It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs

Moufida Sadok, Steven Alter, Peter Bednar

Abstract

Purpose- This paper presents empirical results exemplifying challenges related to information security faced by small and medium enterprises (SMEs). It uses guidelines based on work system theory (WST) to frame the results, thereby illustrating why the mere existence of corporate security policies or general security training often is insufficient for establishing and maintaining information security.

Design/methodology/approach- This research was designed to produce a better appreciation and understanding of potential issues or gaps in security practices in SMEs. The research team interviewed 187 employees of 39 SMEs in the UK. All of those employees had access to sensitive information. Gathering information through interviews (instead of formal security documentation) made it possible to assess security practices from employees' point of view.

Findings- Corporate policies that highlight information security are often disconnected from actual work practices and routines and often do not receive high priority in everyday work practices. A vast majority of the interviewed employees are not involved in risk assessment or in the development of security practices. Security practices remain an illusory activity in their real world contexts.

Research limitations/implications- This paper focuses only on closed-ended questions related to the following topics: a) awareness of existing security policy; b) information security practices and management and c) information security involvement.

Practical implications- Our empirical findings show that corporate information security policies in SMEs often are insufficient for maintaining security unless those policies are integrated with visible and recognized work practices in work systems that use or produce sensitive information. Our interpretation based on WST provides guidelines for enhancing information system security.

Originality/value- Beyond merely reporting empirical results, this research uses WST to interpret the results in a way that has direct implications for practitioners and for researchers.

Keywords information security, security practices, work system theory, socio-technical approach, SMEs.

Paper type Research paper

1. Introduction

Information system (IS) security is a challenge for all companies and government organizations ranging from the largest of the smallest. Our research looks at information security in SMEs, many of which are increasingly dependent on the use of information technologies and networked systems to support their business operations and decision-making processes. That dependence could make them especially vulnerable to IS security threats because of their limited human and technical resources and limited sophistication related to IS vulnerability issues.

The UK has devoted substantial resources toward professional and governmental initiatives aimed at improving security in SMEs because SMEs contribute significantly to the UK economy and comprise the majority of businesses in every main industry sector (Home Office, 2017). For example, the national cyber-security strategy 2016-2021 comprises programmes and sets guidelines to help SMEs with developing and implementing preventive and deterrent security measures.

Despite those programs, the cyber-security breaches survey 2018 (Cyber Security Breaches Survey, 2018) indicates that only 27% of businesses have a formal security policy in place and that most organisations are still unaware of major government cyber security initiatives and accreditation schemes. It is notable that investment in ongoing education and awareness programmes continues to expand. However, the effectiveness of training and awareness sessions is questionable as the number of staff-related security incidents continue to increase. A number of studies have outlined the inadequate impact of general training campaigns and generic security courses on user behaviour and awareness (e.g. Parsons et al., 2014).

Our research emphasizes the centrality of human and organisational factors in information security. It focuses on the visibility and effectiveness of security practices as part of everyday work practices of typical employees. We argue that the adaptation of standardised security frameworks to real business practices requires an understanding of local work systems. The distinction between IS as a data processing system and IS as a human activity system points to potential gaps in matching security practices to organizational and business needs. Our results demonstrate that those issues are relevant and important to explore in information security research.

The remainder of the paper is organized as follows. The next section identifies past research related to information security. Section three introduces work system theory (WST), a theoretical lens that provides many insights about information security even though it has not been used extensively in that area. Section three also provides information security guidelines that follow directly from the main ideas in WST. Section four summarizes the research context, the details of our data collection process, and the findings of our empirical study. Those findings illustrate important weaknesses in SME security practices. We use WST to explain the results by viewing security-related practices in the context of work systems whose participants give highest priority to meeting their assigned work responsibilities and lower priority or, in some cases, no priority to maintaining information security. We purposefully present the guidelines before the empirical results to help in visualising what these results tell us. The final section covers limitations of the current research and plans for future research.

2. Background

Our literature review is organized around three main themes: socio-technical approach to information security, information security in organisational context and information security in SMEs.

Overall, this literature review shows that information security is often viewed as an overlay on top of other tasks and responsibilities. It also shows that SMEs are not well represented in past research on information security. Much of that literature provides survey results or simply makes claims, but very little of it is presented in relation to a theoretical perspective that illuminates what the results mean and how to address the problems that are uncovered.

2.1 Socio-technical approach to information security

We focus on information security even though information security and computer security are intertwined. Siponen (2005) distinguishes between IS, software engineering, computer science and mathematics and associates different research communities with those disciplines. IS researchers use a variety of positivist ad interpretivist orientations, whereas most researchers in computer science and mathematics tend to have a positivist orientation. Irrespective of the separation between computer science and software engineering, the divergence between interpretivism vs. positivism is reflected in the coverage of security practices in IS research. Tryfonas et al. (2001) proposed an interpretive framework for expanding and incorporating security functions in the whole IS development. Coles-Kemp (2009) argues for a need to undertake more research on the complex relationships between human, organisational and technological aspects in information security. While challenging and time consuming, that type of exploration has potential to contribute to more effective information security management. A monolithic secure systems development methodology would be of limited value since information security functions depend on both human and infrastructural elements that should not be considered in isolation from each other. In particular, Coles-Kemp and Hansen (2017) argued that real-world everyday security problems must be seen as an emergent consequence of human activities, and separating social and technical strands is neither desirable nor advisable. That sociotechnical approaches and practices continue to be relevant in today's world is made clear in discussions by several researchers (e.g. Berniker, 2016; Kowalski et al., 2019; Sarker et al., 2019). A contemporary interpretivist sociotechnical approach to information security requires a critically informed mindset (e.g. as described by Myers and Klein, 2011). This would potentially result in better understanding of the role and application of security functions in situated practices.

2.2. Information security in organisational context

The alignment between security and business processes needs is a long-standing issue in security management. A plethora of examples in the literature demonstrate that effective security measures must be established within a clear organisational context. Research has shown that an exclusive emphasis on a technology-centered view induces flaws in the design and implementation of security solutions and that inclusion of people and processes is essential as a core part of secure and usable work systems (Baskerville, 1991; Bednar and Katos, 2009; Siponen and Willison, 2009). One of the fundamental problems is balancing conflicting requirements of security and usability in the context of everyday priorities in real world work systems and job practices (Sommerville, 2011; Furnell, 2016; Dhillon et al., 2016; Sasse and Smith, 2016). In this context, usability is not limited to technological features but also includes matters of efficiency, avoidance of distractions and convenience. Thus, security professionals should develop methods that minimise inconvenience and delays.

