Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2018 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-26-2018

Information Systems Betrayal: When Cybersecurity Systems Shift from Agents of Protection to Agents of Harm

Daniel Pienta
Clemson University, dpienta@g.clemson.edu

Jason Thatcher
Clemson University, jthatch@clemson.edu

Heshan Sun
Clemson University, sunh@clemson.edu

Joey George
Iowa State University, jfgeorge@iastate.edu

Information Systems Betrayal: When Cybersecurity Systems Shift from Agents of Protection to Agents of Harm

Research-in-Progress

Daniel Pienta
Clemson University
100 Sirrine Hall, Clemson, SC 29634
dpienta@clemson.edu

Jason Bennett Thatcher
Clemson University
ITU Copenhagen
100 Sirrine Hall, Clemson, SC 29634
jthatch@clemson.edu

Heshan Sun
Clemson University
100 Sirrine Hall, Clemson, SC 29634
sunh@clemson.edu

Joey F. George
Iowa State University
Ames, IA 50011-1350
jfgeorge@iastate.edu

Abstract

Cybersecurity systems provide a unique opportunity of study as they can be used as agents of protection and harm. Practice uses these systems of protection against employees through the use of red team and black hat tactics for perimeter testing as well as invasive, complex monitoring for defense of internal threats. It is important to understand the effects of these actions on end users. This study seeks to understand the effects of these cybersecurity practices on individuals through the perspectives of trust, betrayal, aversion, and resistance. An integrative model is built and employed to understand the formation and consequences of IS betrayal.

Keywords: *Cybersecurity, Betrayal, Violation, Aversion, Resistance, Trust*

Introduction

Organizations invest in cybersecurity systems at growing rates, with worldwide spending estimated to reach $90 billion in 2017 and increase to $133 billion by 2021 (Gartner 2017). By cybersecurity we reference von Solms (2013, p. 101) who defines it as "the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace". Organizations invest in these systems in hopes of detecting and responding to external and internal threats to information security. Traditional approaches to security systems focus on developing preventative systems to keep cybercriminals at bay. However, by 2020, analysts predict that 60% of enterprise information security budgets will fund detection and response measures (Gartner 2017). Most often, these detection and response measures take a sociotechnical approach, that focus on developing cybersecurity ecosystems that rely on technical features of information systems as well as training and policy measures that encourage employees to detect and respond to cyberattacks.

To be effective, cybersecurity systems must be trusted by employees. IS research has shown that when employees view information systems as reliable, predictable, and helpful, they will be more likely to use it to create value for the firm (McKnight et al. 2011). This essential intuition, that trust is a key enabler for the effective IS use of information systems, has been found again and again across various contexts (Sun 2010; Ba & Pavlou 2002; Gefen et al. 2003; Benbasat & Wang 2005). Absent trust in the

cybersecurity system's ability to protect the firm, it is difficult to imagine a context where employees comply with security policies or use security tools provided by their employers (Posey et al. 2011).

While trust is essential to cybersecurity effectiveness, many cybersecurity best practices can be viewed as possible betrayals of trust. Consider email as an example. Employees routinely use email to share information, sometimes personal, most often work related. When informed that their email is monitored by employers, it is not surprising that employees express a degree of discomfort. Beyond monitoring, firms now routinely use firm email systems to spear-phish employees as a means to assess vulnerability to cybercriminals. Spear-phishing is defined as a highly targeted, context-specific attack that is directed at specific groups of individuals or organizations and aims to appear authentic to message recipients (Wang et al. 2012). Firm actions such as monitoring emails' content or spear-phishing employees as part of perimeter testing can be viewed as intrusive at best and betrayals of trust at worst. Perimeter testing is the act of identifying weaknesses in an organization's cyber defenses. Scant information systems research has directed attention to the interplay between trust and betrayal of trust on the effectiveness of cybersecurity systems. Such research is important, psychological contract violations undermine trust in technical systems and broader social systems (Pavlou & Gefen 2005).

Hence, we leverage the concept of betrayal to examine the effects of trust, and breaches of trust, on cybersecurity effectiveness. *Betrayal* refers to a violation of "pivotal" expectations of a trustor (Elangovan & Shapiro 1998; Morris & Moberg 1994), and can lead to betrayal aversion (Koehler & Gershoff 2003). *Betrayal aversion* refers to the degree to which an individual has feelings of repugnance towards an agent of betrayal. We suspect that when an individual feels betrayed by cybersecurity measures, such as email monitoring or perimeter testing, they will become averse to compliance with cybersecurity policies and avoid using the protective technologies offered by the firm.

