Working Paper No. 1

Leaking Confidential Information by Non-Malicious User Behavior in Enterprise Systems – An Empirical Study

Frank Hadasch[(1)], Alexander Maedche[(1,2)] and Benjamin Mueller[(1)],

(1) Chair of Information Systems IV (ERIS), Business School, University of Mannheim
{hadasch,maedche,mueller}@eris.uni-mannheim.de
http://eris.bwl.uni-mannheim.de

(2) Institute of Enterprise Systems University of Mannheim
maedche@uni-mannheim.de
http://ines.uni-mannheim.de

LEAKING CONFIDENTIAL INFORMATION BY NON-MALICIOUS USER BEHAVIOR IN ENTERPRISE SYSTEMS - AN EMPIRICAL STUDY

Research-in-Progress

Abstract

Information assets of enterprises are vulnerable to theft and need to be protected to avoid information leakage to unauthorized parties. Technical countermeasures to protect confidential information fall to short, as information leaks can emerge from non-malicious behavior of users while they execute a business process in an Enterprise System. Our study investigates characteristics of security incidents in which users are authorized to access information in a secure domain, but cause information flow into an unsecure domain without any malicious objectives. We use a qualitative research method to explore the context, activities, and behaviors that lead to leakage of confidential information. We will collect empirical data in three sequential phases with interviews. In the first phase informants will be security consultants for Enterprise Systems, in the second phase company's security managers will be interviewed and finally narratives are collected from end users. We employ the grounded theory approach to analyze the data and formulate the theoretical framework. The findings are expected to provide insights into the sources of confidential information leakage caused by non-malicious user behavior in Enterprise Systems.

Keywords: Computer Security, Security Incident, Data Leakage, Enterprise System.

1 INTRODUCTION

Enterprises are increasingly concerned about the protection of their confidential information since these represent valuable assets, which provide strategic advantages, contribute to financial strategies, or can impact public safety. Unfortunately, these assets are vulnerable to theft. Company's reputation and value can be negatively influenced by stolen data through security breaches (Campbell et al. 2003; Gordon and Loeb 2002). The financial impact of data breaches on companies is extensive: according to the investigation of U.S. Secret Service in 2010, data breaches caused a direct fraud loss of $500 million and through arrests of criminals additional losses of approximately $7 billion were prevented (Baker et al. 2011). The security incidents, the actors, and causes are diverse, moreover the complexity of enterprise structures is increasing. Major challenges come with the information age's structural changes: in classical enterprises internal employees are physically and digitally protected through "walls" while processing confidential information. However, by the extensive use of information and communication technologies structures evolve towards networked virtual enterprises (Martinez et al. 2001). In such a setting external partners, expanded company networks, and employees' mobile devices blur boundaries. This trend intensifies the problem to control information flow across different domains and cannot be addressed with technological countermeasures solely. Along with recent academic literature our work acknowledges that security is not achieved only by secure programming, security models, or security tools. There is a need to draw attention to individual users as they "represent the weak link in security" (Anderson and Agarwal 2010, p. 614).

Acknowledging the importance of individual user's behavior to improve the overall security in a socio-technical system (A. Lee 1999), latest Information System (IS) security literature investigates behavioral aspects and the role humans have as one element of the entire system to shape a secure environment for corporate information assets. A variety of recent research papers discuss the application of IS security policies, used to define unacceptable IS resource usage, as a promising instrument to reduce

vulnerabilities caused by human behavior. Results of these publications improved the understanding of the behavioral intention of users to comply with security policies in an organization context, by performing protective measures (Dinev and Hu 2007; Liang and Xue 2010), following security guidelines (Bulgurcu et al. 2010; Herath and Rao 2009; Pahnila et al. 2007; Siponen and Vance 2010), and avoiding misuse of IS resources (D'Arcy et al. 2009; Johnston and Warkentin 2010). The investigations employ different perspectives: protection motivation theory (Herath and Rao 2009; Johnston and Warkentin 2010; Lee and Larsen 2009; Woon et al. 2005), deterrence theory (Kankanhalli et al. 2003; Straub 1990), and neutralization theory (Siponen and Vance 2010). Results consistently suggest that compliance with security policies comes with a price: hindrance to the day-to-day job impacts the security motivation of users (Bulgurcu et al. 2010; Herath and Rao 2009), and to an extreme humans justify violations of policies as the only way to solve the dilemma to get the work done (Siponen and Iivari 2006; Siponen and Vance 2010).