Many examples show that the workforce often finds ways of working around security compliance or bypass security controls in order to do their work effectively. Woltjer (2017) argues that workarounds reflect a misalignment between information security and other work goals and result from a lack of awareness or understanding of working practices, which leads to new vulnerabilities. The empirical study by Caputo et al., (2016) shows that there is no single definition of the concept of usable security nor clear evaluation criteria of usability even within the same organisation. According to the same study, many developers of security functionalities show a patronising attitude towards target users and do not really understand the need to deliver usability.

Conflicts between security and usability or convenience can be explained in many ways, one of which is inadequate or nonexistent involvement of professionals with operational knowledge of risk assessment and security policy development (Shedden et al., 2011; Spears and Barki, 2010). Business professionals' individual, contextual understandings of their work roles need to be channeled into design practice if appropriate security measures are to be established. A critical analysis of a sample of security policies from the UK's National Healthcare Service by Stahl et al., (2012) concluded that security policies can privilege certain groups of stakeholders such as managers and IT professionals and do not sufficiently integrate the views and concerns of doctors and nurses about medical matters. Inadequate staffing makes it even less likely that the existence of security policies will lead to effective implementation or relevance from users' perspective (Dhillon and Torkzadeh, 2006).

Albrechtsen and Hovden (2009) used the term "digital divide" to point out that there is a gap in knowledge and interests between security managers and users. In many cases, security professionals tend to focus on a model of business process, rather than on a real world organizational context. As a result, security practices often are developed independent of the needs of the surrounding human activity system. Information security methods that are disconnected from real world business practices often make it necessary for employees to breach security policies as the only way for them to do a good job (Albrechtsen, 2007; Koppel et al., 2015; Kolkowska and Dhillon, 2013; Adams and Sasse, 1999).

Information security research has also focused on the need for proper communication of the relevance of security controls to employees who are involved in the implementation of those controls in everyday work practices (Albrechtsen and Hovden, 2010; Karlesson et al., 2017). Applying network analysis techniques, Dang-Pham et al., (2016) showed the importance of identifying employees who are active in sharing security advice and security troubleshooting and involving them in security awareness programs. Such involvement has potential to support security engagement in the workplace. Hooper and McKissack (2016) question the technically-oriented job descriptions of CISO and suggest that CISOs should play a key role in matching security to business requirements. This entails both broad understanding of business processes supporting the delivery of value and strong communication skills need to work effectively with different groups of stakeholders including managers, business process owners and end-users. Ashenden and Sasse (2013) showed that CISOs often experience difficulties in communicating the why and how behind security measures and that there is need to use more effective channels or methods of communications to “sell” the relevance of such measures.

2.3 Information security in SMEs

Research on security practices in SMEs is limited, especially in relation to assessing security practices from employees’ point of view. While security practices vary by industry and company size, a key challenge for most SMEs is the integration of security functions into business processes. The comparative analysis of Dimopoulos et al., (2004) between two samples of SMEs in Europe and USA identified deficiencies in the main areas of security management practices, especially in a lack of engagement in developing security policies or undertaking risk assessments. These deficiencies were mainly attributed to insufficient technical and investment capacities to counter cyber-risks.

In spite of political initiatives to support SMEs preparedness, gaps in SMEs security practices illustrate their weak understanding of how to implement and manage effective security controls and measures. The latest survey by the UK’s Department for Digital, Culture, Media and Sport found that organisations interviewed prefer advice and guidance that is tailored to their contexts and needs (Cyber Security Breaches Survey, 2018). When it comes to the impact of awareness campaigns, Cyber Security Breaches Survey (2019) showed that around a third of the participants do not know “how to act on the advice they have seen or heard around cyber security”. In the same vein, the empirical study by Renaud (2016) involving 110 Scottish SMEs suggested that official bodies need to provide simple and easily understood advice to SMEs. That observation is consistent with ideas advocated by Mühe and Drechsler (2017).

A key implication of the above literature is that data security processes cannot be built on models that ignore real world organizational behaviour or work practices. Although the importance of security education and training is obvious, focusing only on education and training does not address essential human aspects of security systems such as motivation and relevance to the work context. Beyond the technical systems, a frequent weak link is the difference between the formal models behavior and actual behavior that occurs in human activity systems that involve sensitive information.

The work system approach discussed in the next section provides a systematic way of looking at information security as an integral part of the work that is being done.

3. Work system theory as a lens for information security

This section, which is based partly on Alter (2017), explains how work system theory (WST) can be used as a lens for visualizing and analyzing many information security issues. WST supports broad interpretations of empirical results in the next section that have direct implications for practitioners and researchers.

Sociotechnical researchers have used the idea of work system for decades (e.g., Trist, 1981; Sinha and Van de Ven, 2005; Mumford, 2006). That term appeared in the first edition of *MIS Quarterly* (Bostrom and Heinen, 1977). More recently, it was used as the basis of the work system method (WSM), a systems analysis method developed over several decades to help business professionals understand and analyzing IT-reliant work systems in their own organizations. Students or student teams (mostly MBA and Executive MBA) used versions of *WSM* to produce over 700 management briefings recommending improvments of problematic IT-reliant WS during 2003-2017, mostly in their own organizations. For example, Truex et al. (2010; 2011) discusses results of 75 and later 301 of those assignments. The core ideas in WSM were articulated as WST in Alter (2013). Those ideas have been used in at least 10 PhD theses, most recently Wong (2018), and have provided a usable systems perspective in research concerning topics such as open innovation platforms (Daiberl et al., 2019), crowdworking (Mrass and Peters, 2019), information exchange in health care (Johnsen et al., 2016), transitions from product-centric to customer-centric services (Marjanovic and Murthy, 2016), and alternative views of digitalization (Wolf et al., 2019). It also has formed the basis of WST extensions such as a theory of workarounds (Alter 2014) that has been applied to research related to information security (Jeon et al., 2018)

A brief summary of WST introduces ideas that will be used to explain more about what the empirical findings mean in relation to both the operation of work systems and the iterative process by which work systems evolve over time.

