Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research

Gurpreet Dhillon, Spyridon Samonas, Ugo Etudo

Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research

Gurpreet Dhillon[1], Spyridon Samonas[2], and Ugo Etudo[1]

[1] Virginia Commonwealth University, Richmond, Virginia, USA
{gdhillon, etudouo}@vcu.edu

[2] California State University Long Beach, Long Beach, California, USA
ssamonas@gmail.com

Abstract. Insider security breaches in organizations have been identified as a pressing problem for academics and practitioners. The literature generally addresses this problem by focusing on the compliance of human behavior to stated policy or the conformance with organizational culture. The cultural stance and resultant activities of organizational insiders are key determinants of information security. However, whilst compliance with security policies and regulations is of great importance, the very structure of human activities that facilitates or hinders such compliance have seldom appeared in the literature. In this paper we present a human activity model that captures different aspects of a security culture. The model elucidates the patterns of behavior in organizations. Applying the model before and after an insider security breach allows us to make salient, critical areas that need attention.

Keywords: Human Activity Model, Insider Threats, Security Culture, Action Design Research.

1 Introduction

Cyber-security threats are not always embedded in the technical infrastructure and operations of the enterprise. Vulnerabilities often arise in the socio-technical space of norms, beliefs and shared models of reality that embody an organization's culture. Developing analytics that incorporate the socio-technical environment of the organization is technically and conceptually complex.

The problem of increased security breaches that are instigated by insiders was first recognized by Denning [1]. In later years, issues related with insider threats were further vocalized through a series of reports by the now defunct Audit Commission in the UK [2], [3], [4] and the Office of Technology Assessment in the US [5]. These studies highlighted the importance and the role played by insiders in perpetuating computer related crimes. Subsequently, several case studies on Barings Bank, Kidder

Peabody and Societe Generale provided evidence that, indeed, the majority of computer related threats reside within organizations (see [6]). Similar evidence has been provided by other research organizations, such as the Computer Security Institute and the CERT division of the Software Engineering Institute at Carnegie Mellon University.

Insider threats mainly refer to the intent of dishonest employees to commit some form of cyber-crime ([10]; [11]). Insiders are capable of disrupting operations, corrupting data, infiltrating sensitive information, or generally compromising an IT system, thereby causing loss or damage ([12]; [13]). As the discussion on the insider threat has evolved considerably over the past decade, so has the very definition of the term 'insider'. Nowadays, it is not only employees who have privileged access to the assets of an organization, but also volunteers, consultants and contractors ([14]; [15]). Access is also given to business partners or fellow members of a strategic alliance, whereas contractors now include employees of a cloud service provider [16]. Hence, a more appropriate alternative to the term 'insider' would be a '(person with) specialized access' [16].

In this paper, we build on the Action Design Research (ADR) concept as proposed by Sein et al. [7] to develop a method for modeling insider security threats. This is undertaken in the context of an online business – Crown Confections. Our model is based on an in-depth understanding of human activities at the workplace and aims to capture both malicious and non-malicious insider threats. We draw on the organizational studies literature to argue that human activities and the *silent messages* that are emanated by individuals can be used as key indicators of insider cyber-security breaches. The application of E. T. Hall's theory of *silent messages* allows us to identify any possible trouble areas with respect to insiders and prioritize cyber-security interventions that could take the form of strategy, training or policy initiatives.

The paper adopts the publication schema for a design science research study as suggested by Gregor and Hevner [41] and is organized as follows. The following section presents a review of the literature on insider threats. The third section examines relevant literature on ADR and outlines the different stages of the method. In the fourth section, we sketch our conceptual basis for developing a human activity model of insider threats at Crown Confections. The fifth section discusses the evaluation of the model. The sixth section paper presents an analysis of the key findings, and the final section includes a summary of our research and its limitations, as well as directions for future research.

2 Literature Review

In the insider threat literature, three main informing bodies can be identified. First, studies that present ever so sophisticated technical approaches to manage insider threats. Second, studies that examine the socio-organizational aspects of insider threats. Third, studies that address different response mechanisms following an insider breach.

