Lessons Learned from an Information Security Incident: A Practical Recommendation to Involve Employees in Information Security

Teodora Tatu
Goethe-University Frankfurt
teo.tatu@yahoo.com

Clara Ament
Goethe-University Frankfurt
ament@wiwi.uni-frankfurt.de

Lennart Jaeger
GGS of Management & Law
lennart.jaeger@ggs.de

Abstract

With the increasingly negative impact of information security attacks, measures of information security, which address the weakest link in the information security chain, namely the employee, have become a necessity for today's business world. One way to improve employees' – yet limited – information security awareness is to learn from past information security incidents.

This study theoretically builds upon the so called involvement theory to extend the existing research on information security awareness. Insights gained from 34 interviews suggest that involvement accompanied with a detailed review of past security incidents has a positive effect on staff's information security awareness. Employees, directly affected by an information security incident, gain significant information security expertise and knowledge which they can, again, share with their colleagues. Moreover, constructive team work in the light of information security risks as well as an adequate adjustment of security-related measures is fostered.

1. Introduction

Computers and the along going interconnectedness are necessary for our daily activities and no successful business could thrive without. Web-based technologies have brought with them many benefits to companies and their customers. However, as is the case for security breaches, also negative consequences and risks have become relevant over the last decade. Available statistics show, that the number of organizations that experienced at least one effective attack over the last 12 months, has risen from 70.5% one year prior to 75.6% in 2016 [6]. Thus, information security is momentous on both the private and professional level.

This is why specialists are continuously developing technological solutions for the protection of important systems as well as information assets and, thereby, safeguard operating environments. Hackers, however, choose the weakest link in any organization's security architecture to access information. They try to bypass technological countermeasures by focusing on users with information system access [4]. Attackers often exploit employees' vulnerability or naivety by relying on their willingness to help. This psychological manipulation inducing individuals to share confidential information is called social engineering. In short, social engineering is the attacker's "low-tech" approach to invade the "high-tech" world of the World Wide Web, where trusting individuals are used as "means to an end" [21].

As a consequence, besides focusing on technological security solutions, scholars' (and along managers') attention has recently been redirected to human influences and actions, therefore, entering the behavioral information security field. Both unintended and purposeful actions, such as naïve mistakes, ignorance, passivity, lacking awareness, and intentional destruction, respectively, need to be considered. The risk and impact mitigation of information security incidents begins with the enforcement of effective policies, employees' education, and awareness training. Thereby, limited information security awareness (ISA) seems to be the main obstacle for an effective cyber threat defense and implies a high probability of information security incidents.

This paper introduces a constructive perspective on information security incidents. An information security incident can be an enormous learning opportunity leading to improved security behavior in the future. Information security incidents are a great prerequisite for future security-aware individuals to convert their theoretical knowledge on information security into real practice. This feature is already well-known to practitioners, for instance [38]. According to Schein, the best way for organizations and individuals to learn is through personal experience [29]. Information security incidents can lead to such experience [36].

Studies on how organizations can learn from an information security incident, in terms of raising

URI: http://hdl.handle.net/10125/50359
ISBN: 978-0-9981331-1-9

information security awareness among employees, are currently in an incipient phase. Only a few researchers have focused on information security incidents in general, analyzing, for instance, the number of incidents known by students [39] or addressing whether employees' computers have ever been infected with harmful viruses [17]. Siponen has identified a gap in information security awareness. He based his work on the notion that information security awareness together with an organizational viewpoint should represent a constitutional part of citizens' general knowledge in an information society. He poses that "anyone who regards information in any form as an important asset (…) should be aware of the possible threats related to it" [32]. To the best of our knowledge, we are the first to interpret a threat in the form of an information security incident as a learning source with respect to the concept of involvement. Using the so called involvement theory as a theoretical lens, we aim to extend the existing research concerning employees' information security awareness. By doing so, this study addresses the following research question:

How does involvement influence employees' information security awareness?

This research question is answered by drawing from the existing theoretical background. In addition, we present insights from a qualitative study with data collected through 34 interviews. Results suggest that if a past information security incident is adequately reviewed and based on this review employees occupy a multiplicative role, share their previous experiences, act interactively in a collaborative manner, undergo various organizational security-related interventions, and possess a proper know-how in their working field the level of information security awareness within their organization rises noticeably.

