2014 47th Hawaii International Conference on System Science

Rethinking the Information Security Risk Practices: A Critical Social Theory Perspective

Devinder Thapa
Luleå University of Technology
Luleå, Sweden
devinder.thapa@ltu.se

Dan Harnesk
Luleå University of Technology
Luleå, Sweden
dan.harnesk@ltu.se

Abstract

There is a lack of theoretical understanding of information security risk practices. For example, the information security risks related literatures are dominated by instrumental approach to protect the information assets. This approach, however, often fails to acknowledge the ideologies and consequences of risks practices. In this paper, through critical analysis, we suggest various perspectives to advance the understanding in this regard. In doing so, we present our argument by reviewing the security risk literature using Habermas's concept of four orientations: instrumental, strategic, communicative and discursive. The contribution of this paper is to develop conceptual clarity of the risk related ideologies and its consequences on emancipation.

1. Introduction

The access of information and communication technology (ICT) services has extended to all activities of the organizational premises. No doubt, it has increased the flexibility of time and space for the organizational employees. Contrariwise, general perception of the business organizations is that pervasiveness of the ICT can increase the information security risk from outsider and insider equally. The perception started to intimidate the business organizations. Consequently, the first impression of the organizations on introducing risks practices is to impose strict policies to protect the so called 'information assets' from external and internal attacks [1]. Scholars suggested that this kind of practices fall within the functionalist paradigm [2]. To that end, organizations assume that the information security risks are controllable and predictable and that solutions exist out there. However, scholars started to argue that information security risks are complex, uncontrolled and unpredictable sociotechnical phenomena [3]. Therefore, consideration of other information security paradigms, such as interpretive, structuralist, and humanist is important for implementing effective risk practices [2].

There is a plethora of literature that discusses risks practices under functionalist paradigm and interpretive paradigm. The risks practices in these paradigms are mainly based on the ideology of protection of the object (information assets) through imposition and compliance of security policies. The missing perspective in the existing information security risk practices is emancipation of the subject (human) [4]. To contribute to this missing perspective, the paper proposes to rethink the information 'security as emancipation' [5] rather than imposition. Emancipation in the organizational context refers to freeing employees from oppressive conditions, hence enabling them to realize their full potential [6]. This paper, however, is concerned with information security risk practices, hence borrows the definition of emancipation as "freeing the employees from the power structure by increasing the scope and depth of their information access (from [4], page.2)". The authors [4] also suggested that emancipation of the employee could facilitate information assets protection.

To contribute to the similar research strand, this paper explores various discourses in information security risks practices, and enhances understanding on how to achieve liberty from the traditional ideological stances, and create inclusive risk practices. For this purpose, the paper put the critical social theory, particularly Habermas theory of communicative action [7] in the center. Thereafter, analyzes the existing risk practices through four orientations: *instrumental, strategic, communicative* and *discursive*. The analysis is done in relation to interaction between ideologies of information

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.397

IEEE computer society

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

security risk practices and its consequences on the emancipation (details in the subsequent section).

Rest of the paper is organized as follows. Section 2 discusses the ideologies of information and security risks and its consequences on information security risk practices, furthermore provides brief introduction of the theory of communicative action. Section 3 discusses critical social theory based analyses of information security risks practices; likewise, Section 4 discusses some implications to research and practice. Finally, Section 5 concludes the paper with future research agenda.

2. Theoretical Background

2.1 Risk Ideology

The concept of risk ideology rests on the idea that they are the reification of social constructions for the benefit of some groups over some other groups [8]. Ideology is associated with a set of ideals, which explains how a certain practice is expected to function [9]. Moreover, the literature contains assumptions what is believed to represent the truth and legitimacy in actions carried out to fortify the ideology of the security risk practice [10]. The fundamental assumption is that the security risk practice, commonly considered the background for risk management, does not exist unless framed in the action that occurs when risks methods and risk techniques are considered in their deployment [5].

