Information security: listening to the perspective of organisational insiders

Abstract

Aligned with the strategy-as-practice research tradition, this paper investigates how organisational insiders understand and perceive their surrounding information security practices, how they interpret them, and how they turn such interpretations into strategic actions. The study takes a qualitative case study approach, and participants are employees at the Research & Development department of a multinational original brand manufacturer. The paper makes an important contribution to organisational information security management. It addresses the behaviour of organisational insiders – a group whose role in the prevention, response and mitigation of information security incidents is critical. The paper identifies a set of organisational insiders' perceived components of effective information security practices (organisational mission statement; common understanding of information security; awareness of threats; knowledge of information security incidents, routines and policy; relationships between employees; circulation of stories; role of punishment provisions; and training), based on which more successful information security strategies can be developed.

Keywords

Information security; organisational insiders; information security awareness; strategy as practice

1. Introduction

With the rapid advancement of computer-based information systems and the occurrence of security-related incidents (e.g. acts of human error negligence, deliberate software attacks, software failures, espionage, deliberate acts of trespass, sabotage), information security

management has become an unavoidable aspect of contemporary organisations' operations [1, 2, 3]. Organisations are aware of the threats to information systems security, in particular cyber attacks [4] and the infringement of confidential data [5]. Previous research has significantly focused on the technical controls of information security [6, 7] and it is often argued that early information systems security studies approach perceptions of security from a technology acceptance angle [8]. However, experts growingly argue that the main cause for information security incidents lies mainly with employees' behavioural factors rather than technical issues per se, which implies a turn to internal problems attributed to the users of information systems [9, 10]. In more recent research, practitioners have studied information security management focusing on insiders' security behaviour and attitudes in the context of organisational culture [11, 12].

This paper is located within this emergent stream of research in that it is concerned with the perceptions of information security practices held by ordinary organisational insiders (i.e. full-time employees, part-time employees and temporary workers) who have access to both an organisation's critical operational information and its information systems. Moreover, the paper attempts to introduce contextual innovation by investigating the perceptions of employees within the R&D department of a multinational original brand manufacturer (OBM), henceforth referred to as Textile α (disguised name). This is particularly important as R&D departments are at the core of firms' knowledge flows [13], firms' ability to generate product innovation [14], and firms' capacity to increase value added [15]. Incidents with organisational insiders who disclose sensitive information [16] are challenging for R&D departments, with severe impacts on productivity, revenue, and reputation. Equally challenging are the emergent managerial problems associated to the increased adoption of boundary spanning organisational practices and technologies that emphasise information sharing, networking and mobility [17].

Security is not employed in this study in connection with legal protection mechanisms such as IPR mechanisms and related contractual issues [18] and focuses instead on the processes of securing organisational information integrity and confidentiality [19] yet ensuring it is available to relevant organisational actors when needed. Typically information security deals with a variety of solutions that prepare against and/ or respond to threats to information such as information leaks to competitors and knowledge loss through staff turnover [20]. Such threats inform the design of formal and informal protection measures that share as a common starting point the clear identification of critical information assets [21]. The appropriate recognition of which information sustains business value creation is a specific managerial capability and requires an articulation of the role of information in the business, combined with the specification of practices that deal with how that information should be secured [22].

In order to address the theoretical and practical issues identified in the problem statement introduced above, this paper aims to extend information security theory by exploring organisational insiders' perceived components of effective information security practices. The focus is therefore on the make-up of effective information security practices from the employee's point of view, elicited through the overall question of 'what do organisational insiders want and why?' Such an investigation of how organisational insiders understand and perceive their surrounding information security practices, how they interpret them, and how they turn these interpretations into strategic actions corresponds to what Vaara and Whittinghton [23] describe as uncovering the taken for granted practices that shape strategy work. This endeavour is aligned with the strategy-as-practice research tradition, and its focus on the ways in which organisational actors' decisions and actions are enabled by organisational and social practices.

A practice approach to the study information security in organisations is particularly timely and responds to calls for the examination of the micro-practices and everyday routines of

strategy formation [24]. These micro-practices and daily routines that are the locus of strategy formation comprehend a variety of interconnected elements – cognitive activities, know how, emotional states, motivational knowledge, constitution of symbolic constructs such as organisational procedures [25, 26, 27], which are often absent from the dominant strands of information security research that rely essentially on the adaptation of perspectives borrowed from reference disciplines (e.g. economics, psychology, criminology) and tend to replicate extant theories (e.g. deterrence theory, theory of planned behaviour, protection motivation theory). On the other hand, from a practice perspective, organisational phenomena such as information security strategy are understood not as immanent properties, but as doings and social practices in which individuals actively engage. There is therefore a substantial affinity between the practice perspective and the Weickian tradition of examining the processes of organising, making sense, and enacting reality [28].

In terms of structure, following the presentation of the research area and proposed practice approach in the current section, the following section offers a theoretically sensitising review of the literature [29] on information security (with a focus on purpose, policy and culture). Section 3 introduces the empirical context of the study and describes the methodology. Section 4 presents the results in a narrative that illustrates the themes identified through inductive thematic analysis with the voice of organisational insiders – conveyed in the form of interview excerpts. Finally, a discussion of findings is provided in Section 5, while Section 6 presents conclusions.

2. Information security

The mitigation of security threats towards information assets attributable to both outsiders and insiders has become an important area of organisational strategy [17, 30, 31, 32, 33].

Organisations increasingly focus on implementing information security products such as anti-virus, intrusion detection and prevention systems, total PC security, database/contents security, total security systems and public key infrastructure [6, 7]. However, alongside technical measures, information security requires a strategy that orchestrates structured actions, policy and governance in order to protect organisational information assets [34]. Indeed, despite the prevalence of technical security [32] measures, studies have reported that internal security incidents continue to happen and create more damage and losses than security incidents caused by outsiders [35, 36]. Recent research goes as far as reporting that approximately half of all information security violations can be attributed to the behaviour of organisational insiders [37]. Such results demonstrate the relevance of focusing on the user behavioural dimensions and on the socio-organisational aspects of information security resilience.

Abundant research has focused on users' information behaviour in organisational settings, usually under names such as misuse, compliance or violation of information systems security policies. However, from a theoretical perspective, previous information security research has been relatively poor in theory development, and has mostly borrowed constructs that were originally developed for other disciplines, (e.g. economics, criminology, psychology) such as rational choice theory [38, 39, 40], deterrence theory [41, 42], protection motivation theory [43], neutralization theory [44], or theory of planned behaviour [45]. This development in the literature goes hand in hand with organisations' concerns about security incidents and how they can have negative effects on their competitiveness. More than targeting system or application vulnerabilities, a growing number of security intrusions now tend to focus on and exploit vulnerabilities in the behaviour of organisational insiders [46]. Recent research has focused on information security incidents which can be attributed to human factors such as malicious intention, negligence, a lack of knowledge and communication, and flawed information security policy [9, 47, 48, 49].

