ABSTRACT

The Downsides of Information Systems Security Policy Compliance Efforts:
Toward a Theory of Unintended Reversed Security Action
and Productivity (TURSAP)

Puzant Y. Balozian, Ph.D.

Advisor: Dorothy E. Leidner, Ph.D.

Modern organizations face significant information security violations from inside the organizations to which they respond with various managerial techniques. It is widely believed in IS security literature that enforcing IS security policy compliance on employees through various means is the solution for security effectiveness. Nevertheless, this dissertation challenges that notion and advances a stream of research that suggests increasing security measures may lead to decrease in user productivity, increased user mistrust toward the IT department, increased user frustration, increased user technology avoidance, increased non-malicious volitional security violations and overall may lead to increased security risk, instead of decreasing it. This dissertation explores the how and why of these mechanisms and suggests what to do about this phenomenon. Following a grounded theory methodology, this dissertation develops the Theory of Unintended Reversed Security Action and Productivity (TURSAP), the first of its kind in exploring the downsides of IS security measures.

The Downsides of Information Systems Security Policy Compliance Efforts:
Toward a Theory of Unintended Reversed Security Action
And Productivity (TURSAP)

by

Puzant Y. Balozian, B.S., M.B.A.

A Dissertation

Approved by the Department of Information Systems

_____

Timothy R. Kayworth, Ph.D., Chairperson

Submitted to the Graduate Faculty of
Baylor University in Partial Fulfillment of the
Requirements for the Degree
of

Doctor of Philosophy

Approved by the Dissertation Committee

_____

Dorothy E. Leidner, Ph.D., Chairperson

_____

Timothy R. Kayworth, Ph.D.

_____

Hope A. Koch, Ph.D.

_____

Debra D. Burleson, Ph.D.

_____

Tony L. Talbert, Ed.D.

Accepted by the Graduate School

May 2016

_____

J. Larry Lyon, Ph.D., Dean

Page bearing signatures is kept on file in the Graduate School.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to acknowledge my dissertation committee, Dorothy Leidner, Tim Kayworth, Hope Koch, Debra Burleson, and Tony Talbert for their unfailing support and commitment to this dissertation project. I am deeply grateful to Dr. Leidner. She is not just a distinguished scholar in our field but also a caring advisor.

DEDICATION

To my caring parents and
To my lovely wife

for their constant support and understanding, for their encouragement to me to stay within the program when I was wanting to quit, and for their constant reminder that our Father in heaven will continue to give me grace upon grace in order for me to be able to finish the Ph.D. program in a successful manner

CHAPTER ONE

Introduction

Employees are a major threat to information systems (IS) security (ISsec) in organizations (Chen et al., 2012b; Wall, 2011). To mitigate insider threats, organizations have invested significant resources in developing behavioral as well as technical countermeasures, including policy development, training programs, and technological security updates (PWC, 2013). Recently, one study indicated current employees are responsible for over 50% of reported security breaches (PWC, 2015). Another survey revealed that carelessness or lack of awareness caused 38% of insider security incidents (Young, 2014). Industries in the United States, as well as federal and state level agencies, have advanced standards that regulate organizational IS security measures (Chen et. al, 2012b). Notwithstanding, a class of employees continue to show non-malicious opportunistic behaviors, circumventing IS security policies (e.g., saving passwords on files in unencrypted smartphones, using same or similar passwords across work related and personal accounts, using software that are not security compliant etc.) and thus presumably decreasing IS security effectiveness. A CSI/FBI report (Richardson, 2011) showed that internal actors were responsible for no less than half of the significant cyber security breaches. These figures intensify the constant mandate to decrease the risk of negligent—as well as opportunistic and malicious—insiders in organizations. Furthermore, 29% of data breaches occur through social tactics (Verizon, 2013), which can only be successfully accomplished if the employees are unaware and ill equipped to handle such techniques used by hackers.