Referring to Drummond [5], we interpret and categorize the security risk practice as either *predictive and controlled,* or *complex and unpredicted.* The predictive and controlled approach adopted in risk management routines refers to goal setting procedures, and how methods are used to manage the risk practice. With the use of various risk techniques organizations expect to manage uncertainty, which has its roots in the desire to prepare for the unexpected [1]. Notwithstanding the efforts undertaken by risk managers to deal with risks in practice, such ambition has, according to the literature proven rather difficult and complex [5, 10-11]. For example, [11] point out that a functionalist ideal to risk management is not fully capable of determining the likelihood of threats exploiting vulnerabilities because this ideal assume a stable and predictable environment. A risk management agenda that draws on this type of ideal is defining the risk practice as a product of various proxy measures. For instance, risk mitigation studies focused on measuring observable events [2] through controlling metrics, such as risk checklists [12].

The ideal underpinning the complex and unpredicted policy is advocating for inclusion of different stakeholders perspective on the subject of risk. The advantage of employing stakeholder perspective in the risk practice lies in the recognition that, e.g. computer users bring into risk identification activities. For instance, taking actions based on knowledge about technical and managerial security controls is considered responsive decision-making [13], and falls into risk strategy formulation. Recent research found that stakeholder participation in security risk management creates stronger alignment between risk management and the business context [14]. Similarly, risk awareness studies advocate that socio-organizational factors such as, technical knowledge, organizational impact, and attacker assessment are critical to risk assessment performance [15].

However, these ideals illustrate the means-end-oriented research objectives that substantially have influenced the organization of risk practices in order to protect information assets. To a large extent, these accounts are descriptive as they prescribe 'management-in-action' protocols to render secure IT milieus. It is argued, for instance, that integration of systems theories, i.e. security policy, risk management, control and auditing, management systems, and contingency theories are relevant building blocks of a comprehensive approach to information security management [16]. In many ways, such an integrated approach is meant to better facilitate prioritization of security risks to information systems and the security measures [17]. However, the reach of this functionalist approach is limited to possibility of defining instrumental goals and methods and strategic issues of concern for relevance stakeholders. When this ideology continuously influences the risk practice, there is a significant risk that the ideology itself becomes an illusion, a view that risk factors are under control when indeed they are not [5]. This raises several interesting issues about adherence to risk ideals. For instance, who decides which ideals are important? How to reinforce employees' loyalty towards the ideology? How should the ideology be justified? And, how could it be evaluated? What are the criteria for evaluation? Are the criteria uniform or varying?

2.2 Consequences of risk ideology

Any ideology's conditions are the reflection of the expectations towards the ideology as such. First and foremost there are different individuals with different expectations, which to some extent represent the stakeholders in the risk practice.

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

Secondly, individuals are substantially different because of differences in knowledge, experiences, and values. A consequence of any ideology within the risk practice is thus that it privileges control at someone else's expense [18]. In the literature, this is normally conceptualized as lack of emancipation [6]. An important source to prior research on emancipation in organizations is [7], who suggest that an orientation towards mutual understanding is required to achieve emancipation. It is however rational to assume that various interpretations of emancipation emerge as different discourses of the risk practice take hold. While the intentionality with risk programs in organizations may be for the good of every employee, the outcome may not be as straightforward. This falls back on situations where risk management is seen as a tool rather than an empowering mechanism for employees to reach their full potential as responsible actors. Whereas a tool view reinforces the risk agendas produced by managers, sharing risk conceptions among a wider audience of employees is likely to activate greater participation and generate inflow of risk knowledge from individuals [4]. Furthermore Talib and Dhillon in [4] discuss that lack of participation leads to alienation, which is the result of being isolated from decision processes. A root cause is that organizations often tend to rely on so called key persons, 'experts', safeguarding that effective controls are in place to reduce the risk of breaches [14]. These experts become spokesmen for the selected approach or solution via à priori defined communication channels, which leaves little room for the empowerment of employees. This is indeed problematic as such one-dimensional thinking about risk practice procedures tends to recursively reinforcing narrow scope risk procedures. In such cases, empowerment does not lead to emancipation of employees [6].