The remainder of this paper is structured as follows: section 2 presents the theoretical foundation of the research model and section 3 gives away insights on the data collection. Taking into consideration the presented theoretical foundations, in section 4 the research results are discussed and propositions are formulated. Section 5 concludes with the final implications as well as the research limitations leading to future research possibilities.

2. Theoretical background

This section discusses information security awareness as the central construct followed by a comprehensive explanation of the involvement theory and thereby provides the framework for our information security involvement theory.

Information security awareness is considered as individuals' perception of the relevance and the significance of information security. The concept of ISA implies the existence of conscious individuals, with a good understanding of information security practices, including their clear scope and objectives, and individuals who recognize potential information security exposures to risk [31, 33, 35]. We follow the definition by Bulgurcu et al. who defines ISA as "an employee's general knowledge about information security and his cognizance of the information security policy" [7]. Whereas ISA is a mental condition that does not necessarily have an effect on real practices, information security behavior goes beyond the theoretical general understanding of information security issues and stresses the observable and measurable activities of an employee. Henceforth, this research presents how the involvement theory, a theory from social science, can be applied to the behavioral information security context in order to achieve a more systematic understanding of how information security awareness can be raised within organizations.

If individuals perceive a behavior as positive and let themselves be influenced by others then the probability of having higher intentions rises, and individuals will be more likely to perform a given behavior [1]. In line with this, employees' information security awareness should be triggered by involvement.

2.1. Involvement theory

Involvement fosters employees' information security awareness which in turn establishes a secure behavior within organizations. Formerly, the involvement theory has been applied to different fields, such as product involvement, student involvement, and customer involvement.

The theory takes into account the degree of energy, time, and participation dedicated to a particular activity [19] and distinguishes four sub dimensions of involvement: knowledge sharing, collaboration, intervention, and experience. A study conducted by Safa et al. uses these aspects to reveal the influences of involvement on employees' attitude towards compliance with information security policies (ISP) [28]. Results show that information security knowledge sharing [12, 33], collaboration [37], intervention [3, 24], and information security experience [27] all have significant effects on an individuals' attitudes towards information security compliance with ISP.

2.2. Information security involvement theory

This paper adapts the basic elements of the original theory slightly modifying two of them. In the following, we define the four sub dimensions individually. Furthermore, we describe how these factors enhance employees' information security awareness. A systematic overview is provided by figure 1.

Originally described as knowledge sharing and slightly modified in this paper, experience sharing is a social learning strategy that helps one to gain new insights from others sharing previous experiences and resulting implications [10]. In this research, information security experience sharing refers to the shared lessons one can learn from a direct exposure to an information security risk. Although learning through own experiences might offer more insights, experience sharing may play an important role in the learning process of employees.

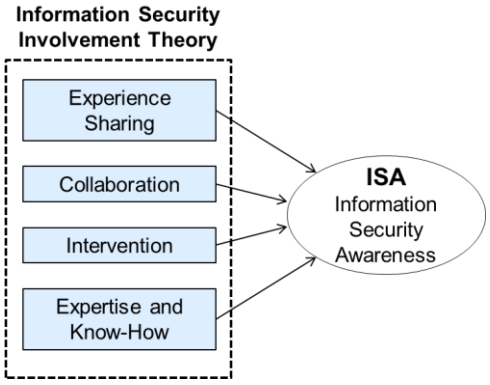

Figure 1. Information security involvement theory

Sharing experiences might create an appreciation for the witness of an incident as it implies braveness and willingness to expand others' knowledge horizons at one's own expense. In return for sharing their experience, witnesses or victims of incidents might be, on the one hand, rewarded with admiration, acknowledgement, and gratitude (e.g. reputation as experts). On the other hand, individuals might feel ashamed. This paper, however, highlights the importance of putting information security incidents into a positive context with a vast learning potential. The act of sharing experiences encourages others to communicate and to develop new concepts together.

Data, information, and human knowledge constitute important organizational information assets when shared properly [18]. Ineffective asset management exposes enterprises to various risks, such as over-subscription, non-compliance payments, and security threats [11]. Preventing the repetition of similar negligent behavior or duplicating the same solutions by sharing the already known lesson allows for a better investment of time and money in other areas [12]. Sharing prior relevant experiences in the field of information security is a considerable source of information security awareness [25]. Thus, on the organizational information security level, it is proposed that experience sharing is an important factor that positively affects employees' information security awareness.