In the realm of technical approaches to insider threats, Denning's [1] intrusion-detection model was one of the earlier works to identify attempted system break-ins by

outsiders, as well as abuse by insiders who misuse their privileges. In subsequent years several other similar models have been proposed. For instance, Bowen [6] define a threat model designed to deceive, confuse and confound attackers so that they ultimately abandon the impregnation efforts. This is undertaken by introducing host and network sensors in the architecture. Yet in other cases, honeypot technologies have been proposed as a means to catch insider threats [17]. Insider threats within database systems have also been well researched, where user tasks are mapped to the transactions (see [18]). Generally speaking, the wealth of research in technical approaches to insider threats has focused on restricting access, technical monitoring or, at most, predictive modeling. While important, an exclusive focus on these approaches falls short of providing a holistic perspective in modeling and managing insider threats.

Socio-organizational aspects of insider threats have also been well researched (see [11] and [16]). Although the problem of the insider threat is defined and framed in different ways, and this has resulted in an abundance of approaches, the majority of studies share one thing in common: they treat all insiders as potentially malicious. In this strand of literature, insider threats emanate from available opportunities, work situations and personal factors [10]. Based on monitoring and profiling, this literature primarily addresses issues of policy compliance, sanctions, deterrence and neutralization techniques ([19], [20], [21], [22], [11]). Non-malicious violations are also examined in the insider threat literature [23]. These are typically associated with lapses, errors and mistakes, which are unintentional ([24], [25]). However, more recent studies transcend the distinction between malicious and non-malicious insiders, and consider the insider threat as the departure of human behavior from compliance with security policies, irrespective of whether this is the result of malice or disregard for such policies ([26], [27]).

Research that examines the response to insider threats has largely been related to aspects of compliance with stated policy. As a result, the focus has been more on deterrence and the disciplinary actions that might influence human behavior. Several studies have focused on identifying antecedents to cyber-security compliance. For instance, Vance [28] found that routine activities of employees along with past behavior have a significant effect on compliance behavior. Herath [29] also found social influence to have a strong impact on compliance intention. In a related piece of research, Herath [22] investigated the role of penalties in encouraging positive information security behavior. Their findings indicate that certainty of detection has a positive impact on compliant behavior, whereas severity of punishment has a negative impact on intention to comply.

The lack of consensus in research regarding compliance antecedents has led to an exploration of other factors that might help achieve security compliance as well as ensure an adequate response to insider threats. Prominent amongst these strands of research is the work of Ramachandran [30] on security culture, Hedström [31] on value conflicts, Talib [32] on employee emancipation. Along similar lines, Dhillon et al. [33] suggest the modeling of silent messages as a way of monitoring insider threats. In this paper we heed to these assertions and provide a human activity model for insider threats.

3 Method

ADR helps in developing a prescriptive design artifact in an organizational setting. Typically, ADR is used to address a particular organizational problem through intervention and evaluation. This is followed by the construction and evaluation of the artifact, which would allow for the problem to be solved. Over the years, ADR has been extended to areas such as business intelligence and security breach detection. However, despite its significant contributions to knowledge creation in IS, both in the form of viable artifacts and abstract theoretical constructs [41], the adoption of ADR in computer security research is still underdeveloped. Most notably, Chen et al. [37] adopted ADR to build a model to assess the risk of system downtime in computer networks due to the exploitation of software vulnerabilities. Puhakainen and Siponen [38] developed a theory-based IS security training approach, which they then validated empirically through an action research intervention. Other relevant applications of ADR include the work of Waguespack et al. [39] in the formulation of security design through Thriving Systems Theory, as well as the risk reporting prototype that Beer et al. [40] developed for information-dense IT projects.

Methodologically, any ADR project follows four well-defined stages: **1)** Problem Formulation; **2)** Building, Intervention, and Evaluation (BIE); **3)** Reflection and Learning; **4)** Formalization and Learning. The problem formulation of this research project is presented in the two preceding sections. In building, intervening and evaluating, we define the *alpha* version of the model (see Fig. 1). We then engage in reflection and learning to identify any new requirements that emerge from our exercise. Finally, we formalize our learning and prepare a second iteration of the model, which would lead to the development of the *beta* version of the model. This paper presents an early *alpha* version of our insider cyber-security threat model and identifies possible research directions in further refining the model towards the development of the *beta* version.