We, however, see somewhat different trajectory of emancipation within risk practices; an approach that actively invites employees to co-opt in risk interventions, and thus contribute to create an inclusive risk management environment, to put emancipation into practice [19]. This corresponds to [20], who suggest that individual emancipation can be achieved if the quest for mutual understanding involves an element of transformation. That means, for instance, seeking to articulate and justify the process of risk identification, determining risk prevention methods, and evaluation of those methods. Essentially, this is about the rediscovery of what type of ideals counts as the truth or knowledge in risk management. To that end, socially critical approaches mean being concerned with conditions of human existence, and be sensitive to a broader set of institutional issues [6].

2.3 Critical Social Theory

The focus of critical social theories (CST) is on emancipation of the people through improving the social conditions. The theory applied in information systems research to understand the potential of freeing employees from repressive social and ideological conditions in the organizational context, which in turn empower the employees through realization of their need [21]. This paper is intended to understand various information security risks practices and their orientation towards emancipation, therefore, the use of CST particularly, Habermas's [7] concept of four orientations make reasonable sense.

In the context of information systems development, Habermas' concept of orientation represents a consistent set of attitudes, beliefs, assumptions and intentions which a developer brings to the process of IS change [21]. This paper adapted the concept of orientation in order to capture the underlying values, goals and epistemological underpinnings that drive the information security risks practices. As reference [21] advocated that "orientations thereby capture the process of change as governed by human intentions [ideology] and goals [consequences]." Habermas theory of communicative actions [7] mentioned four orientations that can be employed to understand the existing information security risk practices and their consequence on emancipation. (Adapted from [21]):

(a) Instrumental orientation is concerned with the achieving of given ends (that have been socially predefined), treating everything in the domain as controllable objects. In the context of information security, the orientation treats employee as mere physical objects that can be controlled, for example, imposition of technology-laden security policies.

(b) Strategic orientation is concerned with achieving given ends (that have been socially predefined), treating humans in the domain as independent, conscious agents with a will of their own. In the context of information security, management tries to understand through employee involvement, but tries to formulating a policy that suits in achieving some influential actors' goal. Therefore, as in instrumental orientation the idea of control and manipulation is there.

(c) Communicative orientation is concerned with achieving a common understanding (through

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

conversation and other forms of communication). The focus of this orientation is on creating shared meanings through sense-making. From information security perspective, the whole idea is to get a consensus on the security risks practices. It is implemented through the vehicles of conversation, interpretations, use of examples and metaphors, and other forms of symbolic interaction.

(d) Discursive orientation is concerned with the achieving of clarification and justification of claims by providing reasons and evidence. The main emphasis in the discursive orientation is on argumentation and explanation, clarification, give reasons and other forms of evidence to justify what was said. In the context of information security risk practices, there can be disagreement with security policies that needs to be justified by whosoever has claims. Therefore, only those information security risks practices will be executed that have clarity of structure and arguments, the weight of evidence, and the validity.

The framework depicted in the figure 1 synthesizes two perspectives, such as ideology of information security risk practices, and consequences of these practices to four orientations of critical social theory. The framework further discusses in section 3 to illustrate the existing information security risk practices and its implications on emancipation.

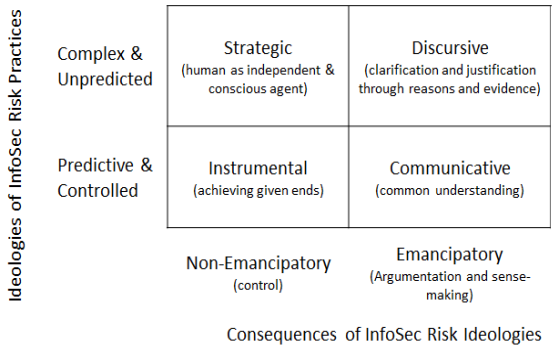

Figure 1. A critical social theory (CST) based framework to analyze information risk practices

3. CST based Analysis of InfoSec risk practices

3.1 Instrumental

An instrumental approach to information security risk practices typically examines risk with a variance methodology. This approach treats the information security risk as a dependent variable and explains it as a function of independent variables. The nature of the instrumental approach is that everything operating within the risk practice is neutral and well behaved. It is assumed that when a certain risk procedure has been subjected implementation by the risk management (the dominant larger unit) it will immediately be adopted independently across organizational entities by the employees (the submissive smaller unit). The central idea is that risk factors are homogeneous and operate evenly across the entire organization, and that they can be linked together to visualize the whole chain of risk factors. The risk management can thus provide evidence that the controlled risk practice is a fully functioning operation. However, the downside of the instrumental approach is its lack of sensitivity to changes in the risk practice procedures, and vice versa its preoccupation with the observable events that comes from assuming the risk practice being predictable and stable [2].