To understand the implications of trust and betrayal for cybersecurity, we examine the following research questions:

1. *How does betrayal in the cybersecurity function form and change individual protective beliefs in the cybersecurity function?*
2. *Does the perception of betrayal lead to decreased levels of security behaviors through betrayal aversion, and what are the negative consequences?*

This research contributes to IS research. First, this research is the first to explore and conceptualize betrayal and betrayal aversion in IS research. Second, we offer a model that describes the formation of betrayal through a violation of trust and identifies its possible negative consequences.

Conceptual Background

Cybersecurity

Over 90% of successful cyberattacks manifest from spear-phishing campaigns (Verizon 2017), with many employees, approximately 97%, unable to discern malicious emails from benign ones (Verizon 2017, eInspired 2017, ProofPoint 2017). This in turn, has led to a focus on perimeter testing and monitoring to identify internal threats as a means to identify opportunities for interventions that can bolster cybersecurity.

Interestingly, other than employee monitoring (George 1996; Posey et al. 2011) or the content of messages (Wright et al., 2011), little behavioral IS research has directed attention to designing detection and response systems (DRS). These systems help to identify employees that are susceptible to socially engineered attacks and offer interventions through training or other means to protect firm cybersecurity. Such sociotechnical DRS are critical to organizations, as over 90% of breaches employ social engineering tactics (Verizon 2017).

Cybersecurity departments continually run DRS to identify internal causes of data breaches. An internal threat to the cybersecurity ecosystem can result from employee negligence (Vroom & Von Solms 2004; Probst et. al 2010) or vindictiveness (Probst et al. 2010). Many firms assign cybersecurity professionals to red teams, that are asked to expose security vulnerabilities from any vector, from socially engineered cyberattacks (e.g., spear- phishing) to physical attacks (e.g., unattended workstations). Red teams are

highly specialized groups that challenge an organization to improve its cybersecurity effectiveness by assuming an adversarial role or point of view. The findings of red exercises are used to identify opportunities for training or new security measures.

Monitoring capabilities have become more dynamic and invasive due to machine learning systems that go beyond simple keystroke logging to track websites, monitor email, and more. For example, the enterprise immunity system of DarkTrace relies on machine learning to detect anomalous behaviors based on an individual's information system use. Such systems move beyond simply identifying a breach to identifying and potentially removing internal threats before a breach can occur.

Consequently, cybersecurity departments' ability to identify individuals that commit breaches has grown increasingly sophisticated. For example, in the Target Breach of 2014, cybersecurity analysts identified the individual that caused the breach. The individual accidentally jeopardized his credentials that had escalated access rights that hackers used to obtain entry into the Target network. Even though it came from an outside ancillary heating and cooling system (Computerworld 2014) network, the analysts were able to trace the breach. Although accidental, this breach jeopardized the sensitive information of over 70 million individuals, resulting in highly publicized negative outcomes for the firm and its employees, such as lost profits or more personal ramifications such as firing or demotion.
Some research has found that employees have varied responses to the use of DRS. George (1996) found that employee attitudes towards computer monitoring are variable, due to the lack of uniformity in monitoring as well as evaluations (George 1996). Posey et al. (2011) found that computer monitoring increased computer abuse, because employees felt that the organization invaded their privacy. Clearly, computer monitoring can have negative consequences for organizations.

While we increasingly see detection, identification, and classification measures used in practice, we lack a deep understanding of employee responses to their use in organizations. Increasing such understanding is important, because we suspect it can affect their compliance with cybersecurity.

Trust and Betrayal

Understanding employee responses to cybersecurity measures requires considering how they perceive DRS. To study this topic, this research takes a perspective of trust-betrayal-aversion (TBA).

Trust in cybersecurity requires that employees trust the cybersecurity department and associated technology to act as protectors, such that they work in a secure, threat free environment. Similar to a police officer and citizen relationship, where the citizen has an expectation that the officer will protect him or her if needing help, but not harm them. Hence, we define trust in cybersecurity as a strong conviction that the individual is protected from a cyberattack (adopted from McKnight 2005).