An organization-wide IS security policy as a manifestation of the governing organization's security risk management (Hoo and John 2000; Spears 2006; Wang et al. 2008), changes individual behavior and contributes to security. However, on an operational level, users have to execute a sequence of actions to process data and deliver work results as an actor in a certain business process, while policy-compliance becomes a cost factor (Bulgurcu et al. 2010; Pahnila et al. 2007). A single negligence during the execution of a business process can constitute a potentially dangerous action resulting in a state, where security properties are not fulfilled anymore. As IS security literature acknowledges the human factor for security, there is a lack of exploration of characteristics of security incidents in which vulnerabilities are caused by user behavior within certain business processes.

Our work builds upon the emerging analysis of secure business processes (Cresswell and Hassan 2007; Neubauer et al. 2005; Zo et al. 2010) and the remarks of Spears and Barki (2010, p. 504): "Security controls can be much more effective, if they are aligned to business objectives and users have an understanding of the relative value of information, how information is used within and across business processes, and at what nodes within a process sensitive information is most vulnerable". Our study focuses on users who employ an Enterprise Systems to execute a business process. The objective of this investigation is to explore characteristics of security incidents in which confidential information is leaked in Enterprise Systems. We focus on human-made non-malicious faults during the use of an Enterprise System (Avizienis et al. 2004) to examine "internal threats and vulnerabilities embedded within business processes" (Spears and Barki 2010, p. 506). Our intention is to explore the characteristics of the enterprise context, technological infrastructure, and the security-relevant commonalities of business processes, that may lead to information flow into domains where information should not be. Thus, our study addresses the question: *What are the characteristics of security incidents perceived as severe, in which confidential information in an Enterprise System is leaked and the opportunity for exploitation by an attacker is caused by Enterprise System user's non-malicious behavior?* In our overall study, the answer of this question will be pursued with a qualitative empirical research. This paper is a research-in-progress report on the early stages of our overall research project. In it, we report on our effort to build a sound conceptual and theoretical foundation for our inquiry and the phenomenon of interest. Based on these foundations, we suggest a research strategy to capture empirical data to shed light on individual user behavior in security scenarios.

To do so, this paper proceeds as follows. First, we outline the conceptual background related to information security in Enterprise Systems and then we formulate the research design. Finally, we discuss intended contributions, along with assumed study limitations and opportunities for future research.

2 CONCEPTUAL FOUNDATIONS

To protect confidential information enterprises employ a highly secure system environment – a digital fortress to protect information. It is argued that such systems meet confidentiality requirements through access control and encryption. The assumption is therefore that confidential information is securely stored. However, trusted users interacting with the system have access to extensive amount of data and pose a risk to the overall security, as they can accidentally store information outside of the secure environment while executing a business process. An insider can disclose data, even without any malicious objective whatsoever. Therefore we are interested in the characteristics of security incidents caused by non-malicious actions of users in Enterprise Systems. This chapter presents a brief review of the relevant literature of Enterprise Systems and security.

2.1 Enterprise Systems

In a strict sense Enterprise Systems are a class of packaged software applications, with "large integrated, process-oriented packages designed to meet most needs of organizations including accounting and control, manufacturing and distribution, sales and order entry, human resources, and management reporting" (Strong and Volkoff 2010, p. 731). In a broader sense Enterprise Systems are the technological subsystem in an organization and enable the integration of transaction-oriented data and business processes throughout an organization (Gosain 2004; Markus and Tanis 2000). Consequently, there is a seamless flow of information through the company across various locations, business entities, and business processes (Davenport 1998). Besides the technological perspective there is an institutional and behavioral perspective. Humans interact independently with information systems and become entrenched in ways of thinking as they use technology (Robey et al. 2002). Through the converging expectations of the actor network a greater stability in the work practices of the users emerges. According to Gosain (2004, p. 152) the pattern of usage "become[s] institutionalized and predetermined and form prescriptions for social actions" as a greater stability in work practices arises based on regularities of human-technology interaction (Gosain 2004). To cover both perspectives, we define *Enterprise System as a socio-technical system consisting of a technological subsystem (application software, system software, hardware, and network) and a sociological subsystem (people and organizational structure) in a context of an organization as enabler for technology-supported execution of business processes.*