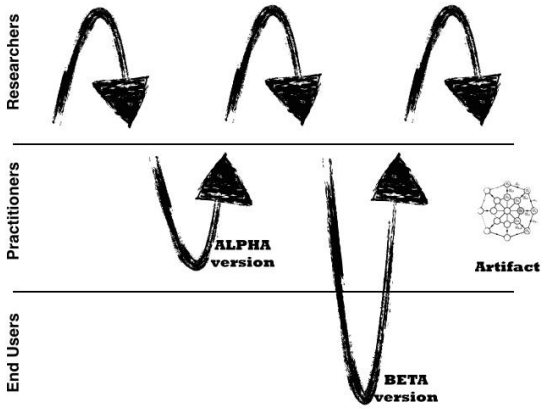

Fig. 1. Action Design Research adopted in this project (based on [7])

The development of an artifact is central to ADR. In our research, we consider artifacts as *ensembles*. As Orlikowski and Iacono [8] note, there are multiple ways in which IT

artifacts come into being. In this research project, we articulate ADR following the 'technology as development process' conception of the artifact [8]. This view of the artifact focuses on the social processes that are related to the design, development and implementation of the technical artifact.

In our research, the artifact in question is the computer-based model for insider cyber-security threats. Using the Orlikowski and Iacono [8] vocabulary, this kind of artifact "examines the role of key stakeholders… [and] how such roles engender conflict, power moves, and symbolic acts." Our computer-based model offers valuable insights into the complex organizational and socio-political processes that are involved in the formulation and implementation of cyber-security strategies and policies. Hence, the model of insider threats becomes a management tool for constant monitoring and assessment of threats as these emerge. In due course, the artifact may reshape itself to influence structure of operations and the related business processes (as postulated by [9] among others). Finally, we argue that given an instrument that faithfully measures the constructs of the model as they manifest in the subjects, the responses of individuals are patterned with (and are therefore not independent of) organizational cyber-security rules, best practices, and technical controls. In other words, our instantiation of the human activity model is sensitive to cyber-security rules, best practices, and technical controls.

4 Artifact Description

To develop our insider threat model, we draw on a conceptual framework that is based on Hall's theory of *silent messages*. Hall [34] argues that silent messages are emanated via human activity interactions, such as language, greeting protocol, gender and status roles, and these get manifested at three levels – *formal*, *informal* and *technical*. In this paper, we argue that an understanding of these cultural streams at the *formal*, *informal* and *technical* levels can be critical for the defense of the organization against insider threats, and should, therefore, be assessed on a regular basis. In our human activity model for insider threats, there are two concepts that need elucidation. First, the Primary Message System (PMS) and cultural streams as proposed by Hall [34]. Second, the manifestation of these cultural streams in terms of *formal*, *informal* and *technical*. These are discussed below.

Hall's [34] taxonomy of behavioral patterns allows us to capture, at a moment in time, the attitudes of employees on matters of security. Each application of the taxonomy generates a panel of data allowing for analyses of changes in organizational security culture over time and between events of interest. In this paper we provide an example of how our adaptation of Hall's [34] taxonomy of behavioral patterns allows us to monitor and interpret the change in attitudes of different employees before and after the occurrence of a security breach. In his intercultural communication theory, Hall [34] argues that "no culture has devised a means for talking without highlighting some things at the expense of other things." Put another way, cultures demonstrate their idiosyncrasies in observable ways. He attempts to unearth different aspects of human behavior that are taken for granted and are often ignored by classifying them into

streams that interact with each other – the silent messages. Laying emphasis on the concepts of time and space, Hall identified ten cultural streams that are rooted in physiology and biology. These streams form the primary message system (PMS), which is essentially a map of a wide variety of cultural and behavioral manifestations. A brief summary of each of the cultural streams is presented below:

- **Interactional (Int):** Speech is one of the most elaborate forms of interaction, and it is reinforced by the tone, voice and gesture. Interaction lies at the hub of the "universe of culture", and hence, every social action grows from it.
- **Organizational (Org):** Refers to the complexity of associations. Hall uses the analogy of bodies of complex organisms as being societies of cells. In his view, association begins when two cells join.
- **Economic (Eco):** Subsistence relates to the physical livelihood, income and work.
- **Gender (Gen):** Refers to the cultural differentiation of sexes and their interactions and associations.
- **Territoriality (Ter):** Refers to the division of space in everyday life, and ownership.
- **Temporality (Tem):** Refers to the division of time and sequencing.
- **Instructional (Ins):** Refers to a basic activity of life that includes learning and teaching. According to Hall, culture is shared behavior that is acquired, and not taught.
- **Recreational (Rec):** Refers to fun and recreation as part of work and occupation. However, this stream also captures competitive human behavior.
- **Protective (Pro):** Defense is a key element of any culture. Different cultures have developed different defense principles and mechanisms. The Protective stream is closely related to the Recreational stream since humor is often used as an instrument to hide or protect vulnerabilities.
- **Exploitational (Exp)**: Hall draws an analogy with the living systems to highlight the importance of evolutionary adaptation to "specialized environment conditions." By extension, the Exploitational stream represents the sophistication in the use of tools, techniques, materials and skills in a competitive and changing environment.

Hall [34] also argues that culture operates at three distinct levels, which are in a state of constant interaction: *formal*, *informal* and *technical*. His theory of culture is, essentially, a theory of change. Formal beliefs shape informal adaptations in behavior; and these, in turn, lead to technical analysis. Each of the ten streams is further broken down into *formal*, *informal* and *technical* to represent the different modes of behavior.

For each impact of the cultural stream at the three levels, we developed an emergent scenario. Each scenario took the form of a statement with a 5-point Likert scale to assess how members of the organization feel about the given situation (refer to Table 1).

5 Evaluation

In our research, we have employed our artifact to undertake an assessment of insider threats at a small, fledgling business. Crown Confections offers an assortment of confections for online or phone-in purchase. Customers have the option of phoning-in

their orders or purchasing their pastries from Crown's website. Crown accepts credit card payments and uses PayPal's commercial suite to process these payments in a secure manner. The Crown staff consists of 20 individuals. The company wanted to develop a mechanism for monitoring insider threats. As researchers, we proposed the use of silent message theory to eventually develop an artifact in the form of a dashboard. It was agreed that the researchers would work with the Crown Confections employees to first develop an *alpha* version, which would then lead to the development of a *beta* version following evaluation and feedback from the end users. In this paper we are sharing the model as it has been shaped in the *alpha* version [7].

For the purposes of our research, we administered the human activity model presented here to the Crown Confections staff twice – once prior to the breach, and again after the breach. The breach included a spear-phishing and a brute force attack that compromised admin and user credentials. All members of the company provided usable responses. Our aim in administering the instrument at Crown Confections is to illustrate its ability to capture nuanced cultural aspects of an organization with respect to the attitudes, behaviors, and perceptions of its members concerning cyber-security.

Given the formative evaluation of the artifact during the *alpha*-cycle, we conducted multiple rounds of semi-formal interviews with organizational members to give them the opportunity to share their experience and shape different aspects of the instrument. This feedback was invaluable as it helped us review key features of the instrument, such as the content and phrasing of certain questions. Alongside areas of improvement, organizational members praised the fact that the questions comprising the instrument touch upon aspects of cyber-security that are often overlooked in typical questionnaires of cyber-security risk assessment. For instance, organizational members highlighted the importance of examining issues of gender or the financial motivation of employees with respect to cyber-security. Furthermore, organizational members also agreed that regular monitoring of the instrument could pinpoint actionable insights on how to improve different aspects of cyber-security across the organization – which is our main research goal in this project. Hence, considering the application of the instrument in Crown Confections, it appears that the *alpha* version represents an insightful canvas for the examination of cyber-security as a diverse and granular socio-technical concept in contemporary organizations.

6 Discussion

The results of our artifact can provide useful visualizations for managers and executives who are interested in 'soft' aspects of cyber-security. Table 2 is a heat map that represents graphically the spectrum of positive and negative changes that were recorded in the post-breach perception of employees in relation to cyber-security. Positive changes indicate a move that is directed towards the high end of our Likert scale ('strongly agree'), whereas negative changes indicate a move in the opposite direction.