When an agent of protection, like the cybersecurity department, violates trust by becoming an agent of harm the consequences can be far more detrimental to the individual and organization (Koehler & Gershoff 2003). Trust in cybersecurity may be violated when monitoring and perimeter testing are deemed as untoward by employees, evoking feelings of violation and betrayal. Research suggests that cybersecurity measures evoke a range of feelings and behaviors associated with betrayal, such as perceived injustice workplace deviance, technostress, and lower levels of commitment (Posey et al. 2011; Ayyagari et al. 2011; Alge et al. 2006a; Ariss 2002; George 1996).

Betrayal of trust by the cybersecurity department can result in employees reporting intense prolonged negative feelings. This dissonance can be evoked by humans as well objects, such as physical artifacts or software that are viewed as sources of betrayal (Koehler & Gershoff 2003), with responses that manifest in different forms (Finkelhor & Browne 1985; Strauss 1994). This research defines betrayal in cybersecurity as a violation of the pivotal protective beliefs cybersecurity measures provide from a cyberattack.

The dissonance between the cybersecurity department being viewed as a protector and betrayer could result in a range of responses. For instance, classic betrayal studies (Davis & Petretic-Jackson, 2000) showed that responses can range from separation, punishment, to no response at all. Regardless of the

response, within organizations, Robinson and Morrison (1997) showed when employees perceived that they were betrayed, satisfaction, trust, and further intentions to stay with the organization eroded.

Understanding betrayal is important, because there is a natural tendency for individuals to take action to avoid such feelings. Betrayal aversion in cybersecurity is defined as the degree to which an individual has feelings of repugnance toward cybersecurity measures. Keohler & Gershoff (2003) noted that individuals will make suboptimal decisions in the presence of a minimal (0.01%) chance of being betrayed by an agent of betrayal. Thus, individuals when sensing that there is a slight chance that an agent of protection, like the cybersecurity department or system, will betray them will react in a far more proactive manner, such as resisting compliance with cybersecurity policies.

Betrayal Aversion and Resistance

Violations in trust in cybersecurity may activate employees' natural tendency to avoid betrayal. Keohler & Gershoff (2003) found in a series of experiments exploring betrayal, individuals would choose to forgo the use of an airbag, vaccination, or smoke alarm in the rare chance that it could cause harm, although it greatly reduced the chance of death even though these products are designed to protect.

Employees' tendency to avoid betrayal may result in resistance to cybersecurity. Resistance can result from a trigger, in which an employee, perceives a threat, such as modification to social structures (LaPointe & Rivard 2005) or power structures in organizations (Markus 1983). We suspect that betrayal or monitoring may be one trigger of resistance to cybersecurity policies.

Resistance can result in apathy, passive, active, and aggressive actions against the object of resistance (LaPointe & Rivard 2005). Where extant resistance research has also revolved around the introduction or implementation of new systems into an organization (Markus 1983; LaPointe & Rivard 2005; Kim & Kankanhalli 2009; Craig et al. Forthcoming), we suspect that employees may demonstrate a similar pattern of resistance behaviors, if they feel betrayed by the cybersecurity function (Table 1).

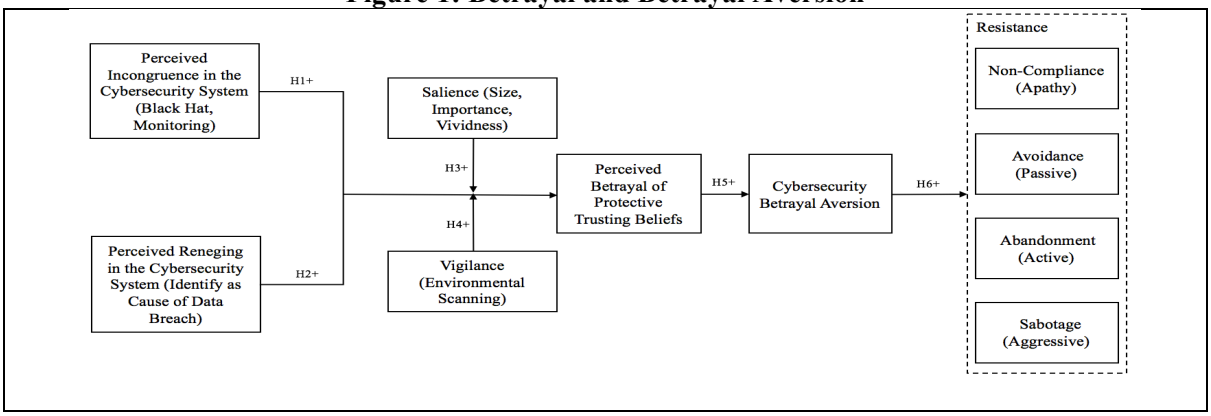
Table 1: Forms of Resistance Manifesting from Betrayal