Work system. A work system is a system in which human participants and/or machines perform work (processes and activities) using information, technology, and other resources to produce specific product/services for specific internal and/or external customers (Alter, 2013). Most significant work systems use IT extensively and can be described as IT-reliant. SMEs and other enterprises that grow beyond a largely improvised start-up phase can be viewed as operating based on the internal activities and interactions of multiple work systems. For example, typical SMEs contain work systems that procure materials from suppliers, produce product/services, deliver product/services, find customers, create financial reports, hire employees, coordinate work across departments, and perform many other functions. The definition of work system includes the phrase "human participants and/or machines perform work" because work systems may be sociotechnical systems with human participants or may be totally automated.

Work system theory. A complete understanding of a work system needs to include both a static view of a work system during a period when it is relatively stable and a dynamic view of how a work system changes over time. WST (Alter 2013) distils the core of that understanding into three components, the definition of work system (above) and two frameworks. The work system framework (Figure 1) is a pictorial representation of a work system in terms of nine elements included in a basic understanding of its form, function, and environment during a period when it is relatively stable. A work system's identity remains unchanged during such periods of stability even though incremental changes such as minor personnel substitutions or technology upgrades may occur within what is still considered the same version of the same work system. The work system life cycle (WSLC) model (Figure 2) is a pictorial representation of the iterative process by which work systems evolve over time through a combination of planned change (formal projects) and unplanned change that occurs through adaptations and workarounds (see Alter, 2014).

Tables 1 and 2 show that the elements of the work system framework and the phases of the WSLC have many direct implications related to information security.

Work system framework. Figure 1 outlines elements of even a rudimentary understanding a work system's form, function, and environment. Figure 1 places the customer on top because work systems exist for the purpose producing product/services for customers. This leads to inherent trade-offs between internal management concerns about performing the work efficiently, maintaining participant morale, and minimizing vulnerability to threats, versus customer concerns about the total cost, quality, and other characteristics of the product/services that they receive. Notice how this system view of work implies that time and effort devoted to information security could be time and effort taken away from serving customers.

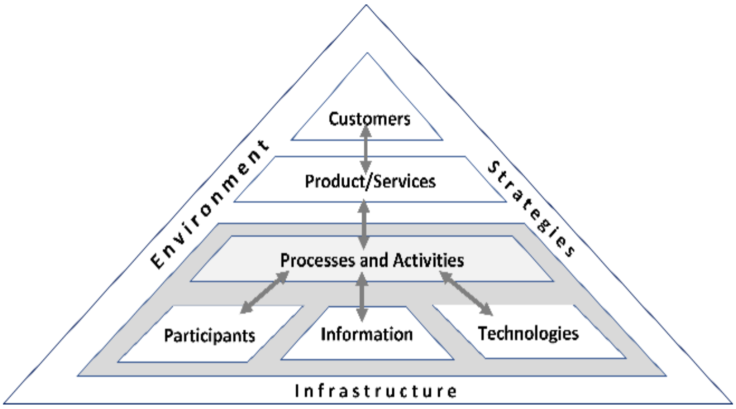
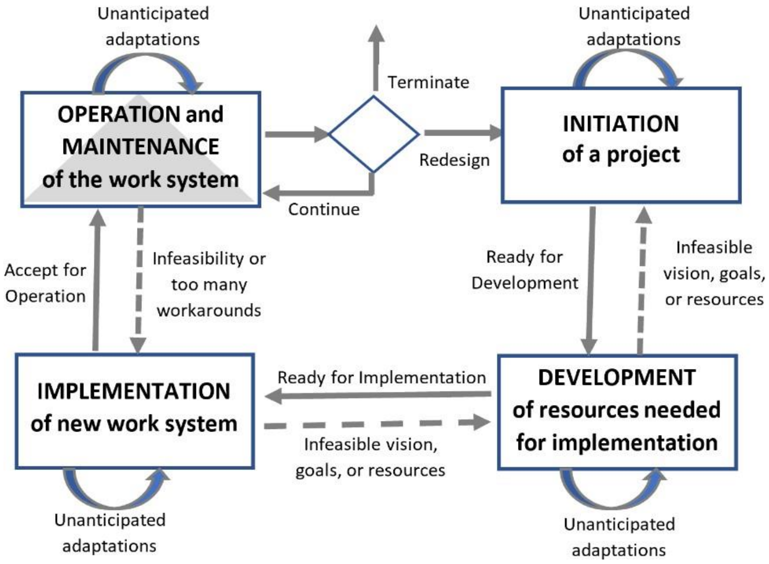


Figure 1. Work System Framework (Alter, 2006, 2013)

Work system life cycle model. Work systems are assumed to evolve over time through a combination of planned change and unplanned (emergent) change. Those changes involve not only changes in hardware and software, but also changes in all other components of a work system. The WSLC (Figure 2) represents planned change as projects that include initiation, development, and implementation phases. Initiation is the chartering of a project whose goal is to create or improve a work system. Development involves creation or acquisition of resources required for implementation of desired changes in the organization. In the WSLC implementation of a sociotechnical work system refers to implementation in the organization, not implementation of algorithms on computers. A full iteration from one operation and maintenance phase to the next operation and maintenance phase might be viewed as a transition from a previous version of the work system to a subsequent version. Figure 2 represents unplanned change in the WSLC using inward-facing arrows that represent ongoing adaptations, bricolage, and workarounds that change aspects of the current work system without separate allocation of significant project resources.

The WSLC is not meant as a rigorous specification of a precise process by which work systems evolve over time. Instead, it summarizes how work systems evolve over time in an iterative manner, noting that planned and unplanned changes are part of the story, that planned change occurs through projects to which resources are assigned, and that unplanned change may occur in a variety of ways.