2.2 Computer Security

To draw on the basics of computer security, the following three main requirements must be met: (1) *confidentiality*, (2) *integrity*, and (3) *availability*. Confidentiality means absence of unauthorized disclosure of information, integrity defines the absence of improper system or data alterations, and availability describes the readiness of systems to deliver correct service (Avizienis et al., 2004). Several mechanisms are used to address these requirements. (1) Access control mechanism ensures data secrecy. Data *objects* are protected through access control to not allow any unauthorized access of *subjects*. Whenever a user tries to access an object, the mechanism checks the right of the user against a set of authorizations. Based on the security policy of the organization the set of authorizations is configured by *administrators*. (2) Data integrity is ensured by the joint mechanism of access control and semantic integrity constraints. In addition to the authorization check the semantic integrity check verifies that the transmitted data is semantically correct and no invalid data constellation is stored. (3) Finally, system readiness and correct service is ensured by recovery mechanism and the concurrency control mechanism to ensure service delivery despite hardware or software failures (Avizienis et al. 2004; Bertino 1998).

Security models are designed to provide concepts for mechanisms that address these requirements. For our study on information flow in Enterprise Systems two main models are highly relevant: *access control* and *information flow control*. Access control models can be differentiated by the employed strategies. These are either based on the owner principle (discretionary access control), system enforced principle (mandatory access control), or task-driven transaction based principle (role based access control). Due to the characteristics of enterprises, business processes require tasks to be executed by groups of users, therefore role based access control is commonly used in EIS (She and Thuraisingham, 2007; Anderson 2008; van de Riet et al. 1998). In theory, information flow control models are described since the 1970s. Denning (1976) introduces for her model lattices to allow information flow between two security classes only in case permitted by an information flow policy. For example this avoids information flow from objects contained in a confidential security class to objects in a non-confidential security class.

However, especially in a practical enterprise context the application of information flow control models is challenged through historically grown and heterogonous systems. Even simple data leak scenarios are technically difficult to tackle as information flow models require own programming languages or redesign of applications to be deployed (Mundada et al. 2011). As extensive technical solutions are difficult and often not implemented exhaustively in enterprises, the flow of confidential information must be controlled also on a human-system interaction. The risk of exploitable data leaks caused by user behavior is elaborated next and touches upon the aspect of attacker behavior to satisfy a comprehensive picture of security incidents.

2.3 Security in Enterprise Systems on Organizational Level

"Information security can be treated as a game between organizations and attackers" (Wang et al. 2008, p. 107). Strategic attackers try to gain unauthorized access to information systems while organizations act as defenders protecting their information assets. To understand the motivation of attackers empirical research in cybercrime resulted in the grouping into "two broad categories: attackers seeking personal gratification – in this case, the motivation could be fame, curiosity, self-esteem, or political antagonism – and attackers looking for monetary gain" (Cremonini and Nizovtsev 2009, p. 242). Recently there is an increasing number of attackers, who are seeking financial gain, act strategically as rational agents, and maximize their cost-benefit function (Cremonini and Nizovtsev 2009; Zhuang et al. 2010). Leveraging a collection of 1,700 security incidents between 2004 and 2010, Baker et al. (2008, 2009, 2010, 2011) conducted four empirical cybercrime forensic studies on data breaches. These reports show a trend towards financially motivated attackers. Based on the data sets of the reporting data forensic units, the United States Secret Service, and the Dutch National High Tech Crime Unit, the majority of attack originators are external sources (Baker et al. 2011). However, the median number of data records compromised per breach is significantly higher for internal threat sources. Statistics from 2008 show that stronger data privileges, grounded in trust towards internals, provide more opportunities: the reported median value is 375,000 data records compromised per breach, if internals were the threat source, compared to 30,000 in case of an external source. Statistics also show that attackers concentrate on information assets that can be turned into cash easily (e.g., payment card data, personal information). However, the price per stolen data record dropped drastically in two years by an average factor of 26. Therefore, attackers adapt and seek for more valuable targets. In 2011 sensitive organizational information assets became more attractive for attackers (Baker et al. 2011). These assets, such as customer data, intellectual property, corporate strategy, and financial records are stored in Enterprise Systems and efforts of attackers are continuously concentrating on these targets.