The second element of the involvement theory is collaboration. Gray defines the term collaboration as "a process through which parties who see different aspects of a problem can constructively explore their differences and search for solutions that go beyond their own limited vision of what is possible" [14]. Incorporating aspects of this research and extending the definition, in this paper collaboration is understood as an interactive affair with a shared common objective (i.e. increasing information security) sustained by voluntary membership, mutual decision making, acceptance of procedures (i.e. compliance with ISP), and a predefined timeline in order to achieve a certain goal.

Safa et al. pose that information security collaboration is a great opportunity for security experts as they can "collect, integrate, classify, distribute, and share knowledge" with other specialists and employees [28]. If employees collaborate with each other, potential information security threats can be evaluated [20]. Information security collaboration expands practitioners' and end-users' knowledge about information security breaches, reducing redundant efforts in collecting and processing information. Contextualizing these findings with this study's concept of raising information security awareness, it can be assumed that collaboration between employees, IT experts, and others can positively influence information security awareness. Consequently, a higher level of information security awareness builds the prerequisite of secure behavior among employees.

Representing the third category, intervention is manifested through a set of tools, which deploy insights gained from security incidents, aiming to change employees' information security behavior. These tools can be provided to many individuals, for instance, in the form of recalling print media or interactive training and workshops, which pick up scenarios colleagues have been confronted with. These tools can positively influence end-users' beliefs, understanding, and prediction of cyber security both on an individual and organizational level [30].

Well-designed measures, which are easy to understand and less time-consuming, are highly desirable. Measures can incentivize and motivate employees to become interested in information security, actively participate, and evolve an intrinsic sense of information security awareness. As a result, their heightened awareness should be reflected in good security practices. "Relevance, timeliness, and consistency" are essential features when assessing security awareness intervention initiatives [26].

Research shows that a positive intervention influences the level of knowledge considering ISP, which is reflected in an improved attitude towards this policy [25]. Analogue to this positive influence, it may be assumed that organizational intervention triggers and influences employees' information security awareness as well.

The fourth and last dimension, expertise and know-how, is also redefined. Within the field of psychology, expertise is defined as the "extent and organization of knowledge and special reasoning processes to development and intelligence" [15]. Expertise is described as skilled performance across physical and cognitive domains [5, 8]. On the one hand, expertise might be independent of the number of years of experience an employee has. It can stem from one's inherent talent, interests, and enthusiasm for a specific domain. On the other hand, expertise can also be fostered by experience, referring to occupation or employment, which may lead employees to actively improve their competencies over time.

In order to amplify the expressiveness of the fourth element, it is completed by the following extension: know-how. In the presented context we focus on intangible know-how, such as strategic practices, developed concepts, ideas, and other acquired learning techniques an employee might possess. Classified as tacit knowledge [26], which is difficult to be transferred to another individual through written or oral communication, know-how refers to practical proficiencies and familiarities within a specific area.

Albrechtsen analyzes users' knowledge and experience and their contribution in the information security context [2]. Findings show that missing information security knowledge and experience represents the main issues with regard to the end-users' roles in an information security-related work. Accordingly, knowledge and experience have, thus, a significant effect on the formation of good (secure) behavior. Relating Albrechtsen's study to our theory, the following idea can be derived: expertise and know-how may foster employees' information security awareness.

3. Methodology

Due to the scarcity of reasonable quantitative measures, it is appropriate and commonly accepted in the IS literature to apply qualitative measures [23]. Thus, the relations described in the theoretical background were analyzed by means of a real-life situation in order to establish causal structures.

The data was collected based on interviews with information security experts, non-IT employees, as well as IT experts, all working for a large organization with more than 5.000 employees. In total 34 semi-structured interviews were conducted. The set of participants comprised of 23 men and 11 women. The average interviewee was 45 years old. Participants received information about the study's academic and independent, nature as well as its objective, namely an information security awareness analysis among employees. During the interviews the respondents related in detail to a severe information security incident which took place two weeks prior to the interviews[1].