Resistance Behavior	Form of Resistance (Lapointe & Rivard 2005)	Example
Non-Compliance	Apathy	The individual does not complete mandatory training, refuses to agree to compliance policies, does not log off when leaving his or her desk.
Avoidance	Passive	The individual uses personal email to avoid screening tools, does not report phishing attacks, masks documents or links in unscreenable files such as PDFs.
Abandonment	Active	The individual utilizes personal devices to complete work like a mobile hotspot network to avoid monitoring, works on their own computer when off the monitored network, downloads files on a USB.
Sabotage	Aggressive	The individual creates a backdoor to the system, obtains confidential records through the use of screenshots, disparages the cybersecurity dept. as incompetent.

Research Model and Theoretical Development

We present a novel integrated model of cybersecurity betrayal and betrayal aversion to explain how trust, and breaches of trust, by cybersecurity can undermine cybersecurity effectiveness (Figure 1).

Figure 1: Betrayal and Betrayal Aversion



Protective beliefs refer to the degree to which an individual believes he or she is safeguarded from a cyberattack. An individual may perceive that the cybersecurity function of the organization will protect them. Betrayal can rise from the conditions of perceived incongruence and reneging on trust or protective beliefs by the protector (Morrison & Robinson 1997). Incongruence refers to the degree to which an individual and agent of an organization have different understandings about a perceived promise (Morrison & Robinson 1997). Perceived incongruence can develop from an individual's expectation that the cybersecurity system is for protecting them from attack rather than exposing them as a potential threat. An individual can be exposed through internal black hat tactical perimeter testing, like internal phishing exercises. Black hat tactics are employed by hackers who use them to violate computer security for little reason beyond maliciousness or personal gain. Reneging refers to the degree to which an agent or agents of an organization knowingly break a perceived promise to an employee (Morrison & Robinson 1997). Reneging in cybersecurity can be the use of the system to identify a source of breach, whether intentional or unintentional, and lead to an individual's feeling betrayed by the cybersecurity system. For instance, a company may be able to identify the individual that accidentally fell prey to a phishing message and punish that individual even though the system failed to protect them. Both incongruence and perceived reneging can lead to a discrepancy between the perception of what the cybersecurity system does and undermine protective beliefs. These misaligned perceptions therefore give rise to betrayal, as the individual may feel his or her trust has been violated (Morrison & Robinson 1997).

H1: Perceived incongruence of the expectations of the cybersecurity system will increase an individual's perception of betrayal.

H2: Perceived reneging of the expectations of the cybersecurity system will increase the individual's perception of betrayal.

Salience and vigilance may magnify the betrayal felt by the individual (Morrison & Robinson 1997). Salience refers to the degree to which a stimulus stands out from its immediate context (Fiske & Taylor 1984). Vigilance refers to the extent to which the individual monitors how well the organization has been fulfilling the terms of its perceived promises. Both play a role in the level of betrayal that an individual feels from the cybersecurity system since some employees may or may not be aware of a discrepancy of expectations. For instance, a user that is warned by the system that he/she has visited an unauthorized site may not feel the same level of betrayal as an individual that falls prey to a phishing attack and is made an example of by the cybersecurity department. The salience of this may be limited since the size, vividness, and importance to individuals may vary (Morrison & Robinson 1997). Additionally, vigilance means the amount of environmental scanning that an individual conducts to see if expectations are being met. For instance, an individual that is more aware of the volume of security breaches, reviews quarantine reports from the system, and follows SETA policies may feel the magnitude of betrayal more than less informed employees, as expectations have not been met.

H3: Salience will moderate the relationships between (a) incongruence and perceived betrayal, and between (b) reneging and perceived betrayal, so that the higher salience is, the stronger the relationships are.

H4: Vigilance will moderate the relationships between (a) incongruence and perceived betrayal and between (b) incongruence and perceived betrayal, so that the higher vigilance is, the stronger the relationships are.