	Int	Org	Eco	Gen	Ter	Tem	Ins	Rec	Pro	Exp
Formal	The tone used in communications affects my understanding of information security	My superiors provide comprehensive rules on security issues	I feel that I get the right compensation for the quality and dedication I put in my work	I consider a formal explication of gender issues to be important with respect to cyber security	I welcome suggestions from security professionals which may change the way my Department or work group operates	I prioritize security related tasks over other day-to-day tasks	I value the mentorship of senior colleagues regarding security and its interaction with my daily tasks	Cyber-security is fun and enjoyable	I believe that everyone in my organization knows about cyber-security	I require a high degree of competence in security as it pertains to my job functions
Informal	When faced with security warnings (for example a notice from an antivirus program that a download poses security risks), I always alter my behavior accordingly	My superiors casually stress the significance of rules on security issues	Money is my primary motivator with respect to work	I respect gender issues when dealing with cyber security issues	I welcome suggestions from security professionals, which may change the way I do my job	I actively follow my own schedule for performing security related tasks, such as changing my password, scanning my machine for viruses etc	I learn a lot about security issues by observing my peers	I joke about publicized cyber-security mishaps	I am aware and appreciative of the importance of cyber-security	I take advantage of the security resources available to me towards improving my cyber-security competence
Technical	I understand the jargon used in information security communications	My superiors technically explain security rules and issues	The decision to undertake work related activities is a function of how much I get paid	I believe that the appearance of men and women working in technical aspects of security are consistent with their proficiencies	I am comfortable with discrepancies between actual and formal job descriptions, which have implications for security	I appreciate when security related tasks are being set out and enforced on a predetermined periodic basis	I understand the importance and relevance of information security training curricula	Cyber-security games enhance my understanding of cyber-security	I understand that technical security of systems is of utmost important for ensuring complete protection	I have developed routines and techniques for dealing with equivocal situations regarding cyber-security

Table 1. Framework depicting human activity interactions

The different shades of green and white account for the different levels of gradation between the most positive and most negative changes. In Table 2, the positive changes are depicted with dark color accents, whereas the negative changes are depicted with white color accents. Shades in between indicate that no change or minor changes (positive or negative).

	Int	**Org**	**Eco**	**Gen**	**Ter**	**Tem**	**Ins**	**Rec**	**Pro**	**Exp**
F	0.85	-0.5	-0.3	-0.4	1.45	1.45	-0.25	-0.75	-0.55	1.4
I	0.95	-1.55	0.15	0.05	0	0	1.25	-0.35	0.75	0.25
T	-0.7	-0.4	0.05	0.4	-0.65	0.75	1.4	-0.15	1	0.4

Table 2. Heat map of human activity interactions

In terms of formalizing our learning, the analysis from the heat map can be represented graphically in the form of a radar map (see Fig. 2). The graphic representation shows how silent messages and attitudes of individuals change following a breach. Even without the occurrence of a breach, the radar maps can form the basis of an insider threat analytics dashboard that benchmarks and monitors different aspects of cyber-security culture. In this way, the model can help us build the cyber-security culture profile of a given organization.

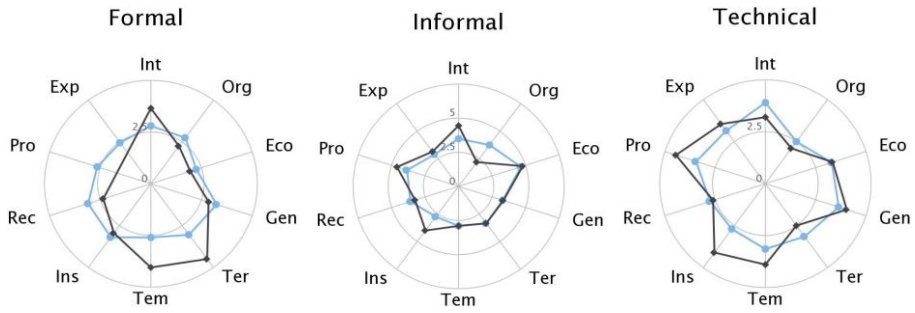

Fig. 2. Radar maps showing pre and post breach scenarios (blue line represents pre-breach situation and black line represents post breach).