The interviews involved a prepared guideline divided into three sections. The first section stressed the demographic and professional characteristics of the interviewees (e.g. age, gender, highest education level, years of work experience, current position in their department). The second section put emphasis on information security awareness. The participants were asked about their current understanding of information security awareness and how they personally define information security awareness. Furthermore, questions addressing the following issues were asked: information security measures (e.g. security education, training, and awareness programs or security warnings) involving their desirability, feasibility, and effectiveness, the roles of employees and security experts, their level of involvement in information security, exchanges on information security in the departments, as well as challenges and success factors of information security awareness. The final section referred to past information security incidents, the course of the events, and the lessons learned from these experiences (e.g. whether it was punctuated by peers or

[1] Selected employees of the case company received prepared data via phishing emails which was contaminated with ransomware. One employee of the involved institution opened the email attachment, thus, encrypting all files in his department. As a consequence, approximately 200 employees were hindered from their workflow. Post-incident measures from the organizational side were sent to all employees. These promoted the correct behavior when receiving suspicious emails. In addition, an intranet message and a pop-up notification were sent out to all workstations.

supervisors, or if and how the information security department communicated it transparently). This last part also involved how participants were personally affected by incidents, and what post-measures were implemented. It was emphasized how the importance of information security for departments changed after an incident took place compared to the status before. Furthermore, it was asked how the employees were sensitized by the incident towards information security as well as whether they recognize a change in their behavior.

Taking into consideration the different perspectives of employees, including the victims of the information security incident, co-workers from the same department, other affected collateral units, and the corresponding information security officers the circumstances of the last security incident are presented with the highest possible degree of objectivity. The data was interpreted to generate theoretical propositions [24]. The analysis of transcripts was done by means of an iterative multilevel coding process which can be found in other information systems studies [e.g. 9]. The answers of the participants were observed to be similar with increasing number of conducted interviews; therefore, the need of a wider sample was alleviated.

4. Results

In the subsequent section, we present the results regarding the information security involvement theory and the effects the four different dimensions of information security involvement have on employees' information security awareness.

We found that the ransomware incident increased the overall information security awareness among the employees. The majority of the affected people became more attentive and skeptical about received emails, thus handling them less hazardously. Post-incident observations of the interviewees indicate that dedicated and passionate workers with a high level of involvement in their profession adopted a multiplicative role and experienced changes in their behavior towards information security.

4.1. Information security experience sharing

Results suggest that experience sharing has a positive influence on the information security awareness of co-workers. The social environment benefits once a witness of an incident reveals the experienced casualties. The interviewees' responses indicate that they need a central information security service desk (separate from the traditional and technical IT helpdesk). Furthermore, employees would benefit from particular expertise when it comes to specific information security matters. One respondent, for example, highlights this need and expresses employees' confusion with regard to the lack of direction in cases of information security challenges:

> *"But the service desk is more responsible for technical matters and explaining them – is there a correct program, is there not? Am I correctly working within a security boundary controlled by given restrictions and guidelines? It is evident that we have a compliance unit, we have a technical one (relating to the IT service desk), we have an IT compliance unit, however, we are lacking when an employee asks questions in regard to IT security. Where do we go from here?"* (male, 53 years)

Alternatively, information security experts or simply people whose awareness is already high could take over this "ambassador" function of the knowledge sharing person in order to share their experiences with other employees for them to gain more direction and support, such as in the following case:

> *"If a colleague would be the correct contact person (…) and source of information (…) and willing to provide help or an answer or even additional teachings, then he would receive my first phone call."* (female, 30 years)

Enabling a network of people responsible for removing confusion, employees will be encouraged to be more communicative and willing to obtain more insights into this topic. Experience sharing can also be considered as a top-down type of communication, especially after an information security incident. Therefore, it is of high importance that team leaders share, transparently, the occurrences of information security incidents and explain the direct consequences, at the same time sensitizing the employees. As observed, there are many ways (e.g. open meeting discussions, direct contact persons) to foster information security experience sharing:

> *"This is extremely important because mistakes made by others don't have to be repeated by yourself."* (male, 51 years)

If people are sensitized with the help of insights from a former information security incident, it is very likely that they gain awareness, thus, it is proposed:

Proposition 1: Experience sharing has a positive effect on employees' information security awareness.