While attackers are one group in the game, organizations play the role of a defender and apply protective measures to reduce exploitable vulnerabilities. Cremonini and Nizovtsev (2009) analyzed the strategic attacker-defender interactions and conclude that protective actions by organizations prevent security incidents. This occurs by reducing exploitable vulnerabilities; in addition, these protections represent signaling instruments to deter attackers by influencing their decision making process to move towards less protected attack targets.

On the defender side technical countermeasures are used, such as firewalls, access control mechanisms, and virus scanners (Baker et al. 2011; Gordon and Loeb 2002). In addition to technical measures IS security policies can be implemented to reduce vulnerabilities created by human behavior. Individual users represent a security risk while they interact with an Enterprise System (Dhillon and Moores 2001; Siponen 2000). The extent and intensity these policies are enforced in an organization depends on priorities derived from the governing organization's security risk management (Hoo and John 2000; Spears 2006; Wang et al. 2008). "Security risk management […] is a continuous process of identifying and prioritizing IS security risk […]" and includes the "strategies, policies, activities, roles, procedures, and people used to manage security risk" (Spears and Barki 2010, p. 505). Findings suggest that security can be improved on an organizational level with a primarily cognitive process. By involving business users in security risk management, the increased awareness and participation stimulates the effect of including security controls in business processes. On an individual level users can be the weak link in security, but on a group and organizational level they can also be the solution if they participate in security risk management. (Spears and Barki 2010).

2.4 Security Behavior in Enterprise Systems on Individual Level

On an individual level a comprehensive number of studies analyzed user security behavior in a non-work and work environment. A huge variety of theoretical lenses has been used to study these phenomena: *Protection Motivation Theory*, *General Deterrence Theory*, *Theory of Planned Behavior*, *Rational Choice Theory*, and *Neutralization Theory*.

To examine computer user behavior in light of the *Protection Motivation Theory*, a non-work environment is an ideal setting as no organizational regulation in form of an IS security policy is present. Home computer users have to use their own believes to assess the risk towards their information assets. To protect their computer they rely on their perception of the susceptibility and severity of threats. Covering non-work and work environments latest research results show that perceived threat, perceived

effectiveness of safeguards, and self-efficacy positively affect behavioral intention to avoid threats by applying protective measures as home computer user (Anderson and Agarwal 2010) and as employees (Johnston and Warkentin 2010; Liang and Xue 2010; Woon et al. 2005).

In a work environment "security policies contain detailed guidelines for the proper and improper use of organizational IS resources" (D'Arcy et al. 2009, p. 2). According to the prediction of the *General Deterrence Theory* improper use of IS resources by employees can be deterred by providing employees knowledge about unacceptable behavior to increase perceived certainty and severity of punishment. Such a knowledge positively influences their behavioral intentions towards compliant behavior (D'Arcy et al. 2009; Herath and Rao 2009; Pahnila et al. 2007).

Beyond motivational factors rooted in *Protection Motivation Theory* and *General Deterrence Theory* to explain employees' compliance behavior, Bulgurcu et al. (2010) suggest a model with constructs informed by *Theory of Planned Behavior.* Their findings reveal that employees' believes about work impediment leads to the perceived consequence of increased cost of compliance. This perceived consequence interferes with the primary goal of the business. Consequently, there is a negative influence on employees' attitude towards compliant behavior in case they sense that following a security policy results in additional work impediment (Bulgurcu et al. 2010).