Information security has evolved together with the rapid changes of technology and society. The technological and societal developments have impelled many organisations to the development of information security management. The International Standard on Information Security (ISO 27000) defines information security in the business context, as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities" [50]. The ISO 27000 series provides organisations with standards for information security management. Within the series, the ISO 27002 standard provides recommendations on the management of information risks through information security controls, including clauses that address specifically the social aspects of information security management (e.g. clause 6 on 'Organization of Information Security' addresses the need to allocate clearly defined roles and responsibilities for information security management processes and activities; clause 7 on 'Human Resource Security' focuses on employees' and contractors' awareness and fulfilment of their information security responsibilities; clause 8 on 'Asset Management' addresses the need to identify organisational assets and define protection responsibilities; clause 9 on 'Access Control' focuses on limiting access to information and information processing facilities to protect against accidental damage, loss and other threats). [51]

In many studies, organisational information has been conceptualised as a fundamental asset and therefore researchers have made consistent effort in assuring information security to protect organisations' interests and minimise risks to information assets [9, 10].

In addition, information security can be viewed as the process involved in keeping information secure. This is through offering protection to its privacy, integrity and availability and through managing with responsibility, integrity, trust and ethicality (RITE) principles for successfully securing the information assets within organisations [9]. For information security to be effective, it should involve technology, security products, procedures and policies. There

is no single collection of products that can address every issue pertaining to information security [52]. Various products are currently in place aimed at addressing issues related with information security. Such products include vulnerability scanners, firewalls and intrusion detection systems. However, it is important to note that such products alone cannot adequately address information security challenges [53].

Information security in its basic form is more of a process. The initial step in information security is the development of an information systems security policy. An information systems security policy refers to a set of guidelines that are well-defined and documented, which provide a description of the ways in which any organisation manages, offers protection to its information assets and plans future decisions concerning the security of its information systems infrastructure [9, 54]. A document describing security procedures outlines precisely how to go about accomplishing specific tasks [55] and how to protect information systems from rising levels of security threats [56]. Moreover, information security policies give employees guidelines on the acceptable use of computer resources alongside with a determination of penalties that can result from non-adherence to those guidelines [57].

In historical terms, there are many ways of describing the development of information security over the past decades. One of the ways of mapping this development is by analysing the waves that signify specific trends. These waves consist of the technical wave, the management wave, the institutionalisation wave, the governance wave, and the cyber security wave. The first wave, signifying a technical approach to information security, is based on the main frame. It considers information security as something that could easily be addressed by use of the features that are inbuilt into the mainframe operating system such as passwords, user-ids and access control lists. The second wave, management approach, attracted the involvement of top management with the emergence of distributed computing. This wave of information security brought about information security policies and also the organisational

structures addressing information security. The outcome of this wave was that it succeeded in gaining the attention of managers and therefore contributed to an overall improvement of organisational information security. The third wave, institutionalisation approach, introduced major improvements in information security. This wave is made up of different components, which include "information security standardization", "international certification of information security" and "cultivating security culture of information throughout an organisation" [58]. The fourth wave refers to the processes leading to the explicit inclusion of information security as a core component of good corporate governance. Finally, the fifth wave refers to the professionalisation of information security practitioners as a fundamental step in the protection against threats raised by Internet-based systems [59].

The standardisation of information security involves adhering to internationally recognised standards for information security. International information security certification addresses the question of how to go about proving information security readiness to an electronic business partner. Processes of information security compliance assist organisations in carrying out comparisons between their real information security operations and international information security management standards. The purpose of compliance is to evaluate and carry out audits on de facto organisational practices vis a vis the standards [60]. Assessing the degree of compliance assists organisations in determining their adherence to the controls defined in the standards. Compliance with standards that are internationally recognised is a common basis for measuring information security. It is therefore vital for organisations to regularly evaluate their information security levels against internationally recognised standards [12].

Finally, cultivating an information security culture addresses the security challenges that emerge mainly from the behaviour of organisational insiders. Security culture is vital to an organisation as employees may pose threats to information security [58]. Therefore, a balance

of people, process and technology is required to improve organisations' information security [61].

2.1. Information security culture

Culture can be conceptualised as a set of common understandings that are expressed in shared patterns of action and meaning, such as a common language. In context of information security, culture is vital and research has established that it has an impact on information security outcomes [47, 62]. Furthermore, through understanding and encouraging a security culture in organisations where the integrity of information as an asset is a vital factor for success can help maintain and enhance their reputation [63].

Culture has influenced the creation of numerous security instruments such as information ethics guidelines, national security policy, and security training [64]. The scope of security culture includes ethical and social dimensions that are meant to enhance the security-related conduct of employees. Information security culture, as a subset of the overall culture of an organisation, should offer support to all organisational tasks in such a manner that information security becomes a normal aspect of employees' daily workplace routines [65]. This contribution is particularly relevant when considering that employees' limited knowledge of information security challenges can lead to vulnerabilities and serious incidents [66]. In order to mitigate employees' limited knowledge of information security threats, comprehensive programmes of awareness and training are developed with a strong emphasis on culture, since there is a recognition that it is not possible to address the human dimension of information security by the simple use of procedural and technical approaches [67].

Zakaria and Gani [68] developed an information security culture framework through adapting the organisational culture typology proposed by Schein [69], and its three levels: artifacts, espoused values and shared tacit assumptions. Each level has been developed to

evaluate the elements of information security culture in organisations: the first level - surface manifestations - includes physical security and any visible and audible security implementation. The second level - values - includes information security policy, standards, procedures and guideline documents. The third level - basic assumptions - includes the implicit assumptions underlying employees' behaviour towards information security on how to inspect, protect, detect, react ad reflect. At the level of values, information security policies are particularly helpful in operating the conversion of tacit knowledge held by senior managers into explicit knowledge that can facilitate employees' understanding of roles and responsibilities [70]. At the level of basic assumptions, employee socialisation and sharing of knowledge are vital to trigger processes of individual and organisational learning [71]. Through focusing on communication, feedback and motivation, such practices reinforce the assimilation of values disseminated by policy [72].

Different organisational factors may interact with organisations' information security culture across the different levels it manifests itself. On the one hand, top management commitment and leadership exert strong influences on the values held by organisational insiders [73]. One the other hand, organisational size and industry sector may add more nuances to an organisation's information security culture. Smaller organisations are less likely to invest in information security due to budget and time constraints [74]. Similarly, top managers in smaller organisations tend to give less support to the development of information security culture, partly due to the fact that security breaches are usually not reported, which leads to organisational insiders failing to fully understand the importance of information security [66]. Variations in industry type are also relevant, with information services, finance and insurance sectors being more aware, investing more, and making greater efforts to develop an organisation-wide information security culture [74].