4.2. Information security collaboration

The first and simplest form of collaboration is interpreted in this paper as the one-way communication within a company. While eliminating fears and inhibitions and stressing their approachability and availability, leaders' collaborative attitude might be an important catalyst of fostering communication between empathetic leaders and employees. A properly chosen management style strengthens employees' self-confidence in sharing their ideas with others more often. At the same time, it might sensitize and encourage them to adopt a stable information security behavior on a long-term basis. A minor change in attitude and leadership style on the strategic and managerial level might have a huge impact on employee perception.

Respondents recognized that organizational discipline depends on the employees' perception of the superior as a role model, as seen in the following statement:

> *"It depends largely on the responsible superior, on the business, on the leading culture in the department. It does not necessarily depend on the sector, but more on how the department-leader reacts. This leads us to the highly important role of the head of department (...) whose function is being a role-model for all the others (...) also in terms of information security."* (male, 37 years)

The one-way communication can be applied in this sense to another situation: people often behave the way they observe others to behave. Suitable management practices will be reflected in good and compliant employee behaviors.

> *"As a matter of fact, I do see this as my responsibility as a leading force. I have to do this, and therefore I just do it. Security topics are also leadership topics. And it [referring to secure behavior] has to be exemplified by the leader as well. This is the biggest problem in security. If security measures are not demonstrated and used correctly by the leader, then no one will take the measures seriously. (...) Performing as a leader means, in the end, to consequently implement a secure mindset from top-level to middle-level and finally to low-level leaders."* (male, 59 years)

Another form of collaboration is the two-way interaction between managers and employees. One way of encouraging people to collaborate is, for example, creating a competitive character in providing improvement suggestions in an open "talent pool". In this pool, good ideas can be voluntarily disclosed and employees can vote for their favorite ones. Sharing suggestions should, however, be kept as simple as possible without high effort costs on employees' side, such as bureaucratic effort.

> *"Well, I think the disclosure of suggestions is helpful in general. If people can, for instance, vote transparently for the best suggestion then an open pool could become a competition."* (male, 26 years)

Creating clear concepts and ideas can be beneficial for developing further information assets of an organization. Giving feedback related to the realization of the concepts oftentimes has an even more satisfactory and constructive effect. An observable change, based on one's input is supposed to impact the individual willingness to collaborate and, therefore, to embrace information security awareness. Thereby, in the context of collaboration, the emphasis is shifted from one-way communication (manager – employee) to two-way interaction (employee's input – manager's feedback), which might have more power over some individuals:

> *"For me personally to see my ideas regarding information security put into action is more important than to receive a reward or payment or whatever else. So, I expect from a system a level of transparency in regard to what happened with past ideas."* (male, 26 years)

Collaboration between employees can develop sustainable information security awareness. Thus, we propose:

Proposition 2: Collaboration has a positive effect on employees' information security awareness.

4.3. Information security intervention

Well-designed and customized information security measures are understood as tools organizations implement with the aim to change individuals' behavior. During the interviews, participants had to evaluate a list of intervention measures. Results suggest that the best-rated measures, in terms of perceived effectiveness and feasibility, are security related training, presentations, informational events, and workshops (96.2%). The second-best perceived measures are a service hotline (with both reactive and preventive purposes) together with an IT helpdesk alternative (over chat and email) (93.7%). The third most voted measures are live hacks, which demonstrate how easy it is to gain access to computer systems (90.5%). The interviews revealed surprisingly positive reactions to the latter, for example:

> *"Oh, no! Participation in a live hack! That gets me really interested! For me, that would be off the scale interesting. But it would also be interesting for the average user."* (male, 44 years)

Besides the self-implying aspect that a security-related measure has, a constructive message that everyone is able to understand, other relevant aspects of a potential measure arise from the responses. Further proposed facets of an effective security tool are integration into the day-to-day workflow, reasonability, practicability, and time strains. These aspects should be integrated into future practices as they might influence employees' willingness to exhibit good behavior.

Besides their harmonic integration into the workflow, reasonable and practical information security measures should be constantly adapted to new business cycles and current market events in terms of information security. The main driver for this ever-changing adaption is one's previous experience (e.g. past information security incidents) and therefrom gained knowledge. By means of involvement, employees can derive lessons especially right after an information security incident. Due to this temporal proximity, they might be prone to new security-related learning.

In line with these identified aspects, it is proposed that if interesting, concise, insightful, and justifiable security-related measure are continuously adapted and correctly implemented people will be more information security aware. Accordingly, it is postulated:

Proposition 3: Intervention has a positive effect on employees' information security awareness.