Along with the significance of the percentage of incidents due to insiders, this threat is also gauged by the percentage of company losses. According to the same CSI study, 66.1% of the respondents reported that up to 20% of total company losses are attributed to non-malicious insiders, and 87.1% of the respondents reported that up to another 20% of losses are attributed to malicious insiders (Richardson, 2011). According to a survey of 671 IT and IT security practitioners, ISsec risks are generally on the rise, and the negligent insider threat risk still remains high (Ponemon Institute, 2012). The same institute found that practitioners and IT managers are witnessing the greatest rise in potential IT security risks within their work environment in both the negligent dimension (according to 43% of the respondents) and in the malicious dimension (according to 16% of the respondents) (Ponemon Institute, 2012).

In summary, the numbers are continuing to be high for non-malicious volitional security violations (NMV-SVs). These security violations or policy circumventions are neither due to malicious reasons nor due to ignorance. They are volitional ISsec policy circumventions without the intent to necessarily harm the organization. Guo et al. (2011) use the term non-malicious security violations (NMSV) thus omitting the volitional component of the security violation. I include the volitional aspect (the V in the middle of NMV-SV) to make it clear in this dissertation that I am not addressing the naively negligent or ignorant employees regarding security policies.

These statistics on non-malicious volitional security violations (NMV-SVs) are alarming, given the fact that there is no paucity of academic research into ISsec research on the organizational level, particularly in the area of ISsec policy compliance. D'Arcy et al. (2014) said that IS security researchers' knowledge of the phenomenon of employees'

security compliance decisions still remains incomplete because of the high percentage of unexplained variance (50%–70%) in employee behavioral outcome variables regarding security violations. In D'Arcy's attempt at finding some of the remaining high-unexplained variance of security violations, he led the study of technostress (stress due to increased ISsec policy requirements) and how it may increase violation intention (D'Arcy et al., 2014). This seminal piece is one of the few of academic studies within the last 25 years, if not the only one, that *categorically* studied a downside of ISsec measures.

The evidence suggests that ISsec literature is incomplete and is focusing on the positive aspects of ISsec policy implementation, altogether neglecting the probable adverse side of ISsec policies. There is a promising field of finding substantial additional variance of NMV-SVs in the dimension of the downsides or constraints of ISsec measures. In this dissertation, the definition of the downsides of IS security measures is any and all *unnecessary* negative consequences that are experienced by the users in organizations because of the implementation of IS security measures. I consider the words downsides, adverse effects and constraints of security measures synonymous in this dissertation and use them although seldom interchangeably. The majority of the IS studies (see literature review section) *assume* that pushing for stronger security policies and security measures is good for organizations. This dissertation focuses on different reasoning. It looks for some clear signs to explain at least one of the main reasons that continual *high numbers of non-malicious volitional security violations (NMV-SVs) may be caused by the continuous increase of ISsec measures.*

Concerning the downsides of ISsec measures, some evidence comes from practitioner journals in the sphere of security in general and ISsec in particular. Security

measurements of buildings and facilities have some less than optimal consequences. Employees who walk into the building may feel they are surveilled or watched and followed. They may think the cameras are intimidating and intrusive to their right of privacy in the workplace. They may feel uncomfortable in working under a surveilling camera. In other words, cameras leave the surveilled employees feeling vulnerable and mistrusted (Rosenberg, 2000; Stanton & Stam, 2006). The latter studies advise the organizations that in order to use camera surveillance, they need to win over employees first (i.e., to justify its use) because the cost of offending employees is "high."

IS practitioner articles have found that employees face a plethora of increasing security requirements that they find to be constraining, demanding, and challenging to understand and follow (Posey et al., 2011b; Post & Kagan, 2007; Wall, 2011). This was evident in a survey of thousands of employees in which reasons such as "not-thinking about policies because of work overload" and "the inconvenience to follow policies" are reported as the main reasons for ISP violations (Cisco, 2011). Other practitioner articles suggest that security requirements have downsides and may induce policy circumvention behavior due to the burdens they put on the employees (Posey et al., 2011b; Siponen, 2000; Stanton & Stam, 2006). Although these are preliminary indications supporting the notion of the downsides of IS security measures, an investigation of the adverse effects of security requirements is absent in ISsec research. Both the practical and managerial ramifications of the downsides of IS security measures on the life, satisfaction, productivity of the organizational users and the clues coming from the industry and practitioner journals are significant enough to launch a full-scale study to understand the dynamics of the downsides of the ISsec measures.

