The Security Awareness Paradox: A Case Study

Muhammad Adnan Tariq*, Joel Brynielsson*†, Henrik Artman*†
*KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
†FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden
Email: {tari, joel, artman}@kth.se

***Abstract*—Knowledge-intensive organizations are characterized by their dependency on highly skilled personnel who perform their daily work in a decentralized manner. In these organizations it is the users who make the important decisions, and therefore the organization's information security awareness is upheld by and depends on its users' combined security awareness. To assess the overall organizational security awareness it therefore becomes interesting to assess both the users' individual level of security awareness, as well as their level of consistency and conformity with regard to other users' awareness.**

In the present case study, 15 semi-structured interviews have been undertaken within a large telecommunication company in order to understand how significant IT security aspects are understood within the organization. The study highlights a number of perception differences where the technical IT staff and the ordinary users do not share the same understanding. It is suggested that these perception differences result from a paradoxical situation where the users' possibility to uphold security awareness is hindered because of security concerns.

***Index Terms*—User awareness; IT security; paradoxical reasoning.**

I. Introduction

In today's decentralized organizations, users need to make well-informed key decisions on a daily basis. From an IT security perspective, the possibility to make such well-informed decisions depends on a user's security awareness with regard to important security objectives. From an organizational point of view, these security objectives are expressed in terms of policies, procedures, etc., stating the expectations that the organization has with regard to user behavior. However, this does not necessarily mean that the stated policies and procedures are sufficient in order for the users to reach a satisfactory level of security awareness [1], [2].

In collaborative environments such as organizations, user awareness can partly be perceived as the understanding of other users' activities in order to put one's own activities into context. To obtain user awareness in this collaborative regard, a certain amount of information sharing is required [3]. From a security point of view, however, it can be argued that certain information sharing should not be undertaken due to the need-to-know principle, which might hinder the collaborative work to some extent. Moreover, a user's security awareness is dependent on the overall user awareness which, hence, means that such non-sharing of information might also give users a false sense of security [4].

The predominant view of users being incapable of handling security related decisions adds a further complication with regard to a user's possibility to achieve sufficient security awareness. Often, this view of the user as being the "weakest link" results in the actual users being left out of the security loop. From a critical point of view, this implies that the whole user dimension of the problem is thereby neglected [5], [6], [7].

This paper presents a case study carried out in a large telecommunication organization. The study was undertaken for the purpose of understanding the organization's internal security awareness. In particular, the study has served to understand perceptions and attitudes with regard to the users within the organization, and how this understanding has influenced the policies and best practices that are in place. As a result, the study sheds light on the differences between the user and organizational perspectives of security.

The paper is structured in seven sections where Section II provides an overview of related work within the area of human behavior and security, and Section III presents the methodology which was followed in order to collect the empirical data. Section IV then presents different perspectives of the respondents in terms of users, security problem solving methodology, and attackers, and Section V relates and analyzes the different perspectives. Finally, Section VI discusses the findings before the paper is concluded in Section VII.

II. Background

Within IT security, the user of a system is often referred to as the weakest link, which underlines that the user plays a critical role for achieving better security. This is particularly true when the user is part of a larger organizational structure involving a variety of users where the overall organizational security is at stake [8]. Also, since it is the user who will be deploying and using the technical solutions and preventive measures that are in place, a system cannot be protected through considering technical solutions in isolation [9], [10], [11], [12]. For addressing user-related security issues, user awareness has been observed to be a key factor [2], [13], [14], [15]. Lack of user awareness may result in situations where users are unable to understand the implications of their actions from a security perspective, become unaware of the security objectives (policies) of their organization, etc. This, in turn, results in that users will need to develop their own mental models of their own organization's approach to security—models which in most cases will not be fully accurate.

A number of previous studies have found and exemplified aspects related to lack of user awareness from a security point of view. In one such study concerning user perception

ASONAM 2014, August 17-20, 2014, Beijing, China
978-1-4799-5877-1/14/$31.00 ©2014 IEEE

of security issues it is argued that the participants' security knowledge was outdated and/or that they were misinformed, and that they considered security to be an entirely technical problem that the technical staff should take care of [16]. In another study it turned out that users who were, from an IT perspective, performing relatively simple tasks also had a very basic understanding of security in general and, moreover, were not aware of security policies related to the tasks they performed [17]. Hence, a possible conclusion is that the nature of one's work duties in terms of the general IT environment is correlated with user awareness: a more complex IT environment requires the users to become more aware of security issues. It was also shown that the expected security behavior according to the policies and guidelines had limited impact on the participants' actual behaviors since they simply did not know about the related documents. A contributing factor turned out to be that the participants lacked the motivation to read the documents which, in turn, was due to lack of IT security knowledge. Further, information campaigns for making the policy documents visible through, e.g., leaflets, booklets, etc., had a limited effect on the user behavior. Instead it is argued that for actually changing the user behavior it will be required to make the users aware of the actual risks that they are creating which, in turn, will make it possible for the users to see and judge themselves regarding the threat [18].