In the following subsection, we will discuss a small number (three) of cases where a change in the perception of cyber-security has been recorded in our study.

6.1 Formal layer

At the *formal* layer, we noticed a positive change in the Territorial stream, which examines how employees welcome suggestions from security professionals, which may change the way their Department or work group operates. A positive change shows

higher agreement rates with the statement that comprises this cell, and it is, in fact, a reasonable reaction to a security breach. Following the breach, there may be an increasing need for openness as organizational members seek to share better security practices and get answers from others with more knowledge. However, an opposite reaction, namely a decreased rate of agreement with the statement, could also be seen as an expected outcome. The insider breach could cause organizational members to isolate themselves in small clusters that do not communicate with each other, or prevent them from reaching out to colleagues to openly discuss cyber-security related issues altogether. Similar effects have been noted in the literature with regards to the moral disengagement that security-related stress seems to produce D'Arcy [47]. This type of organizational stress triggers an "emotion-focused coping response in the form of moral disengagement from [information security policy] ISP violations, which in turn increases one's susceptibility to this behavior" [47, p. 285]. Stress that stems from work overload, complexity and uncertainty in response to a security breach could activate said coping mechanisms and provide the basis for the rationalization of non-compliant security behavior.

6.2 Informal layer

At the informal layer, the Instructional stream refers to how receptive employees are to learning from peers. As the security breach represents a moment of organizational crisis, organizational members increasingly seek help from their peers in order to mitigate difficulties associated with navigating the new, equivocal organizational situation. This would be particularly true in the case where there is a lack of a structured and well-prepared security incident response [49].

6.3 Technical layer

The Interactional stream of the technical layer refers to the understanding of technical jargon in cyber-security issues and communications. Following the breach, there seems to be less agreement with the reference statement of this cell, which is a plausible outcome. A negative change indicates that some employees may feel challenged with the technical jargon associated with a security breach. Despite the increasing investment in cyber-security training and education, organizational members that occupy non-technical posts are not required to use this technical jargon in their day-to-day work. This means that it may be more difficult for them to understand the technical terminology and the details of how a security breach came about.

7 Conclusions

We have examined here the efficacy of a human activity model in providing insights to security culture where this efficacy can, in a sense be characterized as the sensitivity of the human activity model to changes in security culture. We highlight this sensitivity by examining pre and post breach instantiations of the model and the ensuing changes. We do this for a single organization. Naturally, generalizability of these findings to

other organizational settings becomes "problematic." We argue here that this taken-as-given conception of generalization is inappropriate in this case. We have applied a theory (i.e. Hall's [34] human activity model) in a setting that is different from the one in which it was developed. Our findings as discussed in section 5 demonstrate that our application of the theory is valid in our setting. This work is an example of type TE generalization – generalizing from theory to description Lee and Baskerville [43]. Lee and Baskerville write of this form of generalization: "researchers are interested not only in pure or basic research – the development, testing and confirmation of theories – but also in the utility of their theories in the actual business settings of executives, managers, consultants and other practitioners." By applying the human activity model in this setting we demonstrate its ability to be generalized to different settings and provide evidence consistent with its theoretical assertions.

There has been a limited amount of research that focuses on pre- and post-breach attitudinal changes. Berezina [35] undertook a study of hotel guest perceptions following a breach and found changes in perceived service quality, satisfaction and likelihood of recommending a hotel. Similarly, Rosoff [36] conducted a behavioral experiment to explore individual response to cyber-crimes. The results suggest differences in messages that individuals exhibit following a breach. The Rosoff [36] study was an experimental design, which covered predefined scenarios. In one scenario, Rosoff [36] explored if attack characteristics and attack mode had any influence of victim's behavior following a breach. In the second scenario, they assessed if the motivation of the attacker and the resolution of the breach had any impact on the behavior of the victim.

While studies such as those of Rosoff [36] and Berezina [35] do shed some light on the manner in which breaches manifest and how individual behavior changes or how victims respond, they fall short of providing an ongoing assessment of the cyber-security situation. Our research project addresses this gap in the literature by presenting a proof-of-concept demonstration of a human activity model for insider cyber-security threats that considers the perceptions of insiders prior and after a security breach.