Finally, the study of (Siponen and Vance 2010) is informed by research in criminology and utilizes *Neutralization Theory* to explain compliance violations of employees. They find that users excuse actions that lead to violations by employing cognitive neutralization technique. This technique allows them to minimize the perceived harm of their policy violations. To justify malpractice employees argue by drawing back on for example denial of responsibility, denial of injury, defense of necessity, or appeal to higher loyalties (Siponen and Vance 2010; Sykes and Matza 1957).

The extant IS literature on computer security and behavioral aspects of security provides a sound understanding of attacker-defender interaction, attacker behavior, defending strategies, and security policy compliance behavior of users. However, existing literature does not fully provide insights about characteristics of security incidents caused by non-malicious user behavior in Enterprise Systems. For our study the relevant phenomenon of interest are the characteristics of security incidents perceived as severe, where confidential information is leaked. While users interact with the system they can cause non-malicious faults, meaning they do not have the objective to cause harm to the system or data (Avizienis et al. 2004). These faults can cause information flow of sensitive data into an unsecure domain. Our objective is to identify common characteristics of security incidents that can be sorted and classified to security scenarios where commonalities exist across the incidents. To address our research question and examine the phenomenon of interest we suggest the following research design.

3 PROPOSED RESEARCH DESIGN

To address our research question, our study will use a qualitative research method to examine characteristics of security incidents perceived as severe, where confidential information is leaked in Enterprise Systems. The majority of behavioral security literature in the IS field focus on understanding the motivation of individuals to comply with IS security policies. However, we see uncertainty surrounding the understanding of characteristics of security incidents as the interest of our study. Our work will consider the human-system interaction in a business process in the context of an Enterprise System and by qualitative methods we target to gain a rich understanding of the context, activities, and behaviors that lead to leakage of confidential information (Spears and Barki 2010).

In the present study, we will follow an interpretive approach and employ grounded theory as the research method. According to Orlikowski (1993) field studies in real organizations with the objective to derive theory from empirically collected data need a careful examination of the interpretations provided by informants. For our study the security incidents are the unit of analysis and they can have different interpretations for different individuals or groups of individuals. In addition, field research in the area of security incidents and security behavior requires awareness about the sensitivity of the topic. On an organizational level, publicity of security incidents can cause damage in reputation and on an individual level, security incidents can be a consequence of policy violations. Therefore anonymity, individuals' moral and ethical behavior has to be considered. When collecting data for our study, we will consider these reflections to design the data collection instruments carefully and diligently take into account the social construction of data as emerging through subject-researcher interaction (Klein and Myers 1999).

3.1 Data Collection

We will employ a staged research approach in order to collect data relevant to answering our research question. Overall, we intend to conduct a sequential field study to better understand the specific business processes, roles of actors, and behaviors that lead to information flow caused by non-malicious user's behavior. Rich narratives will be the foundation for subsequent examination of groups and categories in the context of confidential information leakage in Enterprise Systems. To collect data, key informants will be identified for a three-phased sequential study. First, we will collect secondary data with semi-structured interviews. The sampling will start with a group of Enterprise Systems security consultants, who have experience and insights in multiple industries and business processes. Through this we intend to gain an understanding of the various incidents and develop an initial classification of scenarios. Second, we will use theoretical sampling based on the identified properties in the first phase. Semi-structured interviews will be conducted with identified informants and documents, which describe technical infrastructure and business processes, will be collected and analyzed. To complete the data triangulation, we will thirdly collect data through structured interviews and observation of end-users working with Enterprise Systems (Myers 2008).

3.2 Data Analysis

We use the coding scheme in grounded theory as the data analysis method. Firstly, we use open coding to identify descriptive codes in the transcribed interviews to create categories. Secondly, we use axial coding to link categories into constructs. Finally we specify correlations among constructs (Orlikowski 1993). This approach will form the basis for our theory development.