Under the flag of control, one stream in the risk literature has shown the usefulness of formal methods, such as risk analysis [22]. The problem is that the use of these methods assumes a given reality and a known environment. There is, however, a chain of critique in the literature, arguing that environments change quickly and therefore organizational and human issues should be an integral part of the information security risk practice [2, 11, 23-25]. The issue is thus not whether any risk approach is qualitative or quantitative in nature, but rather whether they leave room for including employees in the risk value assessment. However, this is exactly the problem with the instrumental perspective, it looks for all possible mechanisms and combinations that optimize the risk practice with regards to the á priori defined requirements.

3.2 Communicative

When the risk practice is characterized as communicative it could lead to emancipated employees, but it requires a process of sense-making. The source of sense-making can be traced back to the 1960s and 1970s and the theoretical advancement in organizational behavior that acknowledged variants of structuralism in which human actions are observed as the result of embedded structural conditions [26, 27] [28, 29]. This seminal work characterizes sense-making as a cognitive process, including commitment, capacity, and expectations, and assumes that reliance on cues and ongoing experience drives the process [30]. Recent research in

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

information security, however, advocates individual behavior as a critical component in the information security risk practice. For instance, [31] argue for the necessity of explicit and continuous communication processes in addition to security training processes in order to improve security policy compliance. In a similar vein, [32] suggest that individuals intention to comply with managerial regulations to some extent depend upon the external cues within the informal learning environment of an organization. In terms of emancipation, external cues, such as, the offering of constructive feedback to employees is likely to shape shared understanding within the risk practice. Some key items that contribute to shared understanding are, the differentiation of risk activities for better match with different organizational functions demand; reduce dependencies between organizational functions for lessening the burden of coordination.

3.3 Strategic

The concept of strategic management has for several decades influenced organizations in their various management-in-action approaches. It has also intrigued scholars in information systems research as well as information security research e.g. [13, 33-38] to study how organizations develop instruments to cope with complex environments. These instruments are often supported by perceived control over external factors, and include measures that are used for quantifying risk factors. The strategic dimension reflects the need for coordination and co-operation between different stakeholders and organizational functions [39].

While this perspective open up for inclusion of various stakeholders to ingest subjective opinions, risk management rarely absorb those opinions and translate them into an integrated risk practice. One major reason is the perpetuation of risk management ideals that view the risk practice as heterogenic – an idealized abstraction - that continuous to influence research in the area e.g. [10]. Underpinning the ideal is the problem with access to risk data as real security risk events are difficult to measure, and therefore risk management relies on calculations. The reference [10] notes that these calculations tend to be reviewed only by experts in the area for reasonableness. To that end, risk management creates a narrative of progress because it holds an optimistic hope that the organization is able to address risk in a universal manner. It is, however, in terms of emancipation not a successful approach because employees are still treated as objects.

3.4 Discursive

The challenge with a risk ideology to take hold in the entire organization is that of communicating the rational behind [40]. Seeking to transit from viewing the risk practice as an objective reality to an arena of debate with opportunities to influence in what ways risk ideology should shape the risk practice [9], requires discursive dialogue between stakeholders. By drawing on Habermas's validity claims, Stahl in [8] identify three types of claims: Truth, Rightness/Legitimacy, and Authenticity/Sincerity in his critical discursive analysis to identify ideological claims. In the best of worlds, this would lead to viewing the security risk practice as socially conditioned. Hirschheim et al. [21] suggest that new discursive processes are needed to understand the relationship between social action and technology. In terms of emancipation, such processes would compose of reasoning about (Truth) what evidence has been provided to support risk argumentation, (Rightness/Legitimacy) what is missing or suppressed in the discourse, and (Authenticity/Sincerity) do connotative words create false assurance [8]. However, while it is reasonable to believe there will be relevance in the answers to these questions, it's highly possible that justification of a risk practice emerges out of the discovery of hidden contradictions in the answers as well. Contradictions fall back on situations where risk managers and employees have distinct interpretation of a certain information security risk. In contrast to discourse analysis suggested in the literature, an analysis rooted in the tradition of Dialectics may shed light on emerging stances among employees at any level in the organization. Because risk assumptions are subject to change at any time, it is inevitable that contradictory opinions occur. At the analytical level, the resolution of contradictory opinions are in Dialectic thinking approaches a product of – stating a thesis – finding antithesis – and develop a synthesis, representing the point where members of the organization have reached consensus.