3. Method and data

Given the relatively emergent state of knowledge with respect to organisational insiders' perceptions of information security practices and culture, this paper takes an inductive thematic analysis approach that emphasises thick description and categorisation, as opposed to hypothesis testing and theory confirmation.

Therefore, from a research philosophy perspective, this research is interpretive. Interpretivists assume that human activity is subjective, that reality is inter-subjective, and that only a research approach focused on the richness of subjective experiences rather than on objectivity and generalisation can contribute to explore and understand the human actors, cultures and phenomena [75]. Accordingly, it is assumed that an interpretive approach will facilitate a deeper understanding and recognition of stakeholders' perspectives and the social, political and cultural aspects that surround them [76].

In terms of research design, a single case study design [77] is chosen not to accentuate generalisability, but rather to carefully examine organisational events that exhibit "the operation of some identified general theoretical principles" [78]. This fits well with our motivation to identify effective components of information security efforts, as perceived by organisational insiders, and is aligned with the role of single case study research as allowing to more clearly understand and explain variables that escape cross-sectional quantitative research [79]. Therefore, the findings do not reflect the statistical conception of generalisability and are instead aligned with the notion of "analytical generalisation", which is determined by the extent to which findings can be "used as guide to what might occur" in similar socio-organisational settings [80]. Accordingly, the resulting outcome of the detailed case analysis is a set of thematic propositions that are suggestive of theory. Furthermore, the use of case studies is well established in the disciplines of Information Science [81, 82, 83], Management of Technology

and Innovation [84, 85, 86], and Information Systems [87, 88, 89]. It has been described as particularly "appropriate for studying state of the art IS questions in a natural setting" [8].

3.1. The case company

Textile α is a South Korean medium-sized original brand manufacturing firm (OBM)[1], with its main office located in South Korea, and two manufacturing branches based in the Philippines and in Vietnam. The firm comprises 300 employees. It has been consistently enjoying sales growth and profitability, and it has been ranked amongst the country's top manufacturers of textile accessories, more specifically sports equipment and backpacks. Because of its strong emphasis on design, there is a general consensus that the R&D department is vital for the firm's success: it develops new products, improves existing products, and above all handles confidential information such as production techniques, customer and partner information, and products' concepts and prototypes.

Similarly to the analysis performed by Nelson [91] on industrial R&D, R&D at Textile α takes place at an in-house specialised laboratory that concentrates a group of individuals trained in science and engineering, and whose primary mission is to introduce technical change. Their location and high degree of specialisation signify that they are simultaneously close enough to solve shop-floor problems (in the sense that they too are organisational insiders), yet sufficiently distant not to be consumed by routine issues that would stand in the way of their role as the company's formal learning unit. In effect this learning capacity of organised R&D is described in the literature as a combination of learning (e.g. acting as a gatekeeper of new information) and creating roles (e.g. through incorporating new components, materials, and manufacturing methods into an established product) [91, 92, 93]. Of particular importance here is the role played by design, more specifically independent design capability that allows

products that stand within stable technology frontiers to move upwards in the value-chain [94], notably through the development of proprietary product-designs.

In order to better align security goals with business goals Textile α integrates information technology with physical security: alongside operating physical entry controls for the information technology facilities that operate core business activities (i.e. key card accessible facilities), it maintains audit logs recording systems' user actions in an integrated server log. Other technical solutions in place to mitigate information security threats include the use of network-attached storage (NAS) array for multimedia files archiving and disaster recovery; and the enforcement of network access control (NAC) that followed the occurrence of virus attacks.

3.2. Data collection and data analysis

Data collection developed through semi-structured interviews with informants from various levels of the R&D department in order to cross-check the reliability of data. Emerging theoretical construction derived from data analysis has also lead us to engage in interviews with the Director of the Strategic Planning Department, and the Director of the Computing Division. In total, we conducted a total of 10 interviews, as shown in Table 1. Each interview lasted for about 1 hour, was audio recorded and transcribed verbatim for analysis.

Table 1. List of interviews

Interviewees	Business unit
RDD1 - Section Coordinator, Innovation	
RDD2 - Section Coordinator, Operations	R&D Department
RDD3 - Section Coordinator, Quality	

RDD4 - Deputy Section Coordinator, New product research	
RDD5 - Deputy Section Coordinator, New product development	
RDD6 - Deputy Section Coordinator, Product update	
RDD7 - Deputy Section Coordinator, Materials and design	
RDD8 - Operational Manager	
SPD - General staff	Strategic Planning Department
CD - General staff	Computing Division

Based on the theoretical sensitivity [29] acquired with the review of the literature, the interview guide was designed to generate a deep understanding of several interlocking dimensions: the function of the R&D department and the role information plays within it; participants' job role and perceptions of information security threats and challenges; existent information security policies and controls; recovery from information security incidents; and recommendations to strengthen information security. Nonetheless, the questions were worded in a sufficiently open way, as to allow informants' recall and free disclosure of their behaviours and perceptions towards information security. Table 2 below provides a complete overview of the semi-structured interview guide employed for data collection. The guide was designed to keep the interview within the parameters defined by the objectives of study. Probing and follow-up questions were used to deepen response to questions and increase the richness of data.

Table 2. Semi-structured interview guide

Questions
1. Can you describe the mission of the R&D department and how important the security of information is in your job role? 2. Can you describe, in your opinion, what are the information security challenges of the R&D department? 3. What in your view is the relationship between information security activities and the business goals of the R&D department? 4. Is there a formal information security policy? How are information security matters managed across the organisation? 5. What in your opinion are the greatest threats to information security at the R&D department? a) Have you experienced or known about any type of breach in the past? 6. Do you feel there is a common understanding of information security and information security threats among the staff at the R&D department? 7. What kind of tasks, responsibilities and routines relating to information security exist in the R&D department? a) Are there any practices that you consider important to develop? 8. In your opinion, which factors affect employees' information security awareness? a) How important are relationships between employees? b) Do you have a training programme in place and induction for news staff? c) What is the role of rewards and punishments? 9. Can you describe the current systems, practices and controls that are used to address information security matters? 10. How are users' actions controlled, logged and audited? 11. What is the R&D's department policy on employees bringing their own computing devices to the workplace? 12. How would the R&D department recover from an information security breach and resume business? a) What type of recovery plans or business continuity plans are in place? 13. Is there anything you would change in the way departments and staff interact and are managed to improve the levels of information security?

Once interview transcription was completed, the interviews were analysed following the inductive thematic analysis technique, whereby data is examined to identify a set of emergent themes. Inductive thematic analysis is a systematic method for "identifying, analysing and reporting patterns (themes) within data" [95], and it is appropriate for analysing the data

collected from interpretive and qualitative methods. The coding transcripts developed collaboratively between the authors, following the principle of consensus, to ensure interpretive agreement and reliability.