Unanticipated adaptations
OPERATION and MAINTENANCE of the work system
Terminate
Redesign
Continue
Unanticipated adaptations
INITIATION of a project
Accept for Operation
Infeasibility or too many workarounds
Ready for Development
Infeasible vision, goals, or resources
IMPLEMENTATION of new work system
Ready for Implementation
Infeasible vision, goals, or resources
DEVELOPMENT of resources needed for implementation
Unanticipated adaptations
Unanticipated adaptations

Figure 2. The Work System Life Cycle Model

3.1 Implications of the work system framework for information security practices

Each of the nine elements of the work system framework (Figure 1) can be a locus or source of an information vulnerability for almost any significant work system, including work systems that might focus on design, sales, manufacturing, HR, finance, and so on. Table 1 shows several typical information security guidelines related to each of the nine elements. Each of the guidelines can be restated as a question that can be raised during the analysis and design of information systems and the work systems that they support (see typical questions in Alter, 2017). The guidelines themselves do not seem remarkable and could be improved in various ways. The point here is not their uniqueness, but rather that the elements provide an organized way to identify and visualize frequently important issues related to information security in the context of work systems through which SMEs and other enterprises operate. Comparison between these guidelines and the empirical results reported in Figures 3, 4, and 5 illuminates a key generalization: many SMEs do not follow these straightforward guidelines and may not be aware of them or similar guidelines.

Element of the work system framework	Typical information security guidelines
Customers	• Significant information that is transferred to or accessed by customers should be protected from inappropriate use by customers or by anyone associated with customers, such as their employees, contractors, customers, and suppliers. • Information about customers should be checked for accuracy and protected from inappropriate use.
Product/services	• Informational product/services should be designed and produced in ways that minimize vulnerability to error or misuse. • Incentives for misstating or otherwise corrupting information included in a work system's product/services should be identified and minimized.
Processes and activities	• Security/ vulnerability – related weaknesses in a work system's processes and activities should be identified and minimized. • Processes and activities should operate in a way that encourages consistency with corporate information security policies. • Processes and activities should be monitored to identify practices that ignore or contradict established security guidelines or are risky in other ways. • Processes and activities should be designed in a way that does not force work system participants to choose between meeting performance goals and conforming with information security guidelines. • Workarounds and other shortcuts that increase security vulnerabilities should be identified and minimized.
Participants	• Work system participants should be fully aware of information security guidelines and the vulnerabilities that result when those guidelines are not followed. • They should receive training or other clear communication that helps them appreciate the negative impacts of security incidents. • Incentives for work system participants should be aligned with requirements for information security and should not encourage participants to ignore or work around those guidelines.
Information	• Sensitive information should be identified. • Information protection should be aligned with the sensitivity of specific information. • Information security mechanisms should not be so onerous and time-consuming that they invite workarounds.
Technologies	• Technologies in a work system should be protected from IS security risks related to intrusion, theft, sabotage, or other issues that conflict with information security. • Technologies should be monitored to identify non-standard operation, non-standard usage, and other conditions that could compromise information security
Environment	• The existence of enterprise policies related to information security does not imply that those policies will be followed or even that those policies will be known by many work system participants.

	• The relevant environment should be monitored for information security threats.
Infrastructure	• Shared technical and informational infrastructure may bring vulnerabilities related to information security. • Enterprise infrastructure should be monitored to identify possible sources of security risk. Infrastructure and infrastructure usage should be designed to minimize such risks.
Strategies	• Work systems should have appropriate strategies related to information security. • Any inconsistencies between a work system's security strategy and enterprise guidelines related to information security should be examined for related benefits and problems.

Table 1. Typical Security Guidelines Related to Elements of the Work System Framework

3.2 Implications of the work system life cycle model for information security practices

Table 2 identifies typical information security guidelines related to the three planned change phases of the WSLC (Figure 2), initiation, development, and implementation. The operation and maintenance phase of the WSLC is covered by Table 1, which presents information security guidelines for the various elements of the work system framework. As with the guidelines in Table 1, each of the guidelines in Table 2 can be restated as a question that can be raised during the analysis and design of information systems and the work systems that they support. As with Table 1, the point here is not about the uniqueness of the ideas related to the phases, but rather that the phases provide an organized way to identify and visualize frequently important issues.

Phase of the WSLC	**Typical information security guidelines**
Initiation	• Information security should be considered in the initiation phase for any work system project that touches sensitive information. • Where information is sensitive, information security requirements should be mentioned in specification documents, user stories, or other indications of the project's scope or goals. • Resources should be allocated for security-related features, activities, and training.
Development	• Development projects that create or update software should devote appropriate attention to information security, even in projects that apply agile methods. • Appropriate attention to information security should be explicit in outputs of the development phase including new or updated software, documentation and training materials.
Implementation	• The implementation phase should devote sufficient time and energy to information security in the new or improved work system.

	- The implementation process should assure that work system participants fully appreciate foreseeable security vulnerabilities and the types of actions and attitudes needed to minimize those vulnerabilities. For example, they should understand expectations related to transferring data to personal devices, using passwords or other authentication schemes, and logging off when sessions end.
Operation and Maintenace	This phase is covered in Table 1, which identifies typical information security guidelines for work systems in operation.

Table 2. Typical Security Guidelines Related to Phases of the Work System Life Cycle Model

4. Empirical study of information security in SMEs

The empirical study involved 187 employees from 39 SMEs situated in the region of Hampshire in the UK. The research was carried out by 39 trainee business analysts (research students) involved in a business analysis project and the lead investigator (a senior academic) was one of the authors of this paper. Each trainee selected the company they collaborated with. Those companies were drawn from a variety of sectors, including manufacturing industry, services and retail. Company size varied from 5 to 250 employees. In each SME, the analyst held approximately ten (or more) semi-structured individual interviews over a period of six months. Interviews took around half an hour and had a specified theme and focus. One of the interview sessions was used for a walk-through of the information security questionnaire which was used to support the interviews. The main objective of our exploration was to assess security practices from employees' point of view and not just as described in formal security documentation. This approach led to a better appreciation and understanding of issues and gaps in security practices. The questionnaire was divided into five sections based partly on the SME questionnaire and guidelines within the Government's National Cyber Security Programme. It also covered additional topics related to human and organizational factors in information security management. The questionnaire also included questions that could be answered by professional employees who might or might not have an IT background. The first three parts of the questionnaire focused on planning, implementation, and review of information security. The fourth part focused on information security management. The fifth dealt with the contribution of employees to information security management activities. The latter section of the questionnaire is of particular interest for this paper's goals as it investigates the extent to which companies integrate information