Betrayal aversion implies that individuals will choose suboptimal options, if they sense betrayal or change behaviors as a means to avoid betrayal (Koehler & Gershoff 2003). Betrayal evokes emotional feelings of intense mistreatment on the behalf of the employee, thus resulting in a desire to avoid the betrayer or punish them severely, especially when they act as an agent of protection and then cause harm (Koehler & Gershoff 2003). When the cybersecurity function is the cause of a breach or identifies an individual as a potential risk, he/she may feel betrayed by the cybersecurity tactics and prime them to be averse.

H5: Perceived betrayal of protective beliefs will increase an individual's betrayal aversion.

Betrayal aversion could lead to employees passively or actively resist the very cybersecurity systems that were implemented as protective measures. For example, an employee may begin to practice non-compliance (apathy) by not attending training or following outlined policies and procedures (passive resistance). Employees could also bypass security measures by using personal devices to complete work rather than company issued devices (abandonment). For example, an employee could transmit sensitive information using a personal wifi hotspot, opening themselves to a man-in-the-middle attack. Finally, an individual may hope to sabotage (aggressive) the cybersecurity system or department by providing sensitive information to an external threat or creating a backdoor into the system. Overall, resistance to cybersecurity measures may lead to negative outcomes for the organization.

H6: Betrayal Aversion will increase an individual's level of resistance to the cybersecurity system.

Method

We will use a multimethod approach, combining a survey and field experiment. Data will be collected in two waves. Before the field experiment is undertaken, participants will be requested to complete a survey developed to measure the protective beliefs of the individual. After the field experiment, another survey will be sent to measure the level of betrayal felt and resistance behaviors. The survey will adapt existing measures of betrayal and resistance to cybersecurity.

Field Experiment Design

A field experiment will be conducted with organizations that use red team tactics and monitor their employees. We will enact a spear-phishing campaign using the organization's internal perimeter testing system. Upon completion of the spear-phishing campaign, we will notify participants of the organization's actions that the system was used against them to identify human vulnerabilities to cybersecurity. Additionally, we will also notify the individuals of the use of computer monitoring technologies (e-mail, keystroke logging, behavioral modeling, personal account access) as well as the actions that have been flagged in the system. We will conduct manipulation checks.

Measures

Measures for resistance, incongruence, reneging, salience, and vigilance will be adapted from the existing literature. We will develop measures of protective beliefs, betrayal, or betrayal aversion using best practices found in the literature, such as judges card-sorting exercises, field testing, and exploratory factor analysis, following standard procedures (Mackenzie et al. 2011).

Data Analysis

We will use structural equation modeling (SEM). We will examine the measurement model issues first (i.e., reliability and convergent and discriminant validities). Then, we will examine the structural model.

Discussion

This research explores the role of betrayal and betrayal aversion in the cybersecurity context. Our expected contributions include:

First, we introduce the new concepts of betrayal, betrayal aversion and perceived protective beliefs to the cybersecurity literature. We illustrate the dyadic nature of cybersecurity systems that are capable of

fostering feelings of protection and betrayal. This is important because organizational psychology has shown that when individuals or objects that are believed to be agents of protection actually betray, the consequences are far more damning for an organization (Koehler & Gershoff 2003).

Second, by studying this dyadic nature of cybersecurity systems, we increase understanding of the implications of black hat techniques as training or auditing tools. While rarely studied (Mahooda et al. 2010), black hat techniques are now more pervasive in use by practitioners in perimeter defense testing. As organizations continue to increase the use of black hat tactics in testing and training of employees, it is important for IS research to understand the consequences of this testing. Such negative consequences, such as betrayal, may lead to adverse impacts for the individual and organization.

Third, we build understanding of betrayal and resistance in the context of cybersecurity. As Craig et al. (Forthcoming) noted, scant research has been directed at the empirical testing of resistance, as most work has been qualitative and offers little guidance to practice. Extant resistance research has also revolved around the introduction or implementation of new systems into organizations (Markus 1983; LaPointe & Rivard 2005; Craig et al. Forthcoming). We direct attention to resistance to existing systems, while not seeking to understand how existing systems can be used to create resistance.

Finally, we contribute to the literature on employee monitoring by seeking to understand its effects in the cybersecurity context. Where prior work suggested mixed implications of computer monitoring, by introducing notions of betrayal and psychological contract breach, we afford opportunities for future research to examine whether betrayal explains why some monitored employees perceive injustice, increase computer abuse, engage in workplace deviance, report technostress, and diminished commitment (Posey et al. 2011; Ayyagari et. al 2011; Alge et al. 2006a; Ariss 2002; George 1996).