4 DISCUSSION

Following the suggestions of latest studies in the area of Management Information Systems, we consider IS security policies as central element in a holistic secure environment. However, we argue that in today's information society secure processing of data in enterprises cannot be achieved by general policies alone. Enterprise Systems need to be designed to compensate user's behavior that poses risk to information assets of companies.

The intended research contributions of our study are an improved understanding of characteristics of data leakage security incidents caused by non-malicious behavior of Enterprise System users. The identified classifications and connections will open a future research avenue to examine behavioral and technical countermeasures to avoid such information leakage. The intended practical contribution can serve as input for improved security design in complex Enterprise Systems. Mechanisms that support users in their decision-making on how to process the company's information assets in distributed software environments will benefit from our study.

As we will collect data through interviews, we will face the following limitations that we accept as a tradeoff to get a rich collection of narratives for the identification of characteristics of security incidents. First, a statistical generalization will not be provided in our study based on the chosen method and the limited sample size. The rational for choosing a non-quantitative method is that we consider the surrounding context as crucial. Social aspects such as security culture and technological infrastructures vary across organizations. We see both as crucial to define the overall security within a business process. Even in case that standard package software is applied, deviations from the standard business process need to be captured as they can have massive impact on vulnerabilities causing security incidents. Second, our interpretive research builds on events that have already transpired. Informants may only vaguely recollect incidents during the interview and might mix these with gained attitudes through interaction with other individuals. The reported and collected data can therefore be a collective viewpoint of others as it has emerged over time (Isabella 1990).

The improved understanding of security incidents and the role of users in these incidents opens future research opportunities. Our qualitative study is the first part of a research stream to design and evaluate dynamic information flow control mechanisms for complex Enterprise Systems. Sometimes the solution is very simple: as shown by Sunshine et al. (2009) changing the message frames to elaborate clearly the risks and consequences of actions, had a significant impact on user's behavior to not continue exposing transmitted to data to leak to an attacker. Motivated by research in the area of human-computer

interaction, we plan future research with an experimental setup to determine how information flow caused by nonmalicious behavior of users can be changed in Enterprise Systems.

References

Anderson, C. L., and Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613 - A15.

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Wiley Publishing.

Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on*, *1*(1), 11 - 33.

Baker, W. H., Goudie, M., Hutton, Alexander, Hylender, C. D., Niemantsverdriet, J., Novak, C., and Sartin, A. B. (2010). *2010 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Baker, W. H., Hutton, Alex, Hylender, C. D., Valentine, J. A., Novak, C., Porter, C., Sartin, A. B., et al. (2009). *2009 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Baker, W. H., Hutton, Alexander, Hylender, C. D., Pamula, J., Porter, C., and Spitler, M. (2011). *2011 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Baker, W. H., Hylender, C. D., and Valentine, J. A. (2008). *2008 Data Breach Investigations Report*. Retrieved from www.verizonbusiness.com/resources/ security/databreachreport.pdf

Bertino, E. (1998). Data security. *Data & Knowledge Engineering*, *25*(1-2), 199 - 216.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523 - A7.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J. Comput. Secur.*, *11*, 431–448.

Cremonini, M., and Nizovtsev, D. (2009). Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers. *Journal of Management Information Systems*, *26*(3), 241 - 274.

Cresswell, A., and Hassan, S. (2007). Organizational Impacts of Cyber Security Provisions: A Sociotechnical Framework. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (p. 98).

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Info. Sys. Research*, *20*, 79–98.

Davenport, T. H. (1998). Putting the enterprise into the enterprise system. *Harvard Bus. Rev.*, *76*, 121–131.

Denning, D. E. (1976). A lattice model of secure information flow. *Commun. ACM*, *19*, 236–243.

Dhillon, G., and Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, *20*(8), 715.

Dinev, T., and Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7).

Gordon, L. A., and Loeb, M. P. (2002). The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, *5*, 438–457.

Gosain, S. (2004). Enterprise Information Systems as Objects and Carriers of Institutional Forces: The New Iron Cage? *Journal of the Association for Information Systems*, *5*(4).

Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106 - 125.