This dissertation investigates the main adverse effects of ISsec measures and their impact on security and productivity. The research objective is summarized in the following: In order to further the research on IS security measures effectiveness in mitigating insider non-malicious volitional security violations and in order to account for the remaining unexplained high variance in employee security violations, this dissertation explores the notion and the dynamics of the adverse effects of increased security measures.

This dissertation investigates whether ISsec masures could be a source or a drive behind the phenomenon of lingering high levels of non-malicious volitional security violations among employees in organizations. The dissertation describes the main possible downsides or adverse effects of increased security measures and based on the qualitative exploratory study and analysis findings, it advances a grounded theory of the adverse effects of ISsec measures.

Importance of This Dissertation

The importance of this dissertation is indirectly linked to the importance of the dynamics of the IT department and the employees. In the case if IT departments are partly behind the reason why the high variations of non-malicious volitional security violations are still unexplained and unaccounted for in organizations. The increased security measures from the IT departments is not the adequate solution, *specially without or prior of discussing with the users the likelihood of the ISsec measure implementation and its justification*. In this dissertation, the findings show how and why ISsec measures are the source of high security violations. Instead of decreasing the security risk,

increasing the enforcement of new IS security policies may unintentionally increase security risk by increasing non-malicious volitional security violations (NMV-SVs).

Furthermore, this research describes how and why security measures may unnecessarily decrease productivity; increase the mistrust of employees toward the IT department, increase technology use avoidance, and increase user frustration. Increased levels of security measures, if not justified in the eyes of employees, may have a myriad of practical adverse effects that IT departments cannot and should not ignore.

The concept of the ISsec downsides changes the perspective how IS academicians, IT security experts and employees may view the role of IT in justifying its increased security measures prior to implementing them in organizations. This dissertation found that employees expect that any additional security measure needs to be explained and justified in their perspective. This finding is important on both managerial and theoretical levels. On the managerial level, the findings of this dissertation suggest a significant new strategy and approach to be adopted by IT departments in decision making regarding IS security policies.

This dissertation also advances an explorative theory to explain the mechanism of how and why ISsec measures decrease security effectiveness and ultimately productivity. There are some theories (ex: general deterrence theory and protection motivation theory) to explain how ISsec measures increase security effectiveness, but the theory developed and advanced in this dissertation describes how ISsec measures may sometimes decrease security effectiveness, along with decreasing the productivity of the employees. This research calls the grounded theory it develops "TURSAP": the Theory of Unintended Reversed Security Action and Productivity.

In summary, this research makes advancement to ISsec research that is both novel and important in three ways. First, it challenges the dominant positive approach to ISsec measures by exposing its downsides to security effectiveness, and it finds that both academia and practitioners should exercise caution in advancing more ISsec measures. Second, while acknowledging that there is a growing sentiment that ISsec measures sometimes may cause more harm than good, this dissertation digs deeper into knowing the mechanisms of how and why this may be so. Third, this dissertation advances an indigenous IS theory called TURSAP that explains the different outcomes and downsides of ISsec measures.

This dissertation is organized as follows. In the next section, it reviews in three separate sections the literature on IS security, ISsec policy compliance, and the downsides of the latter. Then, it presents the methodology, including a description of the grounded theory approach, site selection, data collection, data analysis methodology, and validation. It follows with the analysis and discussion, including a discussion on the TURSAP theory. The study ends with highlighting the contributions of this research, recognizing its limitations, and offering suggestions for future research.

In chapter two, in the section of the literature review of ISsec policy compliance to be published in a peer-reviewed journal, my mentor, Dr. Dorothy Leidner, significantly guided the paper. I am deeply indebted to her insights into that paper.