4. Findings

Altogether, 10 themes referring to information security practices were identified: organisational mission statement; common understanding of information security; awareness of threats; information security incidents; information security routines; information security policy; relationships between employees; circulation of stories; punishment provisions; and training. Appendix 1 presents an overview of these themes, providing operational definitions that highlight their properties, alongside with representative interview quotations.

4.1. Organisational mission statement

The organisational mission statement emerged as a reoccurring theme in informants' appraisal of information security practices. Participants commonly stated that the mission of R&D Department is to design, plan and develop new and existing products up to the manufacturing stage, which entails dealing with different types of data that are critical business assets such as intellectual property, drawing data, modelling data, product specification details, etc. The following response from an operational manager illustrates this theme in action:

> I think that all information pertaining to the products that are handled and produced in this department is important, so the important information can really be all the different things related to the products such as the design of the product, the project and planning data, information on materials, specifications and so on [RDD3].

4.2. Common understanding of information security

Organisational insiders often recounted the role played by the existence of a common understanding of information security challenges, notably an agreement around the R&D's department responsibility for handling and managing information in the most secure way. As stated by an R&D department coordinator:

> The information security challenge faced by the R&D team is to conduct business processes in security, which means to keep all the important data secured from unauthorized persons" [RDD6].

Although commonly shared amongst the majority the informants, this perception seemed more deeply ingrained in the discourse of coordinators and deputy coordinators and indeed a minority of employees recounted feeling less clear about the importance of talking through information security issues and the need to develop a common conceptual framework to tackle them.

4.3. Awareness of threats

Through individual accounts, participants recalled a series of externally-rooted security threats such as virus attacks, data loss due to hacker intervention, or information leakage. Security threats attributed to insiders were also frequent, as explained by a deputy section coordinator:

> Insider threat is another important source of threats that we need to consider. In other words, a dissatisfied employee base provides a vector for insider security events… The inadvertent

> leakage of information through removable devices or internet connections can make any employee the origination point for serious information security violations [RDD2].

Another type of threat identified by the Strategic Planning department refers to R&D knowledge loss occurring via job mobility and employee turnover:

> The company is ranked within the top performing firms in the field, hence a major threat comes from our employees changing jobs within the same field, and eventually sharing all the information with our competitors. In this very tight business area, R&D employees are often headhunted with higher salary prospects offered by a rival company in order to steal important information [SPD].

Overall, there seems to be recognition of a variety of threats but not enough proactive response. A deputy section coordinator reflects on the reasons that may originate this lack of proactiveness, and suggests that the negligent behaviour of staff may have a cultural foundation:

> Due to the fast development of the internet culture, everything can be easily shared and exposed and therefore this culture sticks to people's everyday life behaviour. People unconsciously behave like this in their workplace when they should be thinking business [RDD5].

4.4. Information security incidents

Not all participants had experienced – directly or indirectly – the developing stages and the effects of information security incidents. This varying level of experience contributes to several participants constructing the notion that there are no major threats to the security of information and that the company does not have any formal disaster recovery plan in place. These accounts also reveal that there is insufficient knowledge on how to handle a security breach, should one occur. Only technical staff from the computing division was able to articulate and describe the incident control process, stating that:

> (…) under the case of security infringement, we first check the detailed information through network log, and then if it is later confirmed, we make efforts to prevent the recurrence of accidents, such as network access control and port block [CD].

However, many respondents did not know how to manage the unexpected event of security breaches and to identify who is ultimately accountable for those situations. The most common answer was attributing responsibility to the individual directly triggering the incident, which further indicates a lack of awareness of line of authority and reporting procedures:

> Basically the contributor takes responsibility for the incident and the boss of his or her department is also responsible for neglecting the management and training [RDD7].

4.5. Information security routines

The absence of actionable, repeated patterns of action that reinforce information security behaviour was identified as an area of concern by organisational insiders. The most commonly

mentioned tasks related to security are ensuring doors are locked and backing up data, but in general terms it was not felt that information security tasks were an integral component of R&D staff daily routines. The example below illustrates how the Strategic Department perceives this absence of established routines:

> There are no particular tasks and routines related to information security, but we are trying not to expose the information to the outside - we do not share materials, data and documents with other departments and other employees as well; and we only share these with accepted people in the same department, especially people who carry out same project and so the access is justified [SPD].

4.6. Information security policy

Information security policy also arose as a recurrent theme, but largely due to the widely acknowledged absence of a formal security policy document in the firm. Only one deputy section coordinator claims that:

> (…) It is officially forbidden to take photos inside the R&D department, to access personal blogs and messaging applications, and to bring personal USBs and external hard drives [RDD1].

However, the formal terms of policy are in sharp contrast to a deputy section coordinator's acknowledgement that in practice "all employees are using their smartphones and a few of them bring tablets for personal use" [RDD4]. Another unregulated domain is employees' use of their own personal devices for both work and leisure. Although tacitly permitted, the use of personal electronic devices such as laptops for work purposes is not encouraged: "it is accepted if it fulfils business needs, but it is not supported by the company" [RDD2]. Therefore, calls

for “the establishment of a systematic manual for information security to resolve the confusion of information security practices amongst employees” [RDD6] are nearly unanimous.

4.7. Relationships between employees

Across interviews organisational insiders’ perceptions diverged concerning the impact of employee socialisation on the adherence to information security practices. Employees in the middle echelons tended to consider that “employees should be united and dedicated to the same goals as the organisation’s” [RDD6], which includes the discussion of information security goals in terms that they describe as “horizontal” and “mutually beneficial”. On the other hand, participants holding senior managerial positions such as section coordinators tended to believe that “the relationship between staff does not affect information security activity because Textile α is a medium size firm” [RDD7].

4.8. Circulation of stories

The limited disclosure of organisational insiders’ experience of information security incidents and a reported blanket of silence surrounding the existence of damage resulting from previously undiscussed information security incidents contributed to a generalised feeling of apathy, reinforced by the limited circulation of stories that could instead help articulate experience and make up organisational insiders’ understandings of information security dos *and don’ts*. An example of how stories as a way of remembering personal and organisational meaning could have been used is reccounted by the Strategic Planning Department when recalling a virus attack incident:

> Due to the virus attack, we had run into a problem with the poor network. (…) We could not use the internet properly and therefore it caused that we could not send and receive files, complete tasks and exchange messages with co-workers in other branches [SPD].

The opacity surrounding this event and the absence of narrative mechanisms stood in the way of organisational insiders talking about the real experience of their organisation and reflecting on shared perceptions of dealing with information security incidents. In this particular example, different interpretations surrounding the incident were selected, legitimised and institutionalised, as the R&D department coordinator downplays its consequences and frames in completely different terms: "the company had a virus attack before, but it was not of great concern" [RDD8].