From a usability perspective, security procedures/policies that are perceived as too complicated risk to be ignored regardless of the users' security awareness. As a typical example, rules for selecting secure passwords might be communicated to and understood by the users, but if these rules are too complicated and will be ignored then the rules' effectiveness can be questioned. For example, one might be required to change the password very often and/or the password cannot be chosen so that it is possible to easily remember it. This is a typical example of a general case where theoretical IT security barriers are put aside by users not willing to follow the policies. Hence, there is a tradeoff between user acceptance and the dictated level of security, and sometimes lowering the level of theoretical security might be a better choice: it has been shown that in conditions where the security level was low and the users were able to foresee the potential threats, their behavior towards security-critical information was exemplary [5], [19].

From a threat perception perspective, users generally tend to believe that the risk of being attacked is less likely compared to other users which is an example of an optimistic bias, i.e., people generally tend to assign higher probability to positive outcomes than to negative outcomes [20], [21]. In a recent survey it is reported that information security managers tended to be optimistically biased such that they on the one hand understood the likeliness of the occurrence of a negative event but on the other hand believed that they were less prone to be targeted [22]. It shall be noted that this threat perception is related to the motivation of adopting measures to counter a threat, i.e., people tend to alter their behavior based on the amount of risk that they perceive. The factors affecting such alteration in behavior result from understanding the impact of the threat if it materializes, so if a user believes that he/she is under a higher threat, he/she will alter his/her behavior in order to counter the consequences. However, the opposite also applies, i.e., when the user believes that he/she is not at risk, he/she will also become less cautious [9]. Moreover, it has been argued that users tend to take more risks if they know that they have security related products installed on their machines [23]. This indicates that users who are not kept in the loop might have a false sense of security which thereby complicates the user awareness issue further. In the present paper we report on similar user behavior and describe how the belief in a technical security solution results in a paradoxical situation where the lack of user awareness is compensated through incorporating more technical security measures which, in turn, further degrades the user awareness.

III. Methodology

Fifteen interviews were conducted at a large organization which provides ICT services and is one of the largest service providers in the country. The respondents represent the management of the own organization's computer systems, and the interview study was designed in order to understand the respondents' attitudes and perceptions regarding their organization's own security awareness. In particular, the interview study has served to investigate the IT security specialists' understanding of the user awareness, and how this understanding influences the policies and methods that they implement.

A. Data collection

The interviews were conducted in a semi-structured manner [24] using a set of predefined questions which were thematically separated. Each interview session started with a background theme focusing on the educational and professional background of the respondent, along with his/her duties and role in the organization. The next theme focused on the assets that the respondent is responsible for and has access to. Next, a number of questions related to security problem solving was introduced in order to understand the respondent's perspective on IT security. This theme focused on the practices and policies that are related to protecting the respective assets. The final theme focused on the respondent's understanding of the perpetrator.

B. Respondents

In total, fifteen respondents were interviewed. Their periods of employment differed, but all the respondents were experienced and had been working for several years within their respective fields. Organizationally, one of the respondents was a senior manager, four were at the manager level, and the rest were assistant managers within their respective teams. Regarding work duties, seven of the respondents were system administrators providing services such as e-mail, broadband, UNIX based system management, etc. Three of the respondents had a background in IT security and were responsible for managing the security of the organization in terms of both policies and

TABLE I
THE TABLE ENLISTS THE RESPONDENTS WITH REGARD TO ORGANIZATIONAL CONTEXT, EDUCATIONAL BACKGROUND, AND WORK DUTIES.