CHAPTER TWO

Literature Review

This chapter in its second part to be published as: Balozian, P. & Leidner, D. (2016). Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *The Database for the Advances of Information Systems (forthcoming).*

The literature review section has three subsections. A review of literature in IS security in general is followed by a review of literature in IS security policy compliance in particular. The section ends with a review of the downsides of IS security policy compliance or the adverse effects of IS security measures.

Review of IS Security Literature

ISsec is the "well-informed sense of assurance that information risks and controls are in balance" (Anderson, 2003, p. 310). I am discussing ISsec as it is related to computer systems. To find the relevant articles, keyword and subject searches were conducted in a top senior basket of eight[1] journals with the term *Information Security*. Out of 56 articles, only 21 were empirical studies, of which 15 were relevant to ISsec in organizations. Information security *policy compliance* articles were not included. They will be treated separately for the reasons mentioned earlier.

From the early 1990s, MIS executives put ISsec on the top of their priority list (Loch et al., 1992). This topic is still on the top of the list (Andriole, 2015) because of attacks from outside the organization and from attacks and NMSVs from within.

[1] The senior basket of 8 journals are the following journals: 1) MIS Quarterly, Information Systems Research, Journal of Management Information Systems, European Journal of Information Systems, Information Systems Journal, Journal of the Association of Information Systems, Journal of Strategic Information Systems and Journal of Information Technology.

Ransbotham and Mitra (2009) found the reason why organizational information is attacked and how organizations may defend themselves from outside attacks. They found that organizations have tangible, iconic, and reprisal values that attract hackers to consider breaching organizational security (Ransbotham & Mitra, 2009). Tangible values include information and resources ready to be sold to third parties, and an attack on an iconic value is an attack on large, seemingly impenetrable targets. Attacks for reprisal value comprise acts of vengeance. In the same study, the researchers found that organizations can use five different broad mechanisms for defense: access control (e.g., user and server authentication), vulnerability control (e.g., updating patches), feature control (e.g., disabling certain ports or session encryption), traffic control (e.g., monitoring of data packet source addresses), and audit control (e.g., managing logging and activity records).

Five themes emerged in the senior basket eight journals regarding ISsec literature (excluding ISsec policy compliance articles). These include threats in information sharing among peers, disclosure of software vulnerabilities, themes related to disclosure of security breaches, technical features combatting outsider threats, and technical features preventing insider threats. Each of these themes will be explained and described in the following paragraphs. The last theme will be briefly introduced in this section and treated to the degree it pertains to the technical designs (but not compliance). The second in-depth literature review will address in-depth ISsec policy compliance. Then, the downsides of ISsec policies literature review follows.

Threats in Information Sharing Among Peers

With the advent of the Internet and cloud computing, employees in different or the same departments have started accessing each other's networks, servers, storage, applications, and services. Information sharing among peers has become commonplace. A well-known commercialized form of this type of sharing files and resources among peers is Dropbox. Nevertheless, a study found that file sharing via collaboration tools among peer-to-peer (P2P) networks increases the vulnerability of organizations to data breach or resource leakage (Johnson, 2008). These types of breaches are due to vulnerabilities in the software design. When organizations discover such vulnerabilities or they discover that their data has been breached, they have some incentives to disclose them to software design companies. This incentive leads us to the themes of the next two paragraphs.

Disclosure of Vulnerabilities in Software

Organizations may consider reasonable to conceal software vulnerabilities from the society at large in order to avoid giving attackers information that they can exploit. In fact, research has found that these disclosures increase the diffusion of attacks and intensify the risk of first attack after the vulnerability is reported (Mitra & Ransbotham, 2015). Obviously, hackers want to exploit the vulnerabilities of new software, operating systems, and applications. Their best time of attack is between the time of the disclosure of the vulnerability by an organization and the patch becoming available. This timeframe is known as zero time attack. Nevertheless, disclosing vulnerabilities is strangely beneficial for organizations. It accelerates the patch release time from vendors by 2.5 times compared to when it is not disclosed (Arora et al., 2010). Without disclosing the