Future research will be concerned with the development of a *beta* version of our model. A more mature version of the instrument could be administered across different organizations and industries to get a more informed understanding of the granularity of cyber-security as a socio-technical concept. Different research contexts and organizational settings may result in different iterations of the instrument. Although Crown Confections helped researchers gather sufficient feedback on the design and functionality of the instrument, a larger organization could provide a more challenging research setting with a larger number of responses, and perhaps more contradictory responses and feedback that would lead to more fine-detailed iterations of the model.

References

1. Denning, D.E., An intrusion-detection model. *IEEE Transactions on Software Engineering*, 1987. **SE-13**(February): p. 222-232.
2. Audit Commission, *Losing an empire, finding a role*. 1989, London: HMSO.

3. Audit Commission, *Survey of computer fraud & abuse*, 1990, The Audit Commission for Local Authorities and the National Health Service in England and Wales.
4. Audit Commission, *Opportunity makes a thief. Analysis of computer abuse*, 1994, The Audit Commission for Local Authorities and the National Health Service in England and Wales.
5. Office of Technology Assessment, *Information security and privacy in network environments*. 1994: US Government Publication.
6. Bowen, B.M., et al., Designing host and network sensors to mitigate the insider threat, *IEEE Security & Privacy*, 2009. **7**(6): p. 22-29.
7. Sein, M., et al., Action design research. *MIS Quarterly*, 2011. **35**(1): p. 37-56.
8. Orlikowski, W.J. and C.S. Iacono, Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information systems research*, 2001. **12**(2): p. 121-134.
9. Jones, M.R. and H. Karsten, Gidden's Structuration Theory and Information Systems Research. *MIS Quarterly*, 2008. **32**: p. 127-157.
10. Dhillon, G. and S. Moores, Computer Crimes: theorizing about the enemy within. *Computers & Security*, 2001. **20**(8): p. 715-723.
11. Warkentin, M.E. and R. Willison, Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 2009. **18**(2): p. 101-105.
12. Cappelli, D.M., et al. *Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1*. 2009.
13. Cummings, A., et al. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (Technical Report CMU/SEI-2012-SR-004)*. 2012.
14. Brancik, K., *Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks*. 2007: Taylor & Francis.
15. Ponemon Institute, *Risk of Insider Fraud: Second Annual Study*. 2013.
16. Hartel, P.H., M. Junger, and R.J. Wieringa Cyber-crime Science = Crime Science + Information Security. Technical Report TR-CTIT-10-34, CTIT, University of Twente, Oct 2010. http://eprints.eemcs.utwente.nl/18500/.
17. Spitzner, L. Honeypots: Catching the insider threat. In: *Proceedings of 19th Annual Computer Security Applications Conference*, Las Vegas, NV, USA*:* IEEE, 2003, p. 170–179.
18. Chagarlamudi, M., B. Panda, and Y. Hu. Insider Threat in Database Systems: Preventing Malicious Users' Activities in Databases. In *Sixth International Conference on Information Technology: New Generations, 2009. ITNG'09*. Las Vegas, NV, USA: IEEE, 2009, p. 1616 - 1620.
19. Boss, S.R., et al., If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, 2009. **18**(2): p. 151-164.
20. Bulgurcu, B., H. Cavusoglu, and I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 2010. **34**(3): p. 523-548.