4.4. Information security expertise and know-how

When employees are more proficient and experienced in their field of work, they are more likely to act with greater care and in a proper and compliant manner. Great expertise and know-how are achieved through personal determination, enthusiasm as well as professional experience, and they are not easily transferable to others. People that are classed as good professionals possess this intangible know-how asset, they may exhibit good behaviors in every circumstance; they want to satisfy their curiosities and look for solutions and the best way of handling when faced with suspicions about any irregularities.

Results suggest that information security expertise can be gained through experience, but not vice versa. Therefore, information security awareness is strengthened over time. The more an employee is preoccupied with the topic of information security, the more the individual becomes aware of potential threats. Responses confirm the assumed relationship between experience and expertise. The sensitizing process of employees is perceived as a learning process:

> *"I think this is a learning process. So, I mean this Trojan [referring to the ransomware] two weeks ago – that was not the first time it happened. But it was now even stronger than the others. Maybe if you had sensitized the people before, maybe you could have prevented it [referring to the ransomware incident], but I do not know exactly what to do… I believe the more frequent this happens now, the more one is actually prompted to the thought «OK, strange attachment, strange sender» the more you really have so called learning by doing."* (female, 28 years)

As one's know-how can hardly be transmitted to others in written and/or verbal forms, an information security incident can be used as a great opportunity to increase individuals' receptivity level. This is the case as people may pay considerably more attention to what is being taught to them in regard to security measures right after a detrimental security incident has occurred and affected them. This is supported by the following statement:

> *"Well, since this incident approximately half a year ago, my radar is always on high (…) and since this time [referring to the ransomware incident] I am therefore very*

sensitive to alert something because it is a very relevant issue." (female, 48 years)

One's interests, propensity to learn, and professional experience have a significant role in determining one's professionalism or, in other words, one's information security expertise. Hence, we make the following statement:

Proposition 4: Expertise and know-how have a positive effect on employees' information security awareness.

5. Discussion

This study qualitatively analyzes a sample of 34 interviews conducted among employees of a multinational institute right after an information security incident with the purpose to extend the understanding of how an information security incident impacts employees' perception on information security awareness. We focus on the establishment of information security awareness employing the involvement theory and, thereby, addressing the identified research question.

The results reveal the influential nature involvement has on employees' information security awareness. Henceforth, it can be concluded that employees undergoing an information security incident gain relevant experience which can be shared with peers. Next, they might change their operational approach into constructive team work, thus, acting in a collaborative manner. Based on the newly acquired knowledge, security-related measures can considerably be adjusted, determining people to adopt good information security behaviors within their organization. Using the insights from these results, organizations can develop measures of recovery after and even measures of prevention against information security incidents considering aspects that were found to be relevant to employees.

In the following, we discuss the practical as well as the theoretical implications and end with the research limitations which suggest future research endeavors.

5.1. Contribution and implications

As the interviews confirmed, information security, especially behavioral information security, has gained increasing attention on businesses' and scholars' agenda. While researchers have begun to examine the effect the human factor has on information security, studies identifying the aspects which specifically generate and foster information security awareness, based on social science theories, are limited.

The results of this study provide a starting point for understanding how organizations can benefit from information security incidents. In addition, the study's results shed light on the aspects organizations should focus on in order to increase their employees' level of information security awareness. This qualitative study allows a new interpretation of information security incidents, being a great source of information to organizations on how to best sensitize their employees, and demonstrates the possibility to transform theoretical knowledge of employees (i.e. information security awareness) into real beneficial actions (i.e. information security behavior). Particularly, the contributions go beyond previous research that, for example, studied the importance of organizational security behaviors on the effectiveness of ISP [16] or identified the antecedents of employee compliance with ISP [7]. This paper went further to examine another side of what exactly the significant antecedents of employees' information security awareness are (i.e. experience sharing, collaboration, intervention, expertise, and know-how). Established information security awareness can be then reflected, for example, in compliance with ISP.

Moving along to practical implications for information security practitioners, this paper addresses the absence of information security awareness as a noteworthy matter for organizations, which can cause serious harm in the long run. Human capital intensive businesses ought to take advantage of early improvement possibilities before it is too late. This will enable them to adapt to the existing dynamic and risk-heavy environment and possibly rethink their organizational culture to make secure working as comfortable and intuitive as possible. This, according to the conducted interviews, is highly relevant, as employees wish to recognize security as a benefit, not an impediment, to their workflow. Consequently, the countermeasures should be designed to have an intuitive nature.