4.9. Punishment provisions

Building up on the absence of established organisational narratives of information security incidents, and on the lack of reporting mechanisms, organisational insiders denounced the lenient way in which the firm deals with employee faults associated with the inexistence of punishment provisions in case of information security breach. Both aspects are linked by participants to the dominant family-like organisational culture, where there is room for forgiveness of light faults, but where serious mistakes are heavy-handedly punished:

> There is no particular punishment system, because the culture of the company is like family feeling, the atmosphere of the company is such that the supervisor kindly leads his or her subordinates. Therefore, if an employee makes a mistake, his or her superior helps them to do better, not blaming or punishing the employee. However, if the employee causes extensive damage, commits a fatal mistake or his malicious action has negative effect within the company, the company may give notice of dismissal [RDD7].

4.10. Training

Information security awareness training was described by organisational insiders as superficial and unsystematic, although participants acknowledge its benefits:

> Establishing information security policy and training employees about information security would be helpful to understand the proper security attitude and behaviour [RDD6].

Given the absence of procedure-oriented security policies, organisational insiders recalled only the existence of induction training for new staff, focusing mainly on the technically-oriented dimensions of information security and usually taking amid introductions to other staff, guided visits to the firm's premises, and through direct contact with senior staff: "we do not have a formal training programme but new staff are individually educated by their superior" [RDD3].

The following section discusses the themes emerging from the analysis and situates them in the wider context of the information security literature.

5. Discussion

The enculturation of information security within organisations requires the implementation and management of technical, social, formal and informal controls. The actions and behaviour of organisational insiders, in particular, are recognised as one of the most significant enablers of information security success [43, 46], but the human factor is often overlooked [58, 79]. In Textile α the understanding of information security challenges is uneven among organisational insiders, although specific threats such as the intentional or unintentional behaviour of organisational insiders and knowledge leakage due to employee turnover were reported more

frequently across participants' accounts. Similar threats are echoed in the information security literature [17].

The successful management of information security requires an integrated approach to the administration of people, policies and programmes that simultaneously delivers operational objectives and preserves strategic alignment with the organisation's mission [96]. Small and medium size enterprises often find this integrated approach to the management of information security challenging, more specifically the establishment of security policies and the conduct of risk assessments, since they frequently lack the human and financial resources to coordinate information security [66, 74, 97, 98]. Textile α fits this description and organisational insiders report the absence of a formal security policy. Nevertheless, the literature identifies information security policy as one of the main components of effective information security management and it can assist to enable security-inducing practices [54]. According to Kankanhalli et al. [74], policy statements and guidelines can inform the design of information security activities, spanning from controls on the legitimate use of information assets to the deployment of more advanced security methodologies. Such policy instruments can also help to reduce instances where employees handle security software without adequate information security knowledge [101].

The existence of training programmes can help organisational insiders understand the context of information security policy, and develop awareness of information security practices [72, 101]. Furthermore, the education of employees on the roles and responsibilities related to security can contribute to the reduction of incidents [102]. Despite acknowledging the importance of training programmes in the development of information security awareness, organisational insiders within Textile α describe the unsystematic nature of training opportunities available.

Information security awareness training can be enhanced through integration with the organisation's established communication processes (e.g. product development meetings) and training programmes [67]. This can help employees internalise roles and responsibilities and make security tasks an integral part of their daily routines, something Textile α has been unable to achieve, partly also due to the limited circulation of stories describing, reflecting and extracting learning from the occurrence of previous information security incidents. In reality, when reporting mechanisms are lacking, incidents are covered in a blanket of silence that obliterates opportunities for organisational learning. The impact of learning through social interaction is also limited in Textile α due to ambivalent views on the potential of taking social cues and enacting values from interactions on the job with other organisational actors. The resistance identified in Textile α's senior employees contradicts the general assumption conveyed in the literature that relationships between organisational insiders encourage greater awareness of information security threats, information policy compliance, and collaboration in case of information security incidents [68, 71, 101].

Finally, in line with a variety of studies that raise the pernicious effect of penalties and punishment as a deterrence approach [71, 74], Textile α does not have an established policy that enforces punishment provisions in case of information security breach, although severe misconduct leads to staff dismissal.

Overall, the themes identified and discussed in the paper add to the stream of studies that have advanced the understanding of individuals' motivations and the processes associated to decision-making concerning compliance or non-compliance with information security procedures and policies. On the one hand, the themes of "awareness of threats", "information security incidents", "information security routines", "information security policy", "relationship between employees", "punishment provisions" and "training" align with and complement studies that have explored the extent to which individuals conform to what is

prescribed by organisational information security policy, and the ways in which individuals evaluate and respond to information security threats. This includes the concepts of: attitude towards security [101, 102]; self-efficacy, denoting ability and expertise to enable security measures [38, 103]; commitment, denoting willingness to invest energy and effort in ensuring organisational practices that conform to information security [102, 103]; compliance behavioural intentions [101, 104]; involvement, denoting an attempt to build relationships in connection with information security [101, 103]; the severity of sanctions in case of offence [102, 104] and information richness and its impact on security awareness training effectiveness [105].

On the other hand, the themes of "organisational mission statement", "common understanding of information security", and "circulation of stories" advance the understanding of information security practices through addressing the critical issue of how to turn organisational insiders into information security allies, as opposed to the prevalent view of insiders as a latent source of risk. More specifically, "organisational mission statement" and "common understanding of information security" theorise how the images organisational insiders' hold of organisations effectively act as powerful shapers of their own identification with the organisation they are affiliated with, akin to Dutton et al's proposal that "strong organizational identification may translate into desirable outcomes such as intraorganizational cooperation or citizenship behaviours" [106]. In other words, if insiders believe in the central and enduring nature of information and its security for their organisation's performance, they will be more attuned to its future viability and therefore direct increased effort into practices that signify and operationalise that commitment. As for the role played the "circulation of stories", the theme highlights he vital role played by narratives as organisational sensemaking mechanisms [107] that socialise employees, generate commitment [108] and provide a medium for capturing organisational knowledge [109]. The absence of a stock of stories actively

circulating is interpreted as manifestation of both organisational silence and ignorance, through the deliberate cultivation of taboos and conscious denials [110], suppressed employee voice [111] or the feeling that one's opinions are not valued [112].

6. Conclusion

Information security efforts tend to focus mainly on the technical implementation details, which typically results on a limited integration with existing organisational processes and on the absence of a holistic information protection strategy that is sensitive to organisational insiders' needs and aspirations. Based on the auscultation of organisational insiders' perceptions, the following practices can inform the development of more successful information security strategies:

1. An upfront determination of clear goals and objectives. Organisational information security strategies should help achieve strategic business objectives, so clear objectives based on the organisation's mission are an essential step in ensuring that the information security strategy protects the information assets that are key to the business. This should have input from various business and operating units, so that organisation-wide participation, understanding and acceptance are unlocked.