Nr	Role	Department	Background	Work duties
01	Assitant manager	IT infrastructure and operations	Computer science	Corporate e-mail management
02	Assitant manager	IT infrastructure and operations	Computer science	Corporate e-mail management
03	Assitant manager	IT infrastructure and operations	Computer science	Unix system administration and data storage
04	Manager	IT data center	Computer science	Managing data center network
05	Assitant manager	IT infrastructure and operations	IT security	Managing IT security issues
06	Manager	IT infrastructure and operations	Computer science	Managing IT security issues and the internal network
07	Senior manager	Enterprise resource planning	Computer science	Development and managment of billing and sales systems
08	Assitant manager	Enterprise resource planning	Computer science	Managing material management system
09	Manager	IT data center	Computer science	Managing corporate network
10	Assitant manager	IT data center	Computer science	Managing internal network
11	Assitant manager	IT data center	IT security	Managing firewalls
12	Assitant manager	Core operations	Electrical engineering	Managing telephone connections
13	Manager	Multimedia and broadband	Computer science	Managing DNS, SMTP, and web servers
14	Assitant manager	Multimedia and broadband	IT security	Managing IT security issues
15	Assitant manager	Multimedia and broadband	Electrical engineering	Managing and testing broadband services

technical solutions. The remaining five respondents came from more service-oriented departments related to customer support, generation of management reports, etc. The respondents' backgrounds, work duties, and hierarchical placement in the organization are further summarized in Table I.

C. Interview context

The interviews were conducted face-to-face in a meeting hall that was part of the IT security department premises. Before the start of the interview the anonymity of the respondent was ensured and the respondent was asked whether he/she would allow the interview to be recorded on a dictaphone. Nine out of 15 agreed while the others requested not to record the interview. The respondents were then informed about the purpose of the study and that they had the options to skip questions and/or end the interview at any time. At the end of each interview session the respondent was encouraged to ask any type of question to the interviewer.

IV. RESULTS

This section elaborates on how the respondents perceived IT security in the context of their organization. During the interviews, respondents were asked about different types of attacks which might either have emerged from the internal network of the organization, or have been launched from the internet. Moreover, the respondents were inquired about their understanding of the attacker, their perception of the users in the organization, and the practices that the respondent adopts in order to keep the systems secure. Further, the respondents' understanding of IT security has been divided into three major parts according to the following:

- user perception,
- technical security,
- attacker perception.

Each of these aspects are important to consider in order to understand how the security is maintained and sustained within the organization.

A. User perception

This section presents and discusses how users were perceived by the respondents. Regarding user awareness, ten of the 15 respondents mentioned that users/employees within the organization are generally not familiar with issues related to IT security. Respondent 06 presents his/her understanding of this view by stating that:

> Users are unaware as they are the normal users. They don't know if their AV [antivirus] is updated or their systems are properly patched. Moreover, users who receive an email [spam] containing a link or an attachment will unintentionally execute the malicious content. [R-06]

Moreover, the same respondent presented a case where a user had a wireless cracking tool installed on his/her official system. When the respondent asked the employee regarding this act being deliberate or not, it became evident that the employee was not aware of this cracking tool existing on his/her system. Based on such user observations, the respondent concluded that "most of the users have no awareness, since unintentionally there might be something [malicious] running on their systems." Although the above presented cases are just a few examples, the respondent was adamant in his/her belief regarding the users being unaware.

In line with the above presented understanding of the users being unaware of malicious content existing in their systems, respondent 04 presented a similar perception of the user. Referring to the general users within the organization, the respondent stated that "they [the users] have no idea what is going on." Respondent 04 also mentioned that his/her system might had been compromised, but that his/her practices and knowledge prevented further damage: "I don't know. Maybe my laptop is compromised but we are in the IT department so we update our own systems." For the case of general users within the organization, however, the respondent argued that "a layman who wants to plug in a system on the network to perform routine work has no idea regarding possible spyware or bots that might exist on the system." The respondent further reasons that since the users are not able to detect malicious content such as spyware, etc., the users do not know much about security related issues. In the following quotation, respondent 05 presents the users in the organization by stating:

> The users are not aware of IT security issues, they take it [IT security] very lightly, and the human element of curiosity can easily be exploited [by attackers]. [R-05]

Thus, the respondent links unawareness and curiosity of the user with the attacker aspect, where the attacker can make use of the curiosity to exploit unaware users. The respondent also elaborated on a botnet development activity taking place in the organization, and argued that users tend to download malicious content from the internet which results in incidents such as the described botnet development.