4. Discussion

The paper contributed to the existing information security literatures by presenting a theoretical lens to enrich the understanding of infoSec risk practices. In doing so, we utilized four orientation of critical social theory. In addition, different perspectives on ideologies of infoSec risk practices and its consequences on possible emancipation of the practitioners are analyzed. The paper identified that

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

during the process of conducting risk practices the ideology of the risk practices are perceived as either predictable or unpredictable, and controllable or uncontrollable. Likewise, the consequence of the practices can be emancipatory or non-emancipatory. Based on the critical analysis, the paper provides some implications to research and practice.

4.1 Implication to Research

In this paper, we have identified that majority of infoSec literatures argued that the existing InfoSec risk practices perceive that risk is somehow predictable and controllable, which are marked by techno-deterministic or strategic politicization [10]. Consequently, the analysis of its assumptions, implications and the risk practices through which it is acted or enacted is dominated by such perceptions. The practices therefore are more connected with adapting new technologies and making cost/benefit analysis. This has resulted in an imbalanced view of the InfoSec risk practices. In the recent years, as literatures suggest, the perception of the InfoSec risk practices are accompanied by a tendency to conceive it as socio-technical phenomena, and advocate that the research should incorporate organizational, technical, social and cultural issues [2, 3]. Considering the shift of security risks practices toward socio-technical approach, the practices ought to be oriented towards the emancipation rather than imposition.

The present paper also engages with contributions to the research that advanced understanding of infoSec risks practices as emancipation [4]. The paper argues to rethink the concept of the information risks practices as emancipatory by making the practices more discursive through a systematic engagement of the users with regard to implementing the information risk practices.

To that background, we propose that scholars acknowledge a set of alternative approaches in studies of risk practices compared with what has previously dominated the discipline such as checklists. For example, defining or formulating the risk practices is a process of handling subjective data that emerges in interaction with the organizational context. In this situation, critical approach can be one way to identify a variety of contextual factors. These factors are not quantifiable as such, however the justification of risk ideologies provide a richer picture to the formulation of the InfoSec risk practices.

The discussion of the practices as emancipation in light of ideology and consequences add new value to address these dimensions that have been underplayed in the information security literature.

4.2 Implications to Practice

From the perspective of instrumental and strategic orientation, which is mainly focused on control, the InfoSec risk practices concern with meeting defined objectives. There are numerous examples of traditional check-list style risk practices [12]. This orientation focuses more on finding fit between organizational strategy and resources in hand. In these situations, stakeholder with power aspires to justify the need to use the latest technology to enhance control over the employee [5]. However, this kind of practices may lead to decrease in trust between employer and employee, consequently, may deteriorate the information security environment due to various forms of resistance.

From the perspective of communicative orientation, the InfoSec risk practices are based on forming shared understanding. This orientation aims at achieving the inter-subjectivity of the meaning and purpose of the InfoSec risk practices [31]. In this process, everyone contributes, confront, reflect, make rational decisions, and form a shared understanding of the phenomena. Scholars suggested that such understandings can be reached through a variety of modes of inquiry such as direct participation, modeling and experimentation [21]. The InfoSec risk practices that follows communicative approach is more socially feasible and leads to emancipation. Because the infoSec practices are formed through social interaction, the chances of resistance in implementation of such, instances are less than instrumental and strategic orientation.