References

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extrarole performance. Journal of applied psychology, 91(1), 221.

Ariss, S. S. (2002). Computer monitoring: benefits and pitfalls facing management. Information & Management, 39(7), 553-558.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: technological antecedents and implications. MIS quarterly, 35(4), 831-858.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. MIS quarterly, 243-268.

Benbasat, I., & Wang, W. (2005). Trust in and adoption of online recommendation agents. Journal of the association for information systems, 6(3), 4.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impacton information systems misuse: a deterrence approach. Information Systems Research, 20(1), 79-98.

Dasgupta, Partha (1988). Trust as a Commodity. In Diego Gambetta (ed.), _Trust: Making and Breaking Cooperative Relations_. Blackwell. pp. 49-72.

Davis, J. L., & Petretic-Jackson, P. A. (2000). The impact of child sexual abuse on adult interpersonal functioning: A review and synthesis of the empirical literature. Aggression and violent behavior, 5(3), 291-328.

Durcikova, A., Jensen, M., &. Wright, R.T. (2015) Building the Human Firewall: Organization-wide Strategies to Combat Social Engineered Attacks. Oklahoma University and University of Massachusetts – Amherst. Funded by National Science Foundation. https://www.isenberg.umass.edu/firewall

Elangovan, A. R., & Shapiro, D. L. (1998). Betrayal of trust in organizations. Academy of Management Review, 23(3), 547-566.

Finkelhor, D., & Browne, A. (1985). The traumatic impact of child sexual abuse: a conceptualization. American Journal of orthopsychiatry, 55(4), 530.

Crocker, J., Fiske, S. T., & Taylor, S. E. (1984). Schematic bases of belief change. In Attitudinal judgment (pp. 197-226). Springer, New York, NY.

Gefen, D., Karahanna, E., & Straub, D.W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51-90.

George, J. F. (1996). Computer-based monitoring: Common perceptions and empirical results. MIS Quarterly, 459-480.

Hosmer, L.T. Trust: The connection link between organizational theory and philosophical ethics. Academy of Management Review, 20, 3 (1995), 213–237.

Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. MIS quarterly, 567-582.

Koehler, J. J., & Gershoff, A. D. (2003). Betrayal aversion: When agents of protection become agents of harm. Organizational Behavior and Human Decision Processes, 90(2), 244-261.

Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. MIS quarterly, 461-491.

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and distrust: New relationships and realities. Academy of management Review, 23(3), 438-458.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS quarterly, 35(2), 293-334.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: an editorial introduction to the special issue. MIS quarterly, 34(3), 431-433.

Markus, M. L. (1983). Power, politics, and MIS implementation. Communications of the ACM, 26(6), 430-444.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

McKnight, D. H. 2005. "Trust in Information Technology." In G. B. Davis (Ed.), The Blackwell Encyclopedia of Management. Vol. 7 Management Information Systems, Malden, MA: Blackwell, pp. 329-331.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems (TMIS), 2(2), 12.

Morris, J. H., & Moberg, D. J. (1994). Work organizations as contexts for trust and betrayal. Citizen espionage: Studies in trust and betrayal, 163, 187.

Morrison, E. W., & Robinson, S. L. (1997). When employees feel betrayed: A model of how psychological contract violation develops. Academy of management Review, 22(1), 226-256.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International journal of electronic commerce, 7(3), 101-134.

Pavlou, P. A., & Gefen, D. (2005). Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. Information systems research, 16(4), 372-399.

Clay Posey, Rebecca J. Bennett, Tom L. Roberts, and Paul Benjamin Lowry (2011). "When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse," Journal of Information System Security, vol. 7(1), pp. 24-47 (ISSN 1551-0123).

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Aspects of insider threats. In Insider Threats in Cyber Security (pp. 1-15). Springer, Boston, MA.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 34(3), 487.

Strauss, M. B. (1994). Violence in the lives of adolescents. New York:W.W. Norton.

Sun, H. (2010). Sellers' Trust and Continued Use of Online Marketplaces*. Journal of the Association for Information Systems, 11(4), 182.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. Journal of Management Information Systems, 29(4), 263-290.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Wang, J; Herath, T; Chen, R; Vishwanath, A; and Rao, HR. Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. IEEE Transactions on Professional Communication, 55, 4 (2012), 345-362.