To summarize, the respondents presented multiple user related security issues. As an example, respondents 09, 10, 11, 13, and 14 also argued along the same lines as described above regarding the users potentially downloading malicious content unknowingly. Respondents 01 and 07 presented their view on the users' having a tendency to not changing their passwords unless explicitly required to do so, which further points towards the possibility that users are not aware in terms of securing and/or selecting strong passwords. As a further example, respondents 03 and 08 argued that users are typically interested in the functional aspect only, and are not aware of system level issues. Hence, the presented data shows that most respondents had the perception that the users are not aware of security issues. To tackle this lack of user awareness one could argue that sharing information to the users or educating the users in terms of security could be a fruitful way to improve the organizational security, but this is not done.

B. Technical security

This section focuses on presenting the respondents' understanding of security related issues in terms of how they solve security related problems. Eleven of the 15 respondents pointed towards technical solutions for tackling problems related to security.

Respondent 02, when inquired about external attacks (i.e., attacks originating from the internet), argued that his/her systems are well protected from external attacks by stating that:

> Yes, these [external attacks] cannot reach us because we have Microsoft firewalls, antiviruses, etc., blocking them. [R-02]

Thus, we can conclude that the respondent trusts the technical tools for protecting his/her system, and does not anticipate that an attacker might bypass such measures. Similarly, while discussing system protection, respondent 13 argued that his/her focus is solely directed towards application security, which he/she achieves through patching the application using the patches that are provided by the vendor. However, earlier in the interview the same respondent pointed towards the user awareness aspect and argued that people/customers tend to unknowingly download malicious files from the internet, i.e., files which are potentially self-replicating and will not be stopped by the firewall. Furthermore, the respondent related this unawareness aspect with a DDoS attack which has been faced by the organization. Hence, it follows that the respondent does not seem to incorporate such user related issues whilst describing the practices that he/she adopts for keeping the systems secure. Respondent 07, on the other hand, highlights the use of vulnerability scanners for identifying security related problems by stating that:

> Now the CRM [customer relationship management] and ERP [enterprise resource planning] systems are scanned with QualysGuard. It points out vulnerabilities and puts these on level 1, 2, or 3. The vulnerabilities having the highest level are mitigated/removed by us. [R-07]

Here the emphasis is again put on the technical aspect of security where the respondent does not incorporate the user aspect in terms of protecting assets but rather focus on technical tools (which in this case is the vulnerability scanner).

In summary, the respondents presented a predominantly technology-centered view on security through mentioning a number of technical measures and practices. In terms of practices concerning protection of critical information, respondents 08, 10, and 12 referred to passwords as critical information. In terms of protecting the organizational infrastructure, i.e., servers, etc., respondent 04 proposed to disconnect critical systems from the internet. Respondent 05, on the other hand, presented a scenario where technical tools for detecting malware propagating within the internal network of the organization were preferred. The cause of this malware propagation, however, was associated with the users in the organization. Respondent 01 referred to system patching whilst respondent 03 referred to port blocking and limiting access to root accounts. Respondent 11 explained that the adopted organizational security is based on a multi-layered security infrastructure, and that if an attacker repeatedly attacks the organizational firewall the IP will be blacklisted.

C. Attacker perception

This section discusses the respondents' thoughts and perceptions regarding potential attackers. During the interviews, the respondents distinguished between three different kinds of attacker motives which will be used below for categorizing the respondent perceptions into three categories of (perceived) attackers: 1) for fun, 2) advanced attackers, and 3) usual suspects.

Seven of the 15 respondents brought up the *for fun* motive as being the most frequently occuring attacker motive, and discussed motives where an attacker performs his/her attack in order to gain insight, learn about procedures, or for pure amusement.

Respondent 04 believed that attackers are primarily of two types—the advanced attackers and the script kiddies—and presented script kiddie attackers as novice attackers who are trying different attacks without havig any real knowledge of attacking, and also stated that this is the most common attacker type:

> 80 percent of the attackers are script kiddies. They run scripts and do not know what they are doing. [R-04]

As a further example, respondent 13 presented his/her belief regarding attacker motive from the perspective of a security event taking place in the organization:

> Well, I think this [referring to an event] is done for the sake of fun and thrill. [R-13]

Similarly, when respondent 14 was inquired about the motives of attacks that had taken place in the organization, he/she stated the following:

> There can be many reasons, but I think most of this [referring to attacks] is carried out for the sake of learning and fun. [R-14]

None of the respondents provided any details regarding why they think that attackers are motivated by reasons related to having fun, learning, etc. As it seems, a major reason for this was that the respondents did not know of other types of attackers, and therefore presented a stereotypical understanding based on assumptions. However, respondent 14 knew about other types of attackers as well, but he/she instead referred to lack of monitoring tools for making it possible to investigate details regarding possible attacker motives.

