threefold. First, using empirical data, we have analyzed and described the practices, tacit knowledge, skills, and tools that security practitioners use to create and utilize TDK. The findings enhance the research community's understanding of the local practices of translating threat information into actionable TI. Second, this study identified perceived and potential shortcomings, the ways existing solutions are circumvented and considers implications for design. Lastly, opportunities for future research directions were identified.

VI. CONCLUSIONS

Acting upon threat information is the process of making it locally actionable. If and how to respond to cyber threats is dependent on the local context that defenders aim to defend and the threat that malicious actors pose. We find that this knowledge becomes tacitly distributed throughout the work and

directly informs future interpretations of threat information, hence affecting organizations' ability to be alerted in advance about cyber threats, to contain damage and increase SA. Practitioners thereby rely on a set of informal practices to become aware about the tacit knowledge that is distributed among analysts within the organization, make it available and lastly act upon it. In this context, we have unpacked informal practices that make cybersecurity "work" and that make existing solutions "fail". When designing supportive technologies, the tacit nature and resulting shortcomings should be taken into account. As such, we find that the creation and utilization of relevant knowledge is a process that TI analysts heavily rely on and that may be supported through software-driven process automation and augmentation to increase TDK documentation in a centralized system and support the automated discovery of relevant knowledge and work artefacts.

ACKNOWLEDGMENT

This work was funded through a sponsorship of an EPSRC Industrial CASE Award number OUCL/2013/JMA to the first author in which the industrial partner is Airbus Innovations. This work was greatly supported by the collaborating organization that wishes to remain anonymous. Special thanks to the CTO, CEO and UX Designer for making this research possible by providing data access and highly valuable guidance to the undertaking of the research summarized here. Lastly, we would like to thank the participating organizations and individuals for taking part in this study.

REFERENCES

- [1] Detica, "The Cost of Cyber Crime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office," 2011.
- [2] N. B. Sarter, D. D. Woods, and C. E. Billings, "Automation surprises," *Handb. Hum. factors Ergon.*, vol. 2, pp. 1926–1943, 1997.
- [3] U. Franke and J. Brynielsson, "Cyber situational awareness – a systematic review of the literature," *Comput. Secur.*, vol. 46, pp. 18–31, Jul. 2014.
- [4] B. Schneier, *Liars and outliers: enabling the trust that society needs to thrive*. John Wiley & Sons, 2012.
- [5] H. Jomini, *Traité de grande tactique, ou, Relation de la guerre de sept ans, extraite de Tempelhof, commentée et comparée aux principales opérations de la dernière guerre; avec un recueil des maximes les plus importantes de l'art militaire, justifiées par ces différen.* Paris: Giguët et Michaud, 1805.
- [6] B. Schneier, "Trust in Man/Machine Security Systems," *IEEE Secur. Priv.*, vol. 11, no. 5, pp. 96–96, 2013.
- [7] M. M. de Bruijne and J. J. van den Berg, "A theory driven research project to determine what collaboration design best supports the sharing of pragmatic cyber security related information between organisations," *Syst. Eng. Policy Anal. Manag.*, no. February, 2014.
- [8] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Secur. Priv.*, vol. 1, no. 14, pp. 33–39, 2003.
- [9] M. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 37, no. 1, pp. 32–64, 1995.
- [10] J. Li, X. Ou, and R. Rajagopalan, "Uncertainty and risk management in cyber situational awareness," *Cyber Situational Aware.*, pp. 51–68, 2010.
- [11] S. Lee, D. Lee, and K. Kim, "A conceptual design of knowledge-based real-time cyber-threat early warning system," in *Frontiers of High Performance Computing and Networking-ISPA 2006 Workshops*, 2006, pp. 1006–1017.
- [12] J. Finkle and J. Menn, "Keith Alexander, NSA Chief, Asks For Hackers' Help In Making Internet More Secure," 2012. [Online].