Hoo, S., and John, K. (2000). *How much is enough: a risk management approach to computer security*. Stanford, CA, USA: Stanford University.

Isabella, L. A. (1990). Evolving Interpretations as a Change Unfolds: How Managers Construe Key Organizational Events. *Academy of Management Journal*, *33*(1), 7 - 41.

Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Secuirty Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549 - A4.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139.
Klein, H. K., and Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67 - 93.
Lee, A. (1999). Inaugural Editor's Comments. *MIS Quarterly*, *23*(1), 1.
Lee, Y., and Larsen, K. R. T. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.
Liang, H., and Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394 - 413.
Markus, M. L., and Tanis, C. (2000). The enterprise systems experience-from adoption to success. In R. W. Zmud (Ed.), *Framing the Domains of IT Management: Projecting the Future Through the Past* (p. 173–207). Cincinnati, OH: Pinnaflex Education Resources, Inc.
Martinez, M. T., Fouletier, P., Park, K. H., and Favrel, J. (2001). Virtual enterprise - organisation, evolution and control. *International Journal of Production Economics*, *74*(1-3), 225 - 238.
Mundada, Y., Ramachandran, A., Tariq, M. B., and Feamster, N. (2011). *Practical DataLeakPrevention for LegacyApplications in Enterprise Networks*.
Myers, M. D. (2008). *Qualitative Research in Business & Management*. Sage Publications Ltd.
Neubauer, T., Klemen, M., and Biffl, S. (2005). Business process-based valuation of IT-security. *Proceedings of the seventh international workshop on Economics-driven software engineering research* (p. 1–5).
Orlikowski, W. J. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly*, *17*(3), 309 - 340.
Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (p. 156b).
van de Riet, R., Janssen, W., and de Gruijter, P. (1998). Security moving from database systems to ERP systems. *Database and Expert Systems Applications, 1998. Proceedings. Ninth International Workshop on* (pp. 273 -280).
Robey, D., Ross, J. W., and Boudreau, M.-C. (2002). Learning to Implement Enterprise Systems: An Exploratory Study of the Dialectics of Change. *Journal of Management Information Systems*, *19*(1), 17 - 46.
She, W., and Thuraisingham, B. (2007). Security for Enterprise Resource Planning Systems. *Information Systems Security*, *16*(3), 152 - 163.
Siponen, M. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Inf. Manag. Comput. Security*, *8*(5), 197-209.
Siponen, M., and Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information Systems*, *7*(7), 445 - 472.
Siponen, M., and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487 - A12.
Spears, J. (2006). A Holistic Risk Analysis Method for Identifying Information Security Risks. In P. Dowland, S. Furnell, B. Thuraisingham, and X. Wang (Eds.), *Security Management, Integrity, and Internal Control in Information Systems* (Vol. 193, pp. 185-202). Springer Boston.
Spears, J., and Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, *34*(3), 503 - A5.
Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255-276.
Strong, D. M., and Volkoff, O. (2010). Understanding Organization-Enterprise System Fit: A Path to Theorizing the Information Technology Artifact. *MIS Quarterly*, *34*(4), 731 - 756.
Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. (2009). Crying Wolf: An Empirical Study of SSL Warning Effectiveness. Usenix Security. *Proceedings of the 18th conference on USENIX security symposium*.
Sykes, G. M., and Matza, D. (1957). Techniques of Neutralization: A Theory of Deliniquency. *American Sociological Review*, *22*(6), 664 - 670.
Wang, J., Chaudhury, A., and Rao, H. R. (2008). A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, *19*(1), 106 - 120.
Woon, I., Tan, G.-W., and Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 Proceedings*. Presented at the International Conference on Information Systems.

Zhuang, J., Bier, V. M., and Alagoz, O. (2010). Modeling secrecy and deception in a multiple-period attacker–defender signaling game. *European Journal of Operational Research*, *203*(2), 409 - 418.
Zo, H., Nazareth, D. L., and Jain, H. K. (2010). Security and performance in service-oriented applications: Trading off competing objectives. *Decision Support Systems*, *50*(1), 336 - 346.