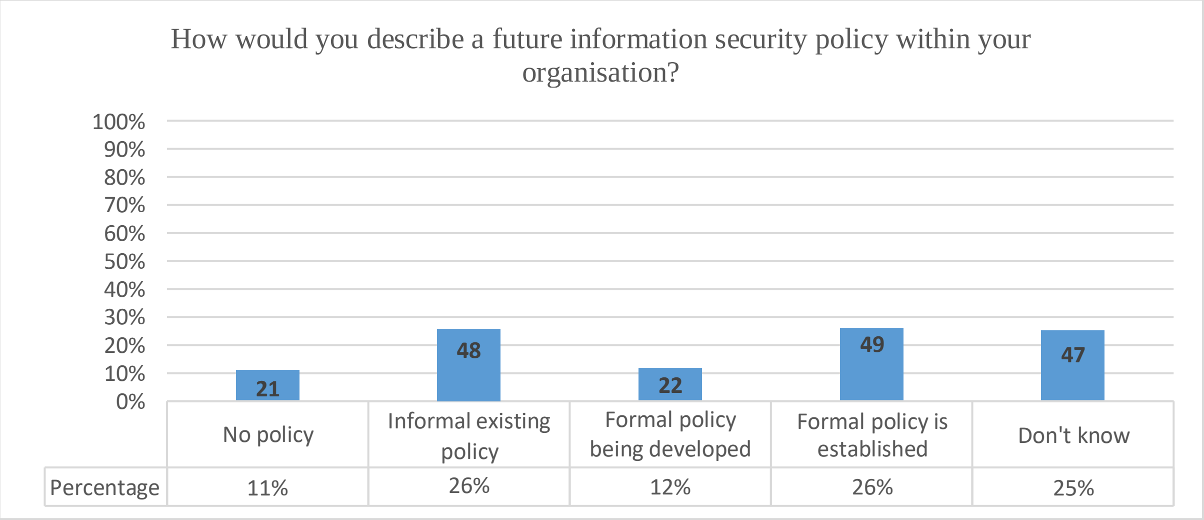
security activities in every day working routines. This is explored through employees' perceptions of the extent to which that integration exists.
The interviewees were all employees who, according to their own description, handle sensitive data, and therefore should take security considerations into account while doing their jobs. The study took place over a six-month period between September 2017 and March 2018. In most companies, three to five employees were interviewed. Most of the questions were closed-ended but a few included an opportunity for interviewees to provide further explanation. All the questions were discussed during the interviews.

The resulting data was analysed by the authors of this paper, which draws mainly on the outcome and discussions of closed-ended questions related to the following topics: a) awareness of security policy; b) information security practices and management and c) information security involvement. The guidelines from Section 3 based on the work system framework and WSLC provide a perspective about what we should have found if the SMEs took information security seriously. Unfortunately, those guidelines point to many aspects of information security awareness and practices that were missing in many of the SMEs.

This study was part of a larger ongoing academic research project which started more than ten years ago. The main project is a an action research project that tries to help SMEs develop a better understanding of their work systems and their potential for change. All participating organizations gave their written consent (in a specific contract of agreement) before the analysis of the interview data began. Additionally, all participating employees each gave separate consent in writing during individual face to face meetings before any further discussions took place. Each individual organization received a full (anonymized) report of the analysis for their particular organization. Each part of the analysis and dataset was validated during the inquiry process. The validation involved collaboration between researchers and interviewees in reviewing all documents, discussions, and models related to a company's information security training, expectations, and practices. Documents discussed with company employees were revised based on those reviews.

4.1 Awareness of security policy

We were surprised to find that that almost half (48%) of the interviewees were not aware of existing security controls and that a quarter of the respondents did not know or apply a formal security policy. As shown in Figure 3, 11% said they did not follow any security policy guidelines and 26% reported that any existing security policy was informal. Only 38% of the interviewees who responded to this question reported that a formal security policy had been established or was being developed. This result illustrates the difference between awareness of security policies and the possible existence of security policies. Even in cases where employees were not aware of the policies, it is possible that their employers had defined security policies or had implemented security controls. A related study by Balozian and Leidner (2016) recommends that security professionals need to make an extra effort to justify the relevance of a security policy from a practitioner's point of view.



	No policy	Informal existing policy	Formal policy being developed	Formal policy is established	Don't know
Percentage	11%	26%	12%	26%	25%

Figure 3: Awareness of security policies

4.2 Information security practices and management

As shown in Figure 4, a significant number of interviewees recommend that a clearly identified individual should be the responsible for information and cyber security. In addition, 45% of the respondents suggested that a permanent incident security response team was needed and 48% thought that it is necessary to clarify responsibility for data ownership and protection within their companies. These findings demonstrate a real need within the SMEs to improve their reporting mechanisms related to security risks in order to identify early signs of risks and to respond to them more effectively. Figure 4 also shows that 51% of the respondents reported that their companies are not reviewing or testing the effectiveness of security controls and 22% are not aware of any update of such controls. This is an alarming result given the dynamic nature of security risks and the necessity of developing proactive approaches to information security.