- Available: http://www.huffingtonpost.com/2012/07/28/keith-alexander-nsa_n_1712185.html. [Accessed: 20-Feb-2016].
- [13] N. Kroes, "Cyber-security – a shared responsibility," 2012. [Online]. Available: http://europa.eu/rapid/press-release_SPEECH-12-774_en.htm. [Accessed: 15-Jan-2016].
 - [14] F. Maude, "Cyber Security Information Sharing Partnership," 2013. [Online]. Available: <https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme>. [Accessed: 15-Jan-2016].
 - [15] E. Brunner and M. Suter, "International CIP Handbook 2008/2009," in *CRN Handbooks*, 4th ed., E. Brunner and M. Suter, Eds. ETH Zurich, 2008.
 - [16] M. Brunner, H. Hofinger, C. Roblee, P. Schoo, and S. Todt, "Anonymity and privacy in distributed early warning systems," *Crit. Inf. Infrastructures Secur.*, pp. 81–92, 2011.
 - [17] R. Klump and M. Kwiatkowski, "Distributed ip watchlist generation for intrusion detection in the electrical smart grid," *Crit. Infrastruct. Prot. IV*, pp. 113–126, 2010.
 - [18] CERT UK, "An Introduction To Threat Intelligence," 2015. [Online]. Available: <https://www.cert.gov.uk/wp-content/uploads/2015/03/An-introduction-to-threat-intelligence.pdf>. [Accessed: 15-Jan-2016].
 - [19] P. Amsel, M. Apel, J. Biskup, U. Flegel, and M. Meier, "Early Warning System on a National Level – Project AMSEL," no. Critis, 2009.
 - [20] J. Goodall, W. Lutters, and A. Komlodi, "I know my network: collaboration and expertise in intrusion detection," in *Proceedings of the 2004 ACM conference on Computer supported cooperative work*, 2004, pp. 342–345.
 - [21] Palantir Inc., "PALANTIR CYBER: An End-to-End Cyber Intelligence Platform for Analysis & Knowledge Management," 2013. [Online]. Available: <https://www.palantir.com/wp-assets/wp-content/uploads/2013/11/Palantir-Solution-Overview-Cyber-long.pdf>. [Accessed: 15-Jan-2016].
 - [22] S. Kowtha, L. Nolan, and R. Daley, "Cyber security operations center characterization model and analysis," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, 2012, pp. 470–475.
 - [23] M. E. Locasto, J. J. Parekh, A. D. Keromytis, and S. J. Stolfo, "Towards collaborative security and p2p intrusion detection," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, 2005, no. June, pp. 15–17.
 - [24] E. Kandogan, E. Haber, R. Barrett, A. Cypher, P. Maglio, and H. Zhao, "A1: end-user programming for web-based system administration," *Proc. 18th ...*, 2005.
 - [25] D. Goodin, "How Adobe's messy password breach can spill to sites like Diapers.com," *Ars Technica*, 2013. [Online]. Available: <http://arstechnica.com/security/2013/11/how-adobes-messy-password-breach-can-spill-to-sites-like-diapers-com>. [Accessed: 15-Jan-2016].
 - [26] Norse Corp, "Norse Dark Intelligence," 2014. [Online]. Available: <http://map.ipviking.com/>. [Accessed: 15-Jan-2016].
 - [27] CERTStation Inc., "CERTStation," 2014. [Online]. Available: <http://www.certstation.com/>. [Accessed: 20-Feb-2016].
 - [28] Deutsche Telekom AG, "Sicherheitstacho.eu," 2014. [Online]. Available: <http://www.sicherheitstacho.eu/?lang=en>. [Accessed: 15-Jan-2016].
 - [29] PRNewswire, "A New Weapon in the Fight Against Cyber Criminals," 2015. [Online]. Available: <http://www.prnewswire.co.uk/news-releases/a-new-weapon-in-the-fight-against-cyber-criminals-561384671.html>. [Accessed: 11-Jan-2016].
 - [30] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," *Inf. Syst. J.*, vol. 11, no. 2, pp. 127–153, Apr. 2001.
 - [31] K. Beznosov and O. Beznosova, "On the imbalance of the security problem space and its expected consequences," *Inf. Manag. Comput. Secur.*, vol. 15, no. 5, pp. 420–431, 2007.
 - [32] D. Jonker, S. Langevin, P. Schretlen, and C. Canfield, "Agile visual analytics for banking cyber 'big data,'" *2012 IEEE Conf. Vis. Anal. Sci. Technol.*, pp. 299–300, Oct. 2012.
 - [33] W. Streilein, J. Truelove, C. R. Meiners, and G. Eakman, "Cyber Situational Awareness through Operational Streaming Analysis," in *Military communications conference, 2011*, 2011, vol. 298, no. 0704, pp. 1152–1157.
 - [34] M. Albanese, S. Jajodia, A. Pugliese, and V. S. Subrahmanian, "Scalable Detection of Cyber Attacks," *Comput. Inf. Syst. Technol.*, pp. 9–18, 2011.