In other cases, the respondents had an additional perception of the attacker as sometimes being very advanced. Three respondents presented such understandings of *advanced attackers*. Respondent 11, for example, described his/her view of advanced attackers as follows when he/she was asked to present his/her understanding of attackers in general:

> Highly skilled attackers are very smart, they know whom they want to target, and they can use social engineering skills to acquire the required information. [R-11]

In the following quotation, respondent 09 elaborates on advanced attackers in terms of skilled entities backed up by the government for the purpose of targeting sites/organizations of strategic interest, and based on this understanding the respondent rejects the idea that these attackers might be interested in attacking his/her own organization:

> The more skilled hackers will not spend time on obtaining information from individuals. If I was to become a very good/proven hacker, I would try to attack an enemy state, the government, or similar strategic places in order to acquire information. I would not gain anything from attacking some company. It would be a total waste to spend energy on such a target. [R-09]

From the above quotation it becomes clear that the respondent sees a direct relationship between skill and motivation which, in turn, leads to a superficial view of advanced attackers as people who no longer cares about basic motives related to individual needs. To summarize, the respondents' understanding of attackers seems to be stereotypical since attackers are either thought of as persons who are attacking for the fun of it or as persons possessing advanced skills that are used for achieving some higher order goal, but the respondents do not combine these two perspectives in order to form a more well-reasoned view of the attacker.

The respondents' understanding of attackers further points towards the so-called *usual suspects* which in most cases refer to foreign countries trying to attack the organization in order to achieve some hidden objective. Six of the 15 respondents point towards such attackers. The following quotations present how two respondents point towards foreign countries whilst discussing about security related events:

> There is lots of scanning of our systems coming from foreign countries such as China, India, and Israel. [R-14]
>
> Secret agencies from foreign countries will be interested in attacking the organization. [R-07]

As can be noted, the respondents tend to identify foreign countries, but they do not elaborate on why these countries are attacking the organization.

A similar case arose when respondent 04 was asked to elaborate on the internal attacks that the organization had faced:

> No, I am talking about external attacks coming from India, China, etc., targeting devices that are directly accessible on the internet. [R-04]

However, when the respondent was asked to elaborate further on these attacks (i.e., attacks originating from foreign countries), the respondent answered that they do not investigate such attacks but rather focus on ensuring that the systems are secure regardless of the type of attacker.

In general, respondents who were specifically asked to elaborate on attacks involving the usual suspect either pointed towards another department or referred to lack of investigation. Respondent 06 further argued that the organizational structure acts as a hindrance with regard to investigating such events. Hence, it can be concluded that the respondents' perception of the usual suspect is often not based on factual information, and thereby risk to be stereotypical.

V. Consequences

This section discusses how the respondents' perceptions, as laid out in Section IV, are upheld whilst dealing with daily security related work duties.

A. User perception and information sharing

The influence that the respondents' perception of the users has on the information sharing within the organization will be elaborated on further within this section.

When asked to present recent security events, respondent 08 stated the following:

> No, so far there hasn't been any intimation of an attack or incident. From 2008 and onwards there hasn't been anything. [R-08]

Similarly, when respondent 12 was asked about recent security incidents that had affected the organization, he/she denied that such events had been reported. The same respondent, however, presented security events that had taken place in the past, which further strengthens that the respondent indeed did not know of any recent security related events. Hence, since recent attacks have indeed affected the organization, this indicates that these respondents have a false sense of security due to lack of information sharing. This view is further strengthened by, e.g., respondent 04 who stated the following when he/she was inquired about sharing information related to practices for avoiding malicious content:

> We do not communicate it [the practices] to them [the users], but we have developed a procedure so that internal systems can be controlled and monitored. We try to make sure that the end user has to take as few decisions as possible because they do not know [about malicious content]. [R-04]

The respondent, hence, argues that no information is or should be shared with the users. As discussed in Section IV-A, respondent 04 also has the opinion that users are generally not aware of malicious activities related to spyware, botnets, etc., taking place. To conclude, it follows that the respondent suggests the use of technical means for enforcing policies on the users in order to tackle the perceived inability of the users to understand security related issues. From another viewpoint, however, it could be argued that the enforcement of such policies brings about that users become even more unaware of the consequences of their actions and, thus, will continue with their existing behavior which, in turn, results in that, e.g., more malicious content is downloaded.