21. D'Arcy, J., A. Hovav, and D. Galletta, User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 2009. **20**(1): p. 79-98.
22. Herath, T. and H.R. Rao, Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 2009. **47**(2): p. 154-165.
23. Guo, K.H., et al., Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*, 2011. **28**(2): p. 203-236.
24. Reason, J., Achieving a safe culture: theory and practice. *Work & Stress*, 1998. **12**(3): p. 293-306.
25. Reason, J.T., *The human contribution: unsafe acts, accidents and heroic recoveries*. 2008, Farnham, England; Burlington, VT: Ashgate. x, 295 p.
26. Greitzer, F.L. and D.A. Frincke, Combining Traditional Cyber-security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation, In C.W. Probst, et al. (eds.) *Insider Threats in Cyber-security - Advances in Information Security, 49*: Springer US, 2010, p. 85-113.
27. Hoyer, S., et al. Fraud Prediction and the Human Factor: An Approach to Include Human Behavior in an Automated Fraud Audit. In *45th Hawaii International Conference on System Sciences Proceedings (HICSS),* Grand Wailea, Maui, HI, USA: IEEE Computer Society, 2012, p. 2382-2391.
28. Vance, A., M. Siponen, and S. Pahnila, Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 2012. **49**(3): p. 190-198.
29. Herath, T. and H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 2009. **18**(2): p. 106-125.
30. Ramachandran, S., et al., Variations in Information Security Cultures across Professions: A qualitative study. *Communications of the Association for Information Systems*, 2013. **33**: p. 163-204
31. Hedström, K., et al., Value conflicts for information security management. *The Journal of Strategic Information Systems*, 2011. **20**(4): p. 373-384.
32. Talib, Y.A. and G. Dhillon. Invited Paper: Employee Emancipation and Protection of Information. In *5th Annual Symposium on Information Assurance (ASIA'10)*. 2010.
33. Dhillon, G. and R. Chowdhuri, Organizational Transformation and Information Security Culture: A Telecom Case Study, In S. Jajodia et al. (eds.), *ICT Systems Security and Privacy Protection*: Springer, 2014, p. 431-437.
34. Hall, E.T., *The silent language*. 2nd ed. 1959, New York: Anchor Books.
35. Berezina, K., et al., The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, 2012. **24**(7): p. 991-1010.
36. Rosoff, H., J. Cui, and R. John. Behavioral Experiments Exploring Victims' Response to Cyber-based Financial Fraud and Identity Theft Scenario

Simulations. In *Tenth Symposium on Usable Privacy and Security (SOUPS)*, Menlo Park, CA, USA: USENIX Association, 2014, p. 175-186.
37. Chen, P.-Y., Kataria, G., and Krishnan, R., Correlated Failures, Diversification, and Information Security Risk Management, *MIS Quarterly*, 2011. **35**(2): pp. 397-422.
38. Puhakainen, P., and Siponen, M., Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, *MIS Quarterly*, 2010. **34**(4): pp. 757-778.
39. Waguespack, L. J., Yates, D. J., & Schiano, W. T., Towards a Design Theory for Trustworthy Information Systems. In *47th Hawaii International Conference on System Sciences (HICSS)*, 2014. pp. 3707-3716.
40. Beer, M., Meier, M.C., Mosig, B. and Probst, F., A Prototype for Information-Dense IT Project Risk Reporting: An Action Design Research Approach. In 47th Hawaii International Conference on System Sciences (HICSS), 2014. pp. 3657-3666.
41. Gregor, S. and Hevner, A.R., Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, 2013. **37**(2): pp. 337-355.
42. Hevner, A., March, S., Park, J., and Ram, S., Design Science in Information Systems Research. *MIS Quarterly*, 2004. **28**(1):, pp. 75-105.
43. Lee, A., and Baskerville, R. L., Generalizing Generalizability in Information Systems Research, *Information Systems Research*, 2003. **14**(3): pp. 221-243.
44. Markus, M. L., Power, Politics, and MIS Implementation, *Communications of the ACM*, 1983. **26**(6): pp. 430-444.
45. O'Connor, C. Target CEO Gregg Steinhafel Resigns In Data Breach Fallout, Forbes, May 5, 2014. In http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/#25ca02fa6e61, last accessed on March 12, 2016.
46. Hu, Q., Dinev, T., Hart, P. and Cooke, D., Managing employee compliance with information security policies: the critical role of top management and organizational culture, *Decision Sciences*, 2012. **43**(4): pp. 615-660.
47. D'Arcy, J., Herath, T. and Shoss, M.K., Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems*, 2014. **31**(2): pp. 285-318.
48. Ruefle, R., Dorofee, A., Mundie, D., Householder, A.D., Murray, M. and Perl, S.J.. Computer security incident response team development and evolution. *Security & Privacy, IEEE*, 2014. **12**(5): pp.16-26.
49. Plester, B., Execution of a Joke: Types and Functions of Humour. In *The Complexity of Workplace Humour: Laughter, Jokers and the Dark Side of Humour*, 2016. Springer International Publishing, pp. 39-66.