 - [35] A. Stotz and M. Sudit, "INformation fusion engine for real-time decision-making (INFERD): A perceptual system for cyber attack tracking," *2007 10th Int. Conf. Inf. Fusion*, pp. 1–8, Jul. 2007.
 - [36] J. M. Beaver, C. A. Steed, R. M. Patton, X. Cui, and M. Schultz, "Visualization techniques for computer network defense," *SPIE Defense, Secur. Sens.*, pp. 801906–801906, 2011.
 - [37] F. C. B. Williams, W. J. Faithfull, and J. C. Roberts, "SitaVis - Interactive Situation Awareness Visualization of large datasets," vol. 5, pp. 273–274, 2012.
 - [38] S. O'Hare, S. Noel, and K. Prole, "A graph-theoretic visualization approach to network risk analysis," *Vis. Comput. Secur.*, pp. 60–67, 2008.
 - [39] J. Barthélemy, R. Bisdorff, and G. Coppin, "Human centered processes and decision support systems," *Eur. J. Oper. Res.*, vol. 136, no. 2, pp. 233–252, 2002.
 - [40] S. Gasson, "Human-Centered vs. User-Centered Approaches to Information System Design," *J. Inf. Technol. Theory Appl.*, vol. 5, no. 2, pp. 29–46, 2003.
 - [41] T. Winograd and D. D. Woods, "The challenge of human-centered design," *Human-Centered Syst. Information, Interactivity, Intell.*, pp. 17–19, 1997.
 - [42] D. A. Norman, *The Design of Everyday Things*, vol. 16, no. 4. Basic books, 2002.
 - [43] S. Parkin, a van Moorsel, P. Inglesant, and M. Sasse, "A stealth approach to usable security: helping IT security managers to identify workable security solutions," *Methodology*, pp. 33–49, 2010.
 - [44] B. Payne and W. Edwards, "A Brief Introduction to Usable Security," *Internet Comput. IEEE*, 2008.
 - [45] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT Technol. J.*, 2001.
 - [46] S. Mahoney, E. Roth, K. Steinke, J. Pfautz, C. Wu, and M. Farry, "A Cognitive Task Analysis for Cyber Situational Awareness," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 54, no. 4, pp. 279–283, Sep. 2010.
 - [47] A. D'Amico and K. Whitley, "The real work of computer network defense analysts," *VizSEC 2007*, pp. 19–37, 2008.
 - [48] A. Doupe, M. Egele, and B. Caillat, "Hit'em where it hurts: a live security exercise on cyber situational awareness," *Proc. 27th Annu. Comput. Secur. Appl. Conf.*, pp. 51–61. ACM., 2011.
 - [49] P. Slovic, "Perception of risk," *Science (80-)*, 1987.
 - [50] J. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Trustworthy and effective communication of cybersecurity risks: A review," in *Socio-Technical Aspects in Security and Trust (STAST)*, 2011, pp. 60–68.
 - [51] P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, and K. Beznosov, "Heuristics for evaluating IT security management tools," *Proc. Seventh Symp. Usable Priv. Secur. - SOUPS '11*, p. 1, 2011.
 - [52] S. Chiasson, P. van Oorschot, and R. Biddle, "Even experts deserve usable security: Design guidelines for security management systems," *SOUPS Work. Usable IT Secur. Manag.*, no. July, pp. 7–10, 2007.
 - [53] J. Rasmussen, K. Ehrlich, S. Ross, S. Kirk, D. Gruen, and J. Patterson, "Nimble cybersecurity incident management through visualization and defensible recommendations," *Proc. Seventh Int. Symp. Vis. Cyber Secur. - VizSec '10*, pp. 102–113, 2010.
 - [54] G. Button and P. Dourish, "Technomethodology: paradoxes and possibilities," *Proc. SIGCHI Conf. Hum. factors Comput. Syst.*, pp. 19–26, 1996.
 - [55] P. Dourish, "Implications for design," *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. - CHI '06*, p. 541, 2006.
 - [56] J. Grudin, "The computer reaches out: The historical continuity of interface design," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 1990, pp. 261–268.
 - [57] E. Haber and E. Kandogan, "Security administrators: A breed apart," *SOUPS USM*, pp. 3–6, 2007.
 - [58] E. Haber and E. Kandogan, "Security Administration in the Wild: Ethnographic Studies of Security Administrators," pp. 1–3, 2007.
 - [59] E. Haber and J. Bailey, "Design guidelines for system administration tools developed through ethnographic field studies," in *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, 2007, p. 1.
 - [60] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Towards understanding IT security professionals and