Considering another example regarding the organization's password policy, respondent 07 stated that users are often not willing to change their passwords on their own:

> To be frank, if you ask me to change my password every two months, I would simply not be doing it. No end-user in the world would do it. [R-07]

The respondent presented a solution to this problem by stating that "we have applied policies on the system," and also stated that "as such, these [policies about password change, etc.] are not communicated." Thus, it can be argued that if no information is shared with the users regarding the underlying reasons for a password policy, then one cannot expect users to comply with the policy. The implementation of policies on the system level further points towards the users being perceived as incapable of understanding the security requirements and therefore technology centered solutions are preferred in order to enforce policies on the user. This aspect will be further discussed below where the perception of the user is related with technical problem solving.

B. User perception and technical security

This section presents how the respondents address security problems in order to deal with unaware users.

In response to a question concerning critical security events, respondent 10 argued that the organization previously lacked a central policy for implementing antivirus software, firewalls, and system patches, but since the implementation of these policies there has not been any events. Hence, the approach presented by the respondent focuses on using technical means for securing systems. Regarding the user aspect, the respondent argued that internal attacks are normally the result of viruses and malware ending up in the internal network as a result of the users' tendency to plug in infected USB drives.

Further, respondent 01 stated that "the users are not used to these [email] systems and they forget to change passwords. They argue that they will not be able to remember passwords and therefore they do not change it." In the following quotation, the respondent presents how polices are implemented and enforced to make users comply with organizational security expectations:

> Now we are forcing them to change their passwords. [R-01]

Hence, it becomes evident that policies are enforced on the users, and that this is due to the perception of users as being unable to comply with the security policy. From a user perspective, such policy enforcement may result in the users being unmotivated to learning about the underlying aspects of security and to keeping their computers secure.

During the interviews, it has become evident that the adopted technology-centered perspective is considered to be an accepted alternative to user awareness. This impression is strengthened by the description of a security event where a botnet was discovered within the organization. When respondent 05, working in the security department, was asked about the investigation of the event, he/she stated that "as you know, end-users are not tech-savvy and the only option was to apply controls on the system level, but the AV [antivirus] could not detect it [the botnet] so they [the users] could not know what was going on." Moreover, while discussing about the general user behavior the respondent referred to the botnet event and stated that "because when we look at the botnet, what happened was that spam emails were sent with a link and they [the users] clicked on it." Here, again, users are criticized for executing malicious files. However, the adopted practice for tackling the problem rely strongly on technical means. Such technical solutions are indeed required for tackling these kinds of events, but to avoid these attacks in the future it is necessary to also address the user behavior so that users become more aware of the risks associated with malicious content.

Considering the above presented practices, it seems that the organization is focused on detecting the security problems and then solving these problems through using technical solutions. The problem, however, originates from the users who download malicious content which tends to spread throughout the organization's internal network, and by making users aware their behavior and attitudes can be affected which would potentially result in a reduced impact of such attacks.

C. Attacker perception and lack of investigation

As already discussed in, e.g., Section IV-C the respondents' generally seem to have a stereotypical understanding of attackers. This stereotypical understanding can be further related with the observed tendency to not investigate and learn from security events. Respondent 09 explains why he/she would not investigate such events by suggesting that "we haven't tried to investigate because there has never been too much destruction." Hence, the respondent suggests that the observed attacks were not investigated since they did not result in severe consequences. However, the respondent did point towards the usefulness of investigating events by stating that "attackers differ regarding their use of IPs, and they also use different techniques for attacking. But we never went into detail in terms of their motives, whether their IP addresses are authentic, and so forth. I can't say anything regarding these things." As elaborated on in Section IV-C, respondent 09 seems to have a somewhat superficial view of advanced/skilled attackers. This may be the result of lacking factual information regarding the attackers as a further result of the here presented tendency to not investigate attacks.