Finally, the discursive orientation aims at realizing the InfoSec risk practices through logical reasoning and argumentation. For example, the existing infoSec practices can be challenged in terms of its existing ideology. A better understanding of different discourses is required because today's business risk environment doesn't stop at the perimeter of the organization. Organizations have to deal with several technology/business discourses. For instance, ubiquitous computing, cloud computing, inter-organizational information systems, areas that allows humans to operate information technology and automate data transfer in ways that are not that easy to control. Although some skeptic voices pinpoint that 'an emancipated employee of an organization may lose interest in the core business and introduce risk [2, p 143]', but at the same time, an emancipatory approach managing security risks holds

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

great promise. For example, an inclusive agenda of risk management is likely to strengthen employee's organizational commitment, which in turn can leads to responsible behavior and information asset protection.

5. Conclusions

In this paper, we tried to flip the idea of InfoSec risk practices from imposition to emancipation. We argued that employees are not merely objects to instruct, but they are rational being who can contribute to better realization of the InfoSec risk practices in the organization. These issues were underplayed due to the lack of theoretical understanding. Therefore, existing literature failed to explain the nuances of the ideology and consequences of risks practices on emancipation. In this paper, through the two dimensional discussion of risk ideology and its consequences for emancipation, we suggested that critical social theory can provide a multidimensional lens to advance the understanding in this regard. Through critical analysis, the paper provided insights about how the risks practice can be liberated from traditional ideological stances to emancipation instead. Consequently, it can strengthen employee's organizational commitment, which in turn can leads to responsible behavior and information asset protection.

6. References

1. Whitman, M.E. and H. Mattord, *Principles of Information Security*. 2005, Boston: Course Technology
2. Dhillon, G. and J. Backhouse, *Current Directions in IS Security Research: Towards Socio-Organizational perspectives.* Information Systems Journal, 2001. **11**(2): p. 127-153.
3. Siponen, M.T., *A conceptual foundation for organizational information security awareness.* Information Management & Computer Security, 2000. **8**(1): p. 31-41.
4. Talib, Y.A. and G. Dhillon. *Invited Paper: Employee Emancipation and Protection of Information*. in *5th Annual Symposium on Information Assurance (ASIA'10)*. 2010.
5. Drummond, H., *The politics of risk: trials and tribulations of the Taurus project.* Journal of Information Technology, 1996. **11**(4): p. 347-357.
6. Alvesson, M. and H. Willmott, *On the Idea of Emancipation in Management and Organization Studies.* Academy of Management Review, 1992. **17**(3): p. 432-464.
7. Habermas, J., *The Theory of Communicative Action*. 1984, Boston: Beacon Press.
8. Stahl, B.C., *Privacy and security as ideology.* Technology and Society Magazine, IEEE, 2007. **26**(1): p. 35-45.
9. Saravanamuthu, K., *Information technology and ideology.* Journal of Information Technology, 2002. **17**: p. 79-87.
10. Baskerville, R., *Strategic Information Security Risk Management*, in *Information security: policy, processes, and practices*, D.W. STRAUB, S.E. GOODMAN, and R. BASKERVILLE, Editors. 2008, ME Sharpe.
11. Dhillon, G. and G. Torkzadeh, *Value-focused assessment of information system security in organizations.* Information Systems Journal, 2006. **16**(3): p. 293-314.
12. Baskerville, R., *Information systems security design methods: implications for information systems development.* ACM Computing Surveys, 1993. **25**(4): p. 375-414.
13. Straub, D.W. and R.J. Welke, *Coping with systems risk: security planning models for management decision making.* Management Information Systems Quarterly, 1998. **22**: p. 441-470.
14. Spears, J.L. and H. Barki, *User participation in information systems security risk management.* MIS quarterly, 2010. **34**(3): p. 503.
15. Mejias, R.J. *An integrative model of information security awareness for assessing information systems security risk*. in *System Science (HICSS), 2012 45th Hawaii International Conference on*. 2012. IEEE.
16. Hong, K.-S., et al., *An integrated system theory of information security management.* Information Management & Computer Security, 2003. **11**(5): p. 243-248.
17. Doherty, N.F. and H. Fulford, *Do information security policies reduce the incidence of security breaches: an exploratory analysis.* Information Resources Management Journal (IRMJ), 2005. **18**(4): p. 21-39.
18. Booth, K., *Security and emancipation.* Review of International studies, 1991. **17**(4): p. 313-326.
19. Spicer, A., M. Alvesson, and D. Kärreman, *Critical performativity: The unfinished business of critical management studies.* Human relations, 2009. **62**(4): p. 537-560.
20. Myers, M.D. and H.K. Klein, *A set of principles for conducting critical research in information systems.* MIS Quarterly, 2011. **35**(1): p. 17-36.
21. Hirschheim, R., H.K. Klein, and K. Lyytinen, *Exploring the Intellectual Structures of Information Systems Development: A Social Action Rethoric Analysis.* Accounting Management & Information Technology, 1996. **6**(1/2): p. 1-64.
22. Vorster, A. and L. Labuschagne. *A framework for comparing different information security risk analysis methodologies*. in *Proceedings of the*