2. Definition and organisation-wide understanding of sensitive (valuable, inimitable and non-substitutable) information assets, so that associated sensitivity risks are assessed and proper controls are implemented (e.g. information flows monitoring).

3. Holistically addressing the people, process and technology dimensions, so that organisations assign clear roles and responsibilities for individuals, rely on fit-for-purpose tools to prevent and identify information security threats, and operate based on effective and well known processes to report, investigate, and respond to incidents.

4. Reinforcing awareness mechanisms, to enable an environment where organisational insiders learn and adhere to social norms and values, more specifically the importance of their organisation's information security practices. This should develop through encouraging greater organisational bonding (e.g. regular meetings to discuss security events and concerns), and through security awareness sessions and training designed to shape organisational insiders' attitudes, and to ultimately equip them with the knowledge and skills necessary to assume responsibility for the safeguard of information assets. Part of the awareness mechanisms should also be a compliance auditing effort, focused on testing and validating organisational insiders' knowledge of information security threats and practices, and on ensuring that a continuous improvement cycle is in place.

The adoption of a practice approach that conceptualises information security as something organisational insiders do, enables information science researchers to further understand how information security strategy is carried out, who are the agents of strategy work, and what resources are mobilised to conduct this work. Similarly, in considering organisational insiders' knowledge of information security as practical accomplishment, this paper contributes to advance understanding of how information security-related knowledge is produced, internalised and performed in routine work practices. Future research can extend this effort and further investigate the discursive practices of those who govern information security strategies

and actively shape the environment where organisational insiders learn about organisational values, in order to establish the impact of organisational citizenship behaviour on information security compliance.

Notes

1. This paper adopts the taxonomy proposed by Yusuf [90], where OBM stands for original brand manufacturing, and is defined as "selling the products under its own brand". In the same taxonomy, ODM refers to original design manufacturing and entails dealing with the functions from "postconceptual design to the manufacturing". Finally, OEM (original equipment manufacturing) refers to firms that only engage in the manufacturing of components following the specifications provided by clientes.

References

[1] Sumner M. Information security threats: a comparative analysis of impact, probability, and preparedness. Information Systems Management. 2009 Jan 13;26(1):2-12.

[2] Abbas H, Magnusson C, Yngstrom L, Hemani A. Addressing dynamic issues in information security management. Information Management & Computer Security. 2011 Mar 22;19(1):5-24.

[3] Yildirim EY, Akalp G, Aytac S, Bayram N. Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management. 2011 Aug 31;31(4):360-5.

[4] Choo KK. The cyber threat landscape: Challenges and future research directions. Computers & Security. 2011 Nov 30;30(8):719-31.

[5] Shabtai A, Elovici Y, Rokach L. A survey of data leakage detection and prevention solutions. Springer Science & Business Media; 2012 Mar 15.

[6] Venter HS, Eloff JH. A taxonomy for information security technologies. Computers & Security. 2003 May 31;22(4):299-307.

[7] Cavusoglu H, Raghunathan S, Cavusoglu H. Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. Information Systems Research. 2009 Jun;20(2):198-217.

[8] Hu Q, Hart P, Cooke D. The role of external and internal influences on information systems security–a neo-institutional perspective. The Journal of Strategic Information Systems. 2007 Jun 30;16(2):153-72.

[9] Dhillon G, Backhouse J. Technical opinion: Information system security management in the new millennium. Communications of the ACM. 2000 Jul 1;43(7):125-8.

[10] Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS quarterly. 1998 Dec 1:441-69.

[11] Alnatheer M, Chan T, Nelson K. Understanding And Measuring Information Security Culture. InPACIS 2012 (p. 144).

[12] Al-Omari A, El-Gayar O, Deokar A. Security policy compliance: User acceptance perspective. InSystem Science (HICSS), 2012 45th Hawaii International Conference on 2012 Jan 4 (pp. 3317-3326). IEEE.

[13] McInerney CR, Koenig ME. Knowledge management (KM) processes in organizations: Theoretical foundations and practice. Synthesis Lectures on Information Concepts, Retrieval, and Services. 2011 Jan 17;3(1):1-96.

[14] Stock RM, Reiferscheid I. Who should be in power to encourage product program innovativeness, R&D or marketing?. Journal of the Academy of Marketing Science. 2014 May 1;42(3):264-76.

[15] Tsang EW, Yip PS, Toh MH. The impact of R&D on value added for domestic and foreign firms in a newly industrialized economy. International Business Review. 2008 Aug 31;17(4):423-41.

[16] Farahmand F, Spafford EH. Understanding insiders: An analysis of risk-taking behavior. Information systems frontiers. 2013 Mar 1;15(1):5-15.

[17] Ahmad A, Bosua R, Scheepers R. Protecting organizational competitive advantage: A knowledge leakage perspective. Computers & Security. 2014 May 31;42:27-39.

[18] de Faria P, Sofka W. Knowledge protection strategies of multinational firms—A cross-country comparison. Research Policy. 2010 Sep 30;39(7):956-68.

[19] Peltier TR. Information security fundamentals. CRC Press; 2013 Oct 16.

[20] Olander H, Vanhala M, Hurmelinna-Laukkanen P. Reasons for choosing mechanisms to protect knowledge and innovations. Management Decision. 2014 Mar 11;52(2):207-29.

[21] Ilvonen I, Vuori V. Risks and benefits of knowledge sharing in co-opetitive knowledge networks. International Journal of Networking and Virtual Organisations. 2013 Jan 1;13(3):209-23.

[22] Schiuma G, editor. Managing Knowledge Assets and Business Value Creation in Organizations: Measures and Dynamics: Measures and Dynamics. IGI Global; 2010 Nov 30.

[23] Vaara E, Whittington R. Strategy-as-practice: taking social practices seriously. The Academy of Management Annals. 2012 Jun 1;6(1):285-336.

[24] Chia R. Strategy-as-practice: Reflections on the research agenda. European Management Review. 2004 Mar 1;1(1):29-34.

[25] Molloy E, Whittington R. Organising organising: the practice inside the process. Advances in Strategic Management. 2005;22:491-515.

[26] Denis JL, Langley A, Rouleau L. The power of numbers in strategizing. Strategic

Organization. 2006 Nov 1;4(4):349-77.

[27] Jarzabkowski P, Paul Spee A. Strategy-as-practice: A review and future directions for the field. International Journal of Management Reviews. 2009 Mar 1;11(1):69-95.

[28] Weick KE. Sensemaking in organizations. Sage; 1995 May 31.

[29] Glaser BG. Theoretical sensitivity: Advances in the methodology of grounded theory. Sociology Pr; 1978.

[30] McFadzean E, Ezingeard JN, Birchall D. Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review. 2007 Oct 2;31(5):622-60.

[31] Ahmad A, Maynard SB, Park S. Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing. 2014 Apr 1;25(2):357-70.