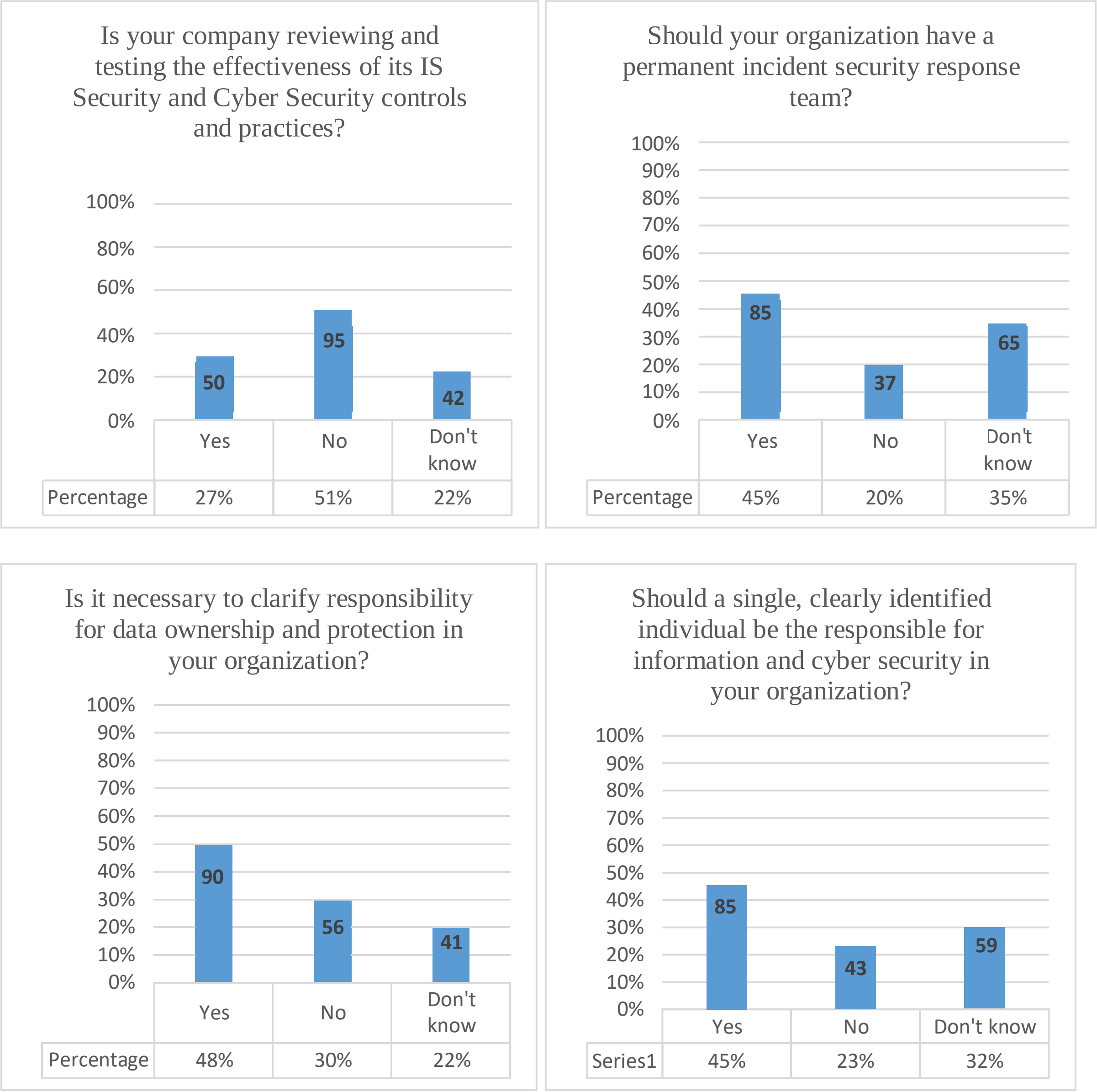


Figure 4: Results related to information security management practices

4.3 Information security involvement

The interview results indicated a clear gap between security requirements and security practices. Figure 5 shows that more than 80% of the interviewees do not participate in developing specific security requirements as a part of their jobs. Instead, security controls are imposed top-down.