- their tools,” in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007, pp. 100–111.
- [61] R. Werlinger, K. Hawkey, D. Botta, and K. Beznosov, “Security practitioners in context: Their activities and interactions with other stakeholders within organizations,” *Int. J. Hum. Comput. Stud.*, vol. 67, no. 7, pp. 584–606, 2009.
 - [62] R. Barrett, E. Kandogan, P. P. Maglio, E. M. Haber, L. A. Takayama, and M. Prabaker, “Field studies of computer system administrators: analysis of system management tools and practices,” *Proc. 2004 ACM Conf. Comput. Support. Coop. Work*, pp. 388–395, 2004.
 - [63] R. Werlinger, D. Botta, and K. Beznosov, “Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis,” in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007, pp. 149–150.
 - [64] E. Haber, E. Kandogan, and P. Maglio, “Collaboration in system administration,” *Commun. ACM*, 2011.
 - [65] E. Kandogan, P. P. Maglio, E. Haber, and J. Bailey, “On the roles of policies in computer systems management,” *J. Hum. Comput. Stud.*, vol. 69, no. 6, pp. 351–361, 2011.
 - [66] H. Tahir and P. Brézillon, “Shared Context for Improving Collaboration in Database Administration,” *Int. J. Database Manag. Syst.*, vol. 5, no. 2, pp. 13–28, 2013.
 - [67] E. Kandogan, P. P. Maglio, E. M. Haber, and J. Bailey, “Communities and Trust,” in *Taming Information Technology: Lessons from Studies of System Administrators*, Oxford: Oxford University Press, 2012.
 - [68] K. Hawkey, D. Botta, and R. Werlinger, “Human, organizational, and technological factors of IT security,” *CHI’08 Ext. Abstr. Hum. Factors Comput. Syst.*, pp. 3639–3644, 2008.
 - [69] E. Kandogan and E. Haber, “Security administration tools and practices,” *Secur. usability Des. Secur. Syst. that people can use*, pp. 374–394, 2005.
 - [70] D. Siegel, B. Reid, and S. Dray, “IT security: protecting organizations in spite of themselves,” *interactions*, pp. 20–27, 2006.
 - [71] R. Werlinger, K. Hawkey, and K. Beznosov, “An integrated view of human, organizational, and technological challenges of IT security management,” *Inf. Manag. Comput. Secur.*, vol. 17, no. 1, pp. 4–19, 2009.
 - [72] W. Yurcik, R. Thompson, and E. Rantanen, “Those Who Shield Others Are Users Too! Experience from User Studies of Security SysAdmins,” *CHI Work. Secur. User Stud.*, no. May, pp. 1–4, 2007.
 - [73] E. Casey, “Case study: Network intrusion investigation – lessons in forensic preparation,” *Digit. Investig.*, vol. 2, no. 4, pp. 254–260, Dec. 2005.
 - [74] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, “Preparation, detection, and analysis: the diagnostic work of IT security incident response,” ... *Comput. Secur.*, 2010.
 - [75] J. Greenbaum, “In Search of Cooperation An Historical Analysis of Work Organization and Management Strategies,” *Proc. 1988 ACM Conf. ...*, pp. 102–114, 1988.
 - [76] D. Botta, K. Muldner, K. Hawkey, and K. Beznosov, “Toward understanding distributed cognition in IT security management: the role of cues and norms,” *Cogn. Technol. Work*, vol. 13, no. 2, pp. 121–134, Sep. 2010.
 - [77] E. Hutchins, *Cognition in the Wild*. Cambridge, MA: MIT Press, 1995.
 - [78] M. Tyworth, N. A. Giacobe, V. Mancuso, and E. The Society of Photo-Optical Instrumentation, “Cyber situation awareness as distributed socio-cognitive work,” *Cyber Sens. 2012*, vol. 8408, no. Level 2, p. 84080F–84080F–9, May 2012.
 - [79] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006.
 - [80] C. Heath, M. Jirotko, P. Luff, and J. Hindmarsh, “Unpacking collaboration: the interactional organisation of trading in a city dealing room,” *Comput. Support. Coop. Work*, vol. 3, no. 2, pp. 147–165, 1994.
 - [81] C. Heath and P. Luff, “Documents and professional practice: ‘bad’ organisational reasons for ‘good’ clinical records,” *Comput. Support. Coop. Work*, pp. 354–363, 1996.
 - [82] M. Hammersley and P. Atkinson, *Ethnography: Principles in Practice*. London, UK: Routledge, 1995.