[32] Baskerville R, Spagnoletti P, Kim J. Incident-centered information security: Managing a strategic balance between prevention and response. Information & management. 2014 Jan 31;51(1):138-51.

[33] Manhart M, Thalmann S. Protecting organizational knowledge: a structured literature review. Journal of Knowledge Management. 2015 Apr 7;19(2):190-211.

[34] Chen PY, Kataria G, Krishnan R. Correlated failures, diversification, and information security risk management. Mis Quarterly. 2011 Jun 1;35(2):397-422.

[35] Coles-Kemp L, Theoharidou M. Insider threat and information security management. InInsider threats in cyber security 2010 (pp. 45-71). Springer US.

[36] Sarkar KR. Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report. 2010 Aug 31;15(3):112-33.

[37] Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future

directions for behavioral information security research. computers & security. 2013 Feb 28;32:90-101.

[38] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly. 2010 Sep 1;34(3):523-48.

[39] Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Systems. 2010 Mar 31;48(4):635-45.

[40] Vance A, Siponen MT. IS security policy violations: a rational choice perspective. Journal of Organizational and End User Computing (JOEUC). 2012 Jan 1;24(1):21-41.

[41] D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research. 2009 Mar;20(1):79-98.

[42] Lowry PB, Posey C, Bennett RB, Roberts TL. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. Information Systems Journal. 2015 May 1;25(3):193-273.

[43] Siponen M, Mahmood MA, Pahnila S. Employees' adherence to information security policies: An exploratory field study. Information & management. 2014 Mar 31;51(2):217-24.

[44] Cheng L, Li W, Zhai Q, Smyth R. Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Computers in Human Behavior. 2014 Sep 30;38:220-8.

[45] Sommestad T, Karlzén H, Hallberg J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information & Computer Security.

2015 Jun 8;23(2):200-17.

[46] Posey C, Roberts TL, Lowry PB, Hightower RT. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & management. 2014 Jul 31;51(5):551-67.

[47] Van Niekerk JF, Von Solms R. Information security culture: A management perspective. Computers & Security. 2010 Jun 30;29(4):476-86.

[48] Kraemer S, Carayon P, Clem J. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & security. 2009 Oct 31;28(7):509-20.

[49] Komatsu A, Takagi D, Takemura T. Human aspects of information security: An empirical study of intentional versus actual behavior. Information Management & Computer Security. 2013 Mar 15;21(1):5-15.

[50] ISO/IEC. Information technology – security techniques – information security management systems – overview and vocabulary. ISO/IEC 27000:2009(E). 2009 May.

[51] ISSO/IEC. Information technology Security techniques - Code of practice for information security controls. ISO/IEC 27002: 2013(E). 2013.

[52] Bishop M. What is computer security?. IEEE Security & Privacy. 2003 Jan;1(1):67-9.

[53] Lampson BW. Computer security in the real world. Computer. 2004 Jun;37(6):37-46.

[54] Doherty NF, Fulford H. Aligning the information security policy with the strategic information systems plan. Computers & Security. 2006 Feb 28;25(1):55-63.

[55] Malcolmson J. What is security culture? Does it differ in content from general organisational culture?. In43rd Annual 2009 International Carnahan Conference on Security Technology 2009 Oct 5 (pp. 361-366). IEEE.

[56] Knapp KJ, Morris RF, Marshall TE, Byrd TA. Information security policy: An

organizational-level process model. Computers & Security. 2009 Oct 31;28(7):493-508.

[57] Stamp M. Information security: principles and practice. John Wiley & Sons; 2011 Nov 8.

[58] Von Solms B. Information security—the third wave?. Computers & Security. 2000 Nov 1;19(7):615-20.

[59] Von Solms SB. The 5 waves of information security–from Kristian Beckman to the present. InIFIP International Information Security Conference 2010 Sep 20 (pp. 1-8). Springer Berlin Heidelberg.

[60] Thomas M, Dhillon G. Interpreting deep structures of information systems security. The Computer Journal. 2011 Nov 30:bxr118.

[61] Hamill JT, Deckro RF, Kloeber JM. Evaluating information assurance strategies. Decision Support Systems. 2005 May 31;39(3):463-84.

[62] Mejias RJ. An integrative model of information security awareness for assessing information systems security risk. InSystem Science (HICSS), 2012 45th Hawaii International Conference on 2012 Jan 4 (pp. 3258-3267). IEEE.

[63] Whitman ME, Mattord HJ. Management of information security. Nelson Education; 2013 Oct 7.

[64] Spears JL, Barki H. User participation in information systems security risk management. MIS quarterly. 2010 Sep 1:503-22.

[65] Schlienger T, Teufel S. Analyzing information security culture: increased trust by an appropriate information security culture. InDatabase and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on 2003 Sep 1 (pp. 405-409). IEEE.

[66] Dojkovski S, Lichtenstein S, Warren MJ. Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. InECIS 2007 Jan 1 (pp. 1560-1571).

[67] Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: an action research study. Mis Quarterly. 2010 Dec 1:757-78.

[68] Zakaria O, Gani A. A conceptual checklist of information security culture. In2nd European Conference on Information Warfare and Security, Reading, UK 2003 Jun 30.

[69] Schein EH. Organizational culture and leadership. Jossey-Bass; 1992.

[70] Thomson KL, von Solms R, Louw L. Cultivating an organizational information security culture. Computer Fraud & Security. 2006 Oct 31;2006(10):7-11.

[71] Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 2009 Apr 1;18(2):106-25.

[72] Waly N, Tassabehji R, Kamala M. Improving organisational information security management: The impact of training and awareness. InHigh Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on 2012 Jun 25 (pp. 1270-1275). IEEE.

[73] Ernest Chang S, Ho CB. Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems. 2006 Mar 1;106(3):345-61.

[74] Kankanhalli A, Teo HH, Tan BC, Wei KK. An integrative study of information systems security effectiveness. International journal of information management. 2003 Apr 30;23(2):139-54.

[75] Orlikowski WJ, Baroudi JJ. Studying information technology in organizations: Research approaches and assumptions. Information systems research. 1991 Mar;2(1):1-28.

[76] Stockdale R, Standing C. An interpretive approach to evaluating information systems: A content, context, process framework. European journal of operational research. 2006 Sep

16;173(3):1090-102.

[77] Yin R. K.(2003). Case study research: Design and methods. Sage Publications, Inc. 2003;5:11.

[78] Mitchell JC. Case and situation analysis. The Sociological Review. 1983 May 1;31(2):187-211.

[79] Stoecker R. Evaluating and rethinking the case study. The Sociological Review. 1991 Feb 1;39(1):88-112.

[80] Kvale S, Brinkmann S. Learning the craft of qualitative research interviewing. Thousands Oaks: Sage Publications. 2009.