The findings point out important steps executives can undertake to foster information security awareness for sustainable organizational development. First, managers should visibly encourage and reward information security experience sharing of the key person with an information multiplicative role. Second, intervening on a repetitive basis (e.g. through reminders such as intranet articles, warning messages, etc.) and leading compassionately, while demonstrating role-model security-related practices, fosters the assimilation of information security concepts among employees. Enforcing this suggestion may trigger employees' information security awareness in the long

run. In this regard, a perceptional change towards information security incidents as learning sources, and implementing the above-mentioned measures would be a beneficial awareness spreading opportunity for organizations, which are more and more exposed to external threats.

5.2. Limitations and future research

Limitations have to be taken into consideration when assessing the relevance of the implications made.

To begin with, the conducted interviews had a limited number of participants. However, it must be said that after conducting a majority of the interviews the answers became noticeably similar, indicating similar statements ameliorating the need for further interviews. The retrospective nature of the interviews, despite the relatively short time period of 14 days from the last notable phishing incident, may have also caused biases in the statements given, as individuals may not accurately remember the exact experiences. As this study is set up as qualitative research, it implicitly involves further limitations such as a degree of subjectivity. The paper's approach was based mainly on the interpretation of the interviews and, therefore, the susceptibility to cognitive biases and, thus, the predisposition to subjectivity, might have been increased. However, it was attempted to maintain the highest possible level of objectivity when identifying and evaluating the theory's components. With the qualitative nature of the study in mind, the need for further research and a quantitative validation of the suggested propositions is identified [22]. In order to reach comparative results, the research should be extended to further case studies across various industries. Such case studies might aim to examine sector-specifically how individuals perceive information security incidents.

In conclusion, it would be a grave mistake to ignore the recent trends of growing automation and our continuously changing technological environment and not to focus on behavioral information security. The human-computer interaction is ever-present in both the private and professional realm, and as individuals are one of the main causes of information security breaches, which may incur great losses to an organization, they should stand in focus when trying to combat such incidences.

6. References

[1] Ajzen, I. & Fishbein, M. A., 1980. Understanding Attitudes and Predicting Social Behavior. NJ: Prentice-Hall: Englewood Cliffs.

[2] Albrechtsen, E., 2007. A qualitative study of users' view on information security. Computers & Security, 26(4), pp. 276-289.

[3] Albrechtsen, E. & Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), pp. 432-445.

[4] Applegate, S. D. M., 2009. Social Engineering: Hacking the Wetware!. Information Security Journal: A Global Perspective, 18(1), pp. 40-46.

[5] Bailey, R. W., 1996. Human performance engineering: using human factors/ergonomics to achieve computer system usability. Englewoods Cliffs: NJ: Prentice Hall.

[6] bluecoat, 2016. Cyberthreat Defense Report 2016. [Online] Available at: http://dc.bluecoat.com/Cyberthreat_Defense_Report_Download?src=GoogleAdwords_BC_CyberEdgeReport_Feb16&gclid=Cj0KEQiAnb3DBRCX2ZnSnMyO9dIBEiQAOcXYH6DIqbwYwRWegcF0wtIIc2dbn_gps2tuViqVjdbyHw4aAoI98P8HAQ. [Accessed January 2017].

[7] Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), pp. 523-548.

[8] Caldwell, B. S., 1997. Components of information flow to support coordinated task performance. International Journal of Cognitive Ergonomics, pp. 25-41.

[9] Charki, M. H., Josserand, E. & Boukef, N., 2016. The paradoxical effects of legal intervention over unethical information technology use: A rational choice theory perspective. Journal of Strategic Information Systems, Band (in press).

[10] Chen, T., Drennan, J. & Andrews, L., 2012. Experience sharing. Journal of Marketing Management, 28(13-14), pp. 1535-1552.

[11] Deloitte & Touche, 2016. Software Asset Management | Reducing costs, mitigating risk, gaining control, s.l.: Deloitte. [Online] Available at: https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/risk/me_risk_sam-reducing-cost.pdf. [Accessed January 2017].