In another case where respondent 13 was encouraged to elaborate on details regarding observed security incidents, the respondent argued that "there are cases where we have received lots of attacks on our servers originating from external countries such as China and India." Upon inquiring about the types of attacks, the respondent said that "normally these attacks involve port scans, and the attacks that originate from other countries seem to be more organized." When the respondent was asked to further elaborate on these attacks, the respondent stated that "we don't know the details. The network team that manages the organization's network can provide this information." This lack of information concerning the security incidents might be due to lack of information sharing between departments or the event never being properly investigated. As mentioned earlier, respondents 04 and 09 who manage the organization's internal network stated that they do not investigate events, which makes it likely that the event was never investigated.

As a further example of the tendency to not investigate attacks, respondent 11, who manages the firewalls in the organization, stated that "I do not care. I just block such traffic by blocking the port, and I do not go into details since I have other activities to take care of." when inquired about details of an attack faced by him/her. This statement thus exemplifies even further that event investigation is not given much priority within the organization. Similarly, respondent 14 explicitly stated that the organization is often targeted from foreign countries, but when asked about the details regarding the attacks the respondent refers to a lack of monitoring tools.

Security event investigation has the potential to provide useful information in terms of how the attack was carried out and who might be the potential perpetrator behind the attack. This information can then be used to obtain a more informed understanding of the attacker. However, one can argue that investigating events might require substantial resources, which need to be contrasted to the added value that a thorough understanding of the relevant attackers might be for the organization.

VI. Discussion

Tackling information security issues requires a sociotechnical approach to be able to address the complex dependencies that exist between people, policies, and technology [25]. From a threat assessment perspective, attacks are generally divided into two categories where the attacker is either 1) an external actor trying to gain unauthorized access to critical resources, or 2) an "insider" who already has a certain level of access to and knowledge about the organization. Regarding the latter-mentioned internal threats, the users within the organization are also often considered as security threats, although users do not, by definition, have a malicious intent per se but rather commit unintentional mistakes/errors that can possibly be exploited by a third party [26], [27]. As shown in Section IV and further elaborated on in Section V, however, this last type of threat also gives rise to side effects within the organization, which risk to further exacerbate the internal threat. These side effects arise due to the respondents' (see Table I) perception of the user as 1) being unaware of IT security risks at large, and 2) not being able to view their own actions from a security perspective. As a consequence, rather than sharing information in the form of policies and user feedback, the technical staff tries to compensate for the lack of user awareness by means of technological IT security solutions. Hence, the respondents' perception of the user effectively hinders the user's awareness process which results in a catch-22 situation where 1) users need to learn about the consequences of their actions in order to become security-aware, but 2) are unable to learn since they are not trusted from a security point of view. At the same time the technical team's perception of the user will be reinforced since the users will keep on repeating the same kind of mistakes over and over again. In the end, such user mistakes result in the implementation of even more technical security solutions, which further prevents the user from making informed security decisions. Hence, the study indicates that technical means are used to make sure that the user is left out of the security loop meaning that non-involvement of the user is taken to be the accepted solution to IT security problems—which is a criticized way of solving IT security problems [10], [28], [29].

From the perspective of threat perception, the study indicates that the respondents exhibit a stereotypical understanding of the attacker. This stereotypical understanding might result from multiple factors. One such factor could be the result of non-investigation of security events: many respondents point at a certain type of attacker without being able to relate the attack with factual information. As it seems, security incidents are not investigated at depth and therefore the respondents lack factual information to be used as a basis for their understanding of the attacker. The described practice regarding non-investigation of security events may result in a second catch-22 situation where respondents are not able to update their beliefs regarding the attacker. This paper has suggested this paradoxical phenomenon which could originate from a conflict between the respondents' perceptions and the adopted practices. It shall be noted, though, that the paper merely discusses the possible existence of such a phenomenon but does not claim generalization per se. Rather, more studies need to be performed in order to explore these possible paradoxical situations and their potential impacts within different contexts.

VII. Conclusions

This paper has presented a case study carried out within a large telecommunication organization in order to understand the perspectives and perceptions of different stakeholders with regard to IT security. In particular, the study has focused on the technical staff's view on 1) users, 2) security related problem solving, and 3) potential attackers.

The study highlights that the technical staff largely considers the users to be incapable of handling security related tasks and making appropriate security related decisions. As a result, information is shared to users on a need-to-know basis. As a further consequence, technical monitoring and detection solutions are the preferred means to implement security, whilst organizational changes with regard to, e.g., security policies are not prioritized. In the end, the technical staff thereby upheld a paradoxical situation where the user's ability to develop and maintain security awareness is hindered which, in turn, results in a degraded organizational ability to make appropriate security related decisions.