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.

2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries. 2005. South African Institute for Computer Scientists and Information Technologists.
23. Hitchings, J., *A practical solution to the complex human issues of information security design*, in *Information Systems Security: Facing the Information Society of the 21st Century*, S.K. Katsikas and D. Gritzalis, Editors. 1996, Chapman & Hall: London, UK. p. 3-12.
24. Karyda, M., S. Kokolakis, and E. Kiountouzis, *Content, Context, Process Analysis of IS Security Policy Formation.* Security and Privacy in the Age of Uncertainty, 2003: p. 145-156.
25. Stahl, B.C., M. Shaw, and N.F. Doherty, *Information Systems Security Management: A Critical Research Agenda*, in *Association of Information Systems SIGSEC Workshop on Information Security and Privacy (WISP2008)*2008: Paris.
26. Hermann, C.F., *Some consequences of crisis which limit the viability of organizations. Administrative Science Quarterly*, 1963. **8**: p. 61-82.
27. Powers, W.T., *Behavior: The Control of Perception*. 1973, Ghicago: Aldine.
28. Salancik, G.R., *Commitment and the control of organizational behavior and belief*, in *New Directions in Organizational Behavior*, B.M. Staw and G.R. Salancik, Editors. 1977, St. Glair: Ghicago. p. 1-54.
29. Staw, B.M., *Rationality and justification in organizational life*, in *Research in Organizational Behavior*, L. Gummings and B. Staw, Editors. 1980, JAI Press: Greenwich, GT. p. 45-80.
30. Weick, K.E., *Sensemaking in Organizations*. 1995, Thousand Oaks, CA: Sage.
31. Puhakainen, P. and M. Siponen, *IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY.* MIS Quarterly, 2010. **34**(4): p. 767-793.
32. Warkentin, M., A.C. Johnston, and J. Shropshire, *The influence of the informal social learning environment on information privacy policy compliance efficacy and intention.* Eur J Inf Syst, 2011. **20**(3): p. 267-284.
33. King, W.R., *Strategic planning for management information systems.* MIS quarterly, 1978: p. 27-37.
34. Henderson, J.C. and N. Venkatraman, *Strategic alignment: leveraging information technology for transforming organizations.* IBM systems journal, 1993. **32**(1): p. 4-16.
35. Reich, B.H. and I. Benbasat, *Factors that influence the social dimension of alignment between business and information technology objectives.* Management Information Systems Quarterly, 2000. **24**(1): p. 81-114.
36. Doherty, N.F. and H. Fulford, *Aligning the information security policy with the strategic information systems plan.* Computers & Security, 2006. **25**(1): p. 55-63.
37. LeVeque, V., *Information security: a strategic approach*. 2006: Wiley.
38. Johnston, A.C. and R. Hale, *Improved security through information security governance.* Communications of the ACM, 2009. **52**(1): p. 126-129.
39. Ciborra, C., *De profundis? Deconstructing the concept of strategic alignment.* Scandinavian Jornal of Information Systems, 1997. **9**(1): p. 67-82.
40. Webler, T., *A critical theoretic look at technical risk analysis.* Indistrial Crisis Quarterly, 1992. **6**: p. 23-38.

Authorized licensed use limited to: IEEE Xplore. Downloaded on May 25,2024 at 07:54:39 UTC from IEEE Xplore. Restrictions apply.