[12] Feledi, D., Fenz, S. & Lechner, L., 2013. Toward web-based information security knowledge sharing. Information Security Technical Report, 17(4), pp. 199-209.

[13] Flores, W. R., Antonsen, E. & Ekstedt, M., 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, Band 43, pp. 90-110.

[14] Gray, B., 1989. Collaborating: Finding Common Ground for Multiparty Problems. San Francisco: Jossey-Bass.

[15] Hoffman, R. R., Feltovich, P. J. & Ford, K. M., 1997. A general framework for conceiving expertise and expert systems in context. Expertise in context, pp. 543-580.

[16] Hsu, J. S.-C., Shih, S.-P., Hung, Y. W. & Lowry, P. B., 2015. The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. Information Systems Research, 26(2), pp. 282-300.

[17] Kranz, J. & Haeussinger, F., 2013. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. Milan, Italy, Proceedings of the 34th International Conference on Information Systems (ICIS 2013).

[18] Lee, G., Lee, W. J. & Sanford, C., 2011. A motivational approach to information providing: A resource exchange perspective. Computers in Human Behavior, 27(1), pp. 440-448.

[19] Lee, S. M., Lee, S.-G. & Yoo, S., 2004. An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), pp. 707-718.

[20] Mace, J. C., Parkin, S. & van Moorsel, A., 2010. A collaborative ontology development tool for information security managers. San Jose, California, CHiMiT '10 Proceedings of the 4th Symposium on Computer Human Interaction for the Management of Information Technology.

[21] Manske, K., 2006. An Introduction to Social Engineering. Information Systems Security, 9(5), pp. 1-7.

[22] Mingers, J., 2001. Combining IS Research Methods: Towards a Pluralist Methodology. Information Systems Research, 12(3), pp. 240-259.

[23] Myers, M. D., 1997. Qualitative Research in Information Systems. MIS Quarterly, 21(2), pp. 241-242.

[24] Myers, M. D. & Klein, H. K., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly, 23(1), pp. 67-93.

[25] Parsons, K. et al., 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, Band 42, pp. 165-176.

[26] Polanyi, M., 1958. Personal Knowledge – towards a Post-Critical Philosophy. Chicago: University of Chicago Press.

[27] Rhee, H.-S., Kim, C. & Ryu, Y. U., 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), pp. 816-826.

[28] Safa, N. S., Von Solms, R. & Furnella, S., 2016. Information security policy compliance model in organizations. Computers & Security, Volume 56, pp. 70-82.

[29] Schein, E. H., 1993. How can organizations learn faster? The challenge of entering the green room. Sloan Management Review, 34(2), pp. 85-92.

[30] Shaw, R. S., Chen, C. C., Harris, A. L. & Huang, H.-J., 2009. The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), pp. 92-100.

[31] Siponen, M. T., 2000. A Conceptual Foundation for Organizational Information Security Awareness. Information Management and Computer Security, 8(1), pp. 31-41.

[32] Siponen, M. T., 2001. Five dimensions of information security awareness. Computers and Society, 31(2), pp. 24-29.

[33] Straub, D. W. & Welke, R. J., 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22(4), pp. 441-469.

[34] Tamjidyamcholo, A., Shuib, N. L. M., Rohani, V. A. & Baba, M. S. B., 2014. Evaluation model for knowledge sharing in. Computers & Security, Band 43, pp. 19-34.

[35] Thomson, M. E. & Von Solms, R., 1998. Information security awareness: educating your users effectively. Information Management & Computer Security, 6(4), pp. 167-173.

[36] Tyre, M. J. & Orlikowski, W. J., 1994. Windows of Opportunity: Temporal Patterns of Technological Adaptation in Organizations. Organization Science, 5(1), pp. 98-118.

[37] Vroom, C. & Von Solms, R., 2004. Towards information security behavioural compliance. Computers & Security, 23(3), pp. 191-198.

[38] Wilson, M. & Hash, J., 2003. Building an Information Technology Security Awareness and Training Program, Washington DC: National Institute of Standards and Technology Special Publication 800-50.

[39] Zhang, P. & Li, X., 2015. Determinants of Information Security Awareness: An Empirical Investigation in Higher Education. Forth Worth, USA, Proceedings of the 36th International Conference on Information Systems (ICIS 2015).