[81] Rasmussen L, Hall H. The adoption process in management innovation: A Knowledge Management case study. Journal of Information Science. 2016 Jun 1;42(3):356-68.

[82] Yang TM, Wu YJ. Exploring the determinants of cross-boundary information sharing in the public sector: An e-Government case study in Taiwan. Journal of Information Science. 2014 Oct 1;40(5):649-68.

[83] Hussain Z, Taylor A, Flynn D. A case study of the process of achieving legitimation in information systems development. Journal of Information Science. 2004 Oct 1;30(5):408-17.

[84] Boonstra A, Govers MJ. Understanding ERP system implementation in a hospital by analysing stakeholders. New Technology, Work and Employment. 2009 Jul 1;24(2):177-93.

[85] Fogarty H, Scott P, Williams S. The half-empty office: dilemmas in managing locational flexibility. New Technology, Work and Employment. 2011 Nov 1;26(3):183-95.

[86] Ogbonna E, Harris LC. Organisational culture in the age of the Internet: an exploratory study. New Technology, Work and Employment. 2006 Jul 1;21(2):162-75.

[87] Benbasat I, Goldstein DK, Mead M. The case research strategy in studies of information

systems. MIS quarterly. 1987 Sep 1:369-86.

[88] Walsham G, Waema T. Information systems strategy and implementation: a case study of a building society. ACM Transactions on Information Systems (TOIS). 1994 Apr 1;12(2):150-73.

[89] Keutel M, Michalik B, Richter J. Towards mindful case study research in IS: a critical analysis of the past ten years. European Journal of Information Systems. 2014 May 1;23(3):256-72.

[90] Yusuf S, editor. Innovative East Asia: the future of growth. World Bank Publications; 2003.

[91] Nelson R. The roles of firms in technical advance: a perspective from evolutionary theory. Technology and enterprise in a historical perspective. 1992:164-84.

[92] Cohen WM, Levinthal DA. Absorptive capacity: A new perspective on learning and innovation. Administrative Science Quarterly. 1990 Mar 1:128-52.

[93] Forbes N, Wield D. Managing R&D in technology-followers. Research Policy. 2000 Dec 31;29(9):1095-109.

[94] Walsh V. Design, innovation and the boundaries of the firm. Research Policy. 1996 Jun 30;25(4):509-29.

[95] Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006 Jan 1;3(2):77-101.

[96] Choobineh J, Dhillon G, Grimaila MR, Rees J. Management of information security: Challenges and research directions. Communications of the Association for Information Systems. 2007 Dec 31;20(1):57.

[97] Williams MA. Privacy management, the law & business strategies: A case for privacy driven design. InComputational Science and Engineering, 2009. CSE'09. International Conference on 2009 Aug 29 (Vol. 3, pp. 60-67). IEEE.

[98] Torres JM, Sarriegi JM, Santos J, Serrano N. Managing information systems security: critical success factors and indicators to measure effectiveness. InInternational Conference on Information Security 2006 Aug 30 (pp. 530-545). Springer Berlin Heidelberg.

[99] Gundu T, Flowerday SV. The enemy within: A behavioural intention model and an information security awareness process. In2012 Information Security for South Africa 2012 Aug 15 (pp. 1-8). IEEE.

[100] Ruighaver AB, Maynard SB, Chang S. Organisational security culture: Extending the end-user perspective. Computers & Security. 2007 Feb 28;26(1):56-62.

[101] Ifinedo P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management. 2014 Jan 31;51(1):69-79.

[102] Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 2009 Apr 1;18(2):106-25.

[103] Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security. 2012 Feb 29;31(1):83-95.

[104] Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 2009 May 31;47(2):154-65.

[105] Shaw RS, Chen CC, Harris AL, Huang HJ. The impact of information richness on information security awareness training effectiveness. Computers & Education. 2009 Jan 31;52(1):92-100.

[106] Dutton JE, Dukerich JM, Harquail CV. Organizational images and member identification. Administrative science quarterly. 1994 Jun 1:239-63.

[107] Czarniawska B. Narrating the organization: Dramas of institutional identity. University of Chicago Press; 1997 Apr 15.

[108] Boyce ME. Organizational story and storytelling: a critical review. Journal of organizational change management. 1996 Oct 1;9(5):5-26.

[109] Patriotta G. Sensemaking on the shop floor: Narratives of knowledge in organizations. Journal of Management Studies. 2003 Mar 1;40(2):349-75.

[110] Roberts J. Organizational ignorance: Towards a managerial perspective on the unknown. Management Learning. 2013 Jul;44(3):215-36.

[111] Blackman D, Sadler-Smith E. The silent and the silenced in organizational knowing and learning. Management Learning. 2009 Nov;40(5):569-85.

[112] Knoll M, van Dick R. Do I hear the whistle…? A first attempt to measure four forms of employee silence and their correlates. Journal of Business Ethics. 2013 Mar 1;113(2):349-62.

Appendix 1 – Themes definition and illustrative quotations

Themes	Operational definition	Illustrative quotations
Organisational mission statement	Shared value system, behavioural guidelines and focus on common objectives	"The mission of the R&D department is to promote, develop and facilitate creative endeavours and research, to provide innovative and sustainable solutions to societal challenges in the field of product manufacturing and

		designs. Their integrity needs protection" [RDD6].
Common understanding of information security	Employees' common understanding of information security challenges	"I think partly the top management people considers information security threats seriously, but for others, I don't think they care that much about information security at work" [RDD4].
Awareness of threats	Variations in the extent to which employees are knowledgeable of information security topics and threats	"There are possible threats to information security that come from a easy outside access through the Internet. Most of our data and files are exchanged as e-mail attachments or instant messaging applications. Also, a lot of confidential information such as drawings and the design of products become exposed because it ends up in a print out. But above all, I think the most threatening factor is how little security conscious employees can be" [CD].
Information security incidents	Experiences with information security	"Direct responsibility rests with the person who causes a security breach" [RDD7].

	incident response and handling.	
Information security routines	Repeated patterns of action that reinforce information security	“There is no particular routine related to information security but we try not to expose ourselves to the outside” [SPD].
Information security policy	Management direction and support for information security	“The establishment of a systematic manual for information security would be necessary to resolve confusion and bring information security practices to all employees” [RDD2].
Relationships between employees	Adherence to information security practices through socialisation	“A bond of sympathy has developed among employees that helps understanding the importance of security and security threats” [CD].
Circulation of stories	Circulation of storied information security breaches recalled by employees	“The company has already experienced a virus attack” [RDD3].
Punishment provisions	Existence of rewards as an incentive for	“I don’t know whether there is a system of rewards and punishments because I

	exemplary security behaviour, and punishments to penalize negligent behaviour	have not been rewarded or punished" [RDD6].
Training	Induction, orientation and training activities focused on information security	"We don't have any formal induction but for the new staff we have a get-together meeting after work" [RDD5].