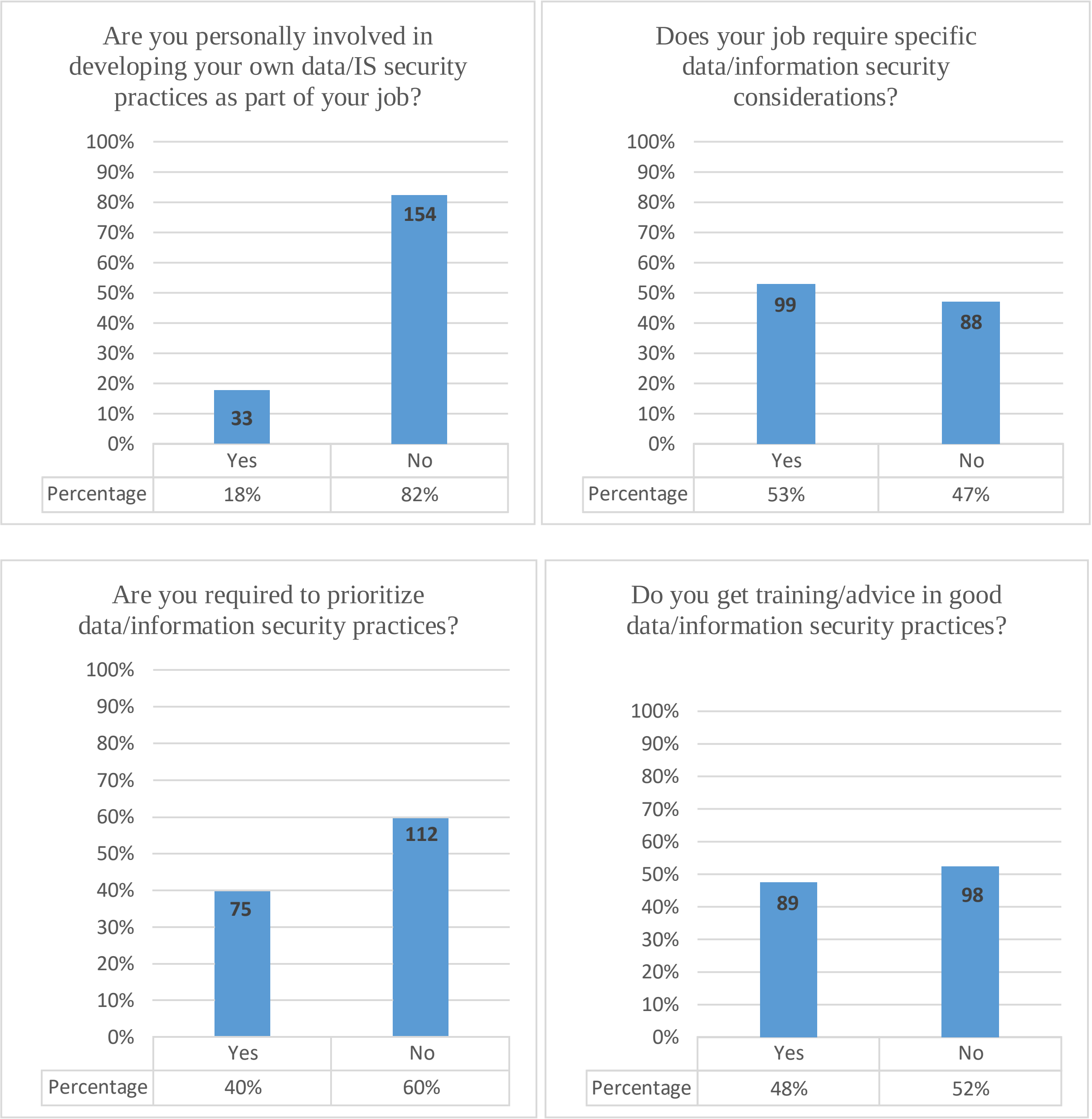


Figure 5: Information security involvement

Another interesting finding is the discrepancy between information security considerations as a requirement of the job and information security as a priority for doing the job. While all the interviewees handle sensitive data to do their job 53% said their job does not require careful attention to data security. Interestingly, 60% of the interviewed employees stated that information security is not prioritised when doing their job. With regards to staff training, 52% of survey respondents said they did not get any training or advice in good information security practices. That finding is consistent with the work system framework's implication that work system participants typically give much higher priority to performing their assigned tasks within the work system than to following information security guidelines.

These results indicate serious deficiencies in the security practices of the SMEs in our sample. While security practices vary by industry and company size, we believe our sample was broad enough to be representative of SMEs in the UK. Our clear conclusion is that most SMEs face challenges related to the integration of security function into work processes and in many cases may not be aware of the extent and significance of those challenges. Despite of political initiatives to support SMEs preparedness, the observed gaps in SMEs security practices illustrate their weak understanding of how to implement and manage effective security controls and measures. Our findings also support the conclusion that security practices must be influenced by those employees who are affected by the deployment of security controls in their own work practices. If decisions on security practices remain solely within the domain of security experts, we should expect that those decisions will not be integrated well with everyday work practices and in some cases will simply prove unworkable.

5. Conclusion

Our exploratory research study reveals that security practices of many SMEs do not go far enough in recognising the importance of effective information security management. Even when security is considered important in an SME, it may not receive high priority in the context of everyday work practices. While all of the interviewed employees handle and use sensitive data to do their jobs, a vast majority are not involved in risk assessment or in the development of security practices. Security practices are not prioritised and remain an illusory activity in their real world working contexts. Our empirical study indicates that actual work practices and routines of most employees were often ignored in the development and operation of security management efforts. Moreover, security processes that are designed outside of the real world organizational context are prone to undermine effective organizational practices and to create unintended consequences in the operation of work systems. These key findings are consistent with previous literature discussed in the second section.

One of the main limitations of this study is its reliance on closed-ended questions. In future research, we hope to expand upon the questions explored here. We hope to embark on a series of in-depth interviews with selected respondents in order to obtain a richer understanding of their security practices. A further analysis of collected data according to company size or activity sector is also desirable.

The empirical results show that many SMEs do not follow typical information security guidelines such as those shown in Tables 1 and 2. Those guidelines are organized around the central ideas in WST. The direct relevance of those guidelines to our empirical findings implies that a work system perspective might provide a coherent container for describing, analysing, and evaluating situations related to IS security and for studying IS security as a research endeavour (Alter, 2017).

The challenge of introducing security in an effective and useful manner can be addressed by considering the nine elements within the work system framework in order to streamline risk management processes, involve relevant stakeholders in operational security risks mitigation and set up well-targeted security awareness and training programmes. This means that information security should not be seen as an add-on, but rather should be integrated into work system design efforts and into changes in work practices. We found major disconnects between straightforward guidelines about information security (Section 3) and actual security related practices (Section 4). Providing guidelines couched in a work system perspective could be a practical way to explain that security needs to be taken more seriously. At minimum, SME managers and workers should recognize that security guidelines need to be linked to local security practices if they are to help in mitigating security risks.

2. References

Adams A, Sasse A. (1999) “Users are not the enemy” Communications of ACM; 42:41–6. doi:10.1145/322796.322806.

Albrechtsen, E. (2007), “A qualitative study of users’ view on information security”, *Computers & Security*, Vol. 26, pp 276-289.

Albrechtsen, E. and Hovden, J. (2010), “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study”, *Computers & Security*, Vol. 29, pp 432-445.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. Computers & Security, 28(6), 476-490.

Alter, S. (2006). *The work system method: connecting people, processes, and IT for business results*. Work System Method. Work System Press.

Alter, S. (2013). Work system theory: overview of core concepts, extensions, and challenges for the future. *Journal of the Association for Information Systems*, *14*(2), 72-121.

Alter, S. (2014). Theory of Workarounds. *Communications of the Association for Information Systems*, 34 (55), 1041-1066

Alter, S. (2017). Six Work System Lenses for Describing, Analyzing, or Evaluating Important Aspects of IS Security. *International Journal of Systems and Society (IJSS)*, *4*(2), 69-82.

Ashenden D. and Sasse A. (2013). "CISOs and organisational culture: Their own worst enemy?" Computers & Security, 39, 396-405.

Balozian P. and Leidner D., (2016), "IS Security Menace: When Security Creates Insecurity", Proceedings of Thirty Seventh International Conference on Information Systems, Dublin.

Baskerville, R. (1991) Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems, 1, 121–130.

Bednar, P. and Katos, V. (2009), "Addressing The Human Factor In Information Systems Security", MCIS 2009 Proceedings, Athens, Greece, 25-27 September, Paper 72.

Berniker, E. (2016). "The Future of Sociotechnical Systems Theory and Practice: The Challenges for Information System Design," *International Journal of Systems and Society*, vol. 3, no. 1, 2016.

Bostrom and Heinen, J. S. (1977). MIS problems and failures: a socio-technical perspective, part II: the application of socio-technical theory. *MIS Quarterly*, 1(3), 11-28.

Caputo, D.D., Pfleeger, S.L., Sasse, A., Ammann, P., Offutt, J., Deng, L.: Barriers to usable security? Three organizational case studies. IEEE Secur. Priv. 14(5), 22–32 (2016)
Cybersecurity breaches survey 2018 retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Coles-Kemp L. (2009) "Information security management: An entangled research challenge" Information Security technical report, 14, 181-185.