Investigation of security-critical events is a crucial factor for threat perception, but the case study also suggests that observed cyber-attacks—whether successful or not—are seldom investigated at depth. Consequently, several stakeholders within the organization proved to have a superficial understanding of the attacker, where attackers were often perceived as mysterious entities choosing to target the organization's systems for unknown reasons.

Acknowledgments

This work was partly supported through the strategic research center Security Link which is funded by the Swedish Government.

References

[1] M. T. Siponen, "Five dimensions of information security awareness," *Computers and Society*, vol. 31, no. 2, pp. 24–29, Jun. 2001.

[2] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, Sep. 2010.

[3] P. Dourish and V. Bellotti, "Awareness and coordination in shared workspaces," in *Proceedings of the 1992 ACM Conference on Computer-Supported Cooperative Work*, ser. CSCW'92. New York, NY: ACM, 1992, pp. 107–114.

[4] A. Adams and A. Blandford, "Bridging the gap between organizational and user perspectives of security in the clinical domain," *International Journal of Human-Computer Studies*, vol. 63, no. 1–2, pp. 175–202, Jul. 2005.

[5] A. Adams and M. A. Sasse, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[6] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Computers & Security*, vol. 25, no. 1, pp. 27–35, Feb. 2006.

[7] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, May 2009.

[8] S. M. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983–988, Nov. 2012.

[9] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior*, vol. 24, no. 6, pp. 2799–2816, Sep. 2008.

[10] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, Mar. 2009.

[11] M. E. Zurko and R. T. Simon, "User-centered security," in *Proceedings of the 1996 New Security Paradigms Workshop*, ser. NSPW'96. New York, NY: ACM, 1996, pp. 27–33.

[12] M. E. Zurko, "User-centered security: Stepping up to the grand challenge," in *Proceedings of the 21st Annual Computer Security Applications Conference*, ser. ACSAC'05. Washington, DC: IEEE Computer Society, 2005, pp. 187–200.

[13] J. D'Arcy and A. Hovav, "Does one size fit all? Examining the differential effects of IS security countermeasures," *Journal of Business Ethics*, vol. 89, no. 1, pp. 59–71, May 2009.

[14] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*, ser. HICSS'13. Washington, DC: IEEE Computer Society, 2013, pp. 2978–2987.

[15] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "Investigating information security awareness: Research and practice gaps," *Information Security Journal: A Global Perspective*, vol. 17, no. 5–6, pp. 207–227, Sep. 2008.

[16] J. B. Gross and M. B. Rosson, "Looking for trouble: Understanding end-user security management," in *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology*, ser. CHIMIT'07. New York, NY: ACM, 2007.

[17] E. Albrechtsen, "A qualitative study of users' view on information security," *Computers & Security*, vol. 26, no. 4, pp. 276–289, Jun. 2007.

[18] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: an exploratory field study," *Information & Management*, vol. 51, no. 2, pp. 217–224, Mar. 2014.

[19] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium*, ser. SSYM'99. Berkeley, CA: USENIX Association, 1999.

[20] N. D. Weinstein and W. M. Klein, "Unrealistic optimism: Present and future," *Journal of Social and Clinical Psychology*, vol. 15, no. 1, pp. 1–8, Mar. 1996.

[21] V. Hoorens, "Self-favoring biases for positive and negative characteristics: Independent phenomena?" *Journal of Social and Clinical Psychology*, vol. 15, no. 1, pp. 53–67, Mar. 1996.

[22] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, "Unrealistic optimism on information security management," *Computers & Security*, vol. 31, no. 2, pp. 221–232, Mar. 2012.

[23] R. West, "The psychology of security: Why do good users make bad decisions?" *Communications of the ACM*, vol. 51, no. 4, pp. 34–40, Apr. 2008.

[24] A. Bryman, *Social Research Methods*. Oxford University Press, Inc., 2001.

[25] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal*, vol. 11, no. 2, pp. 127–153, Apr. 2001.

[26] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, Mar. 2005.

[27] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Computers & Security*, vol. 32, no. 1, pp. 90–101, Feb. 2013.

[28] D. B. Parker, "Restating the foundation of information security," *Computer Audit Update*, vol. 1991, no. 10, pp. 2–15, Oct. 1991.

[29] P. Dourish, R. E. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, Nov. 2004.