Coles-Kemp L. and Hansen R. (2017) "Walking the Line: The Everyday Security Ties that Bind" HAS 2017, LNCS 10292, pp. 464–480.

Daiberl, C. F., Oks, S. J., Roth, A., Möslein, K. M., and Alter, S. 2019. "Design principles for establishing a multi-sided open innovation platform: lessons learned from an action research study in the medical technology industry," Electronic Markets (21:4), p. 335.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Impacts of security climate on employees' sharing of security advice and troubleshooting: Empirical networks. Business Horizons, 59(6), 571-584. doi:10.1016/j.bushor.2016.07.003

Dhillon G., Oliveira T., Susarapu S., Caldeira M. (2016) Deciding between information security and usability: Developing value based objectives *Computers in Human Behavior*, 61, 656-666.

Dhillon, G. and Torkzadeh, G. (2006) "Value-focused assessment of information system security in organizations", *Information Systems Journal*, Vol. 16, pp 293-314.

Dimopoulos V., Furnell1 S., Jennex M. and Kritharas I. (2004) "Approaches to IT Security in Small and Medium Enterprises", Proceedings of the 2nd Australian Information Security Management Conference, Securing the Future, Perth, Western Australia.

Furnell S. (2016) "The usability of security – revisited", *Computer Fraud & Security*, September, 5-11.

Home Office (2017) Business population estimates 2017 Retrieved from https://www.gov.uk/government/statistics/business-population-estimates-2017

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. Business Horizons, 59(6), 585-591.

Jeon, S., Hovav, A., Han, J., & Alter, S. (2018). Rethinking the Prevailing Security Paradigm: Can User Empowerment with Traceability Reduce the Rate of Security Policy Circumvention?. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 49(3), 54-77.

Johnsen, H. M., Fruhling, A., and Fossum, M. 2016. "An Analysis Of The Work System Framework For Examining Information Exchange In A Healthcare Setting," Communications of the Association for Information Systems (39), pp. 73–95.

Karlsson F., Karin Hedström K. and Göran Goldkuhl G. (2017) " Practice-based discourse analysis of information security policies", Computers & Security, 67, 267–279

Kowalski, S., Bednar, P., Nolte, A. and Bider, I. (2019). *Proceedings of the 5th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2019), CEUR Workshop Proceeding*. Available: http://ceur-ws.org/Vol-2398/

Kolkowska, E., and Dhillon, G. (2013), "Organizational power and information security rule compliance", *Computers & Security*, Vol. 33, pp. 3-11.

Koppel, R., Smith, S., Blythe, J. and Kothari, V. (2015), "Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?", *Studies in Health Technology and Informatics*, Vol. 280, pp. 251-220.

Marjanovic, O., and Murthy, V. (2016) "From product-centric to customer-centric services in a financial institution –exploring the organizational challenges of the transition process," Information Systems Frontiers (18:3), pp.479–497.

Mühe S. and Drechsler A. (2017) "Towards a framework to improve IT security and IT risk management in Small and Medium Enterprises" International Journal of Systems and Society, 4(2), 44-56.

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, *16*(4), 317-342.

Myers MD. And Klein HK. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly* 35(1), 17-36.

Parsons K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", Computers & Security, Vol. 42, pp 165-176.

Renaud K. (2016) How smaller businesses struggle with security advice *Computer Fraud & Security*, August, 10-18.

Sarker, S., Chatterjee, S., Xiao, X. and Elbanna, A. (2019). “The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and its Continued Relevance,” *MIS Quarterly*, vol. 43, no. 3, pp. 695–719. Available: https://doi.org/10.25300/MISQ/2019/13747

Sasse A. and Smith M. (2016) “The security-usability tradeoff myth”, IEEE Security & Privacy September/October.

Shedden P., Scheepers R., Smith W., Ahmad A. (2011), “Incorporating a knowledge perspective into security risk assessments”, *VINE Journal Information Knowledge Management System*, Vol. 41, No. 2, pp 152-166.

Sinha, K. K., & Van de Ven, A. H. (2005). Designing work within and between organizations. *Organization Science*, *16*(4), 389-408.

Siponen, M. (2005) “Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods”, Information and Organization (15), pp. 339-375.

Siponen, M. and Willison, R. (2009), “Information security management standards: Problems and solutions”, *Information & Management*, Vol. 46, pp. 267-270.

Sommerville, I. (2011), *Software engineering*, Pearson Education Inc, ISBN: 978-0-13-705346-9.

Spears, J. L. and Barki, H. (2010) “User participation in information systems security risk management”, *MIS Quarterly*, Vol. 34, No. 3, pp 503-522.

Spears, J. L. and Barki, H. (2010), “User participation in information systems security risk management”, *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

Stahl, B. C., Doherty, N. F. and Shaw, M. (2012), “Information security policies in the UK healthcare sector: a critical evaluation”, *Information Systems Journal*, Vol. 22, pp. 77-94.

Trist, E. (1981). The evolution of socio-technical systems. *Occasional paper 2*, June, 1981.

Truex, D., Alter, S., and Long 2010. “Systems Analysis for Everyone Else: Empowering Business Professionals through a Systems Analysis Method that fits their needs,” in European Conference of Information Systems 2010, Pretoria, South Africa.

Truex, D., Lakew, N., Alter, S., and Sarkar, S. 2012. “Extending a Systems Analysis Method for Business Professionals,” in Practical aspects of design science: European Design Science Symposium, EDSS 2011, Leixlip,

Tryfonas, T., Kiountouzis, E., Polymenakou, A. 2001. Embedding security practices in contemporary
V. C. Wolf, C. Bartelheimer, and D. Beverungen, “Digitalization of Work Systems—An Organizational Routines’ Perspective.” HICSS 2019

Woltjer, R. (2017) "Workarounds and trade-offs in information security – an exploratory
Sasse A. and Smith M. (2016) “The security-usability tradeoff myth”, IEEE Security & Privacy September/October.

Wong, H. M. L. (2018). Demystifying and Solving the Knowledge Sharing Problems in a Regional Operations Division of a Global Courier and Delivery Services Firm: An Action Research Approach. PhD thesis, City University Hong Kong.