vulnerability, organizations will wait longer until a software patch becomes available in an update or upgrade. In my opinion, a better solution for the hackers' exploitation upon the release of vulnerability is to create a protected network of all the major vendors and businesses and releasing the vulnerability in this network rather than releasing it publicly. By this, a win-win situation is created, and an incentive is given to the vendor to release a patch quickly because of a fear of competitor vending a better product without that particular vulnerability. Thus, a "safe" incentive is created (competition among vendors) rather than a risky incentive in an environment where the information can be exploited by hackers. Of course, the protected network among vendors will be the next target for hackers, but that target will be better protected in comparison to the target of organizations using a product with publically disclosed vulnerability.

Disclosure of Security Breaches

Sometimes, laws dictate a minimum threshold of security standards and practices (Backhouse et al., 2006). For example, the Sarbanes-Oxley act requires a level of disclosure regarding organizations' activities in preventing, detecting, or correcting ISsec breaches. Research has found that such voluntary disclosures (i.e., going beyond and above the minimum level demanded by the law) benefit organizations by giving them a better market value (Gordon et al., 2010). This finding may encourage firms to disclose information about their security activities because people will have a perception that they know the firm in question, and thus they trust it. The finding of Sen and Borle (2015), who suggested that there is a direct correlation between the strictness of state-level data breach disclosure laws and the reduced risk of data breach, complements this research. Nevertheless, researchers still needs to investigate what might happen if hackers were to

gather enough critical "voluntarily or required by law disclosed info" (ibid) so that they could devise more robust plans to attack the firms or industries in question. Some ISsec activities may give enough clues regarding the types of intrusion detection systems (IDS) that are used, thus increasing the likelihood of consolidated and coordinated attacks specifically sponsored by state nations. Recently, the Chinese state was accused of being the active agent behind major breaches in U.S. businesses and industries (Ward, 2015). Nevertheless, organizations can boost their technical configurations to be protected from outside attacks.

Technical Capabilities Against Outside Attacks

To protect against outside attacks, IS research sheds light on the need for proper configuration (the process of setting software quality restrictions or limits to meet detailed user requirements). Thus, IS research has different security technologies (e.g., firewall and intrusion detection systems) to rely on. Nevertheless, these technologies interact with each other, altering and diminishing each other's contribution and thus increasing the security risk by undermining the effectiveness of these protective systems. The authors conclude that there is a need for proper configuration for these types of software (Cavusoglu et al., 2009).

There is a lack of technical research in the domain of ISsec in the senior basket eight journals. Nevertheless, this is understandable and justified because IS deals with the interaction between people and IT artifacts. If researchers in the IS discipline wanted to study only IT artifacts, then the discipline would not have been differentiated from the fields of computer science or computer engineering. Perhaps the presence and interaction of both people and IT artifacts inside the organization is causing an increase in IS

research in the area of insider threats or mitigating non-malicious violations of ISsec policies. To complete the four areas in this section—information leakage, disclosure of software vulnerabilities, disclosure of ISsec items, implementation of technical capabilities to fortify against outside attack, or opportunistic inside employees—the following paragraph covers a small sample of IS research on technical capabilities to help motivate employees to abide by ISsec policies.

Technical Capabilities to Fortify Against Opportunistic Employees

Unethical IT use is a complex phenomenon and has ethical, social, economic, and technological dimensions that need to be addressed in multiple intervention cases (Chatterjee et al., 2015). This may have led some IS researchers to conduct cognitive neurophysiological lab experiments. These experiments usually involve testing the cerebral firing of neurons and their patterns and strengths. Such IS research found that only those employees who have neurocognitive evidence of having higher self-control (neurons of the brain related to self-control are for some reason more developed) need to be trusted with and assigned to more sensitive digital assets (Hu et al., 2015). Nevertheless, schools of law assert that this type of neurological research, although interesting, is of little practical implication because of ethical sensitivity and legal regulations governing practices such as employee job assignments that are the results of psychological screening (London & Bray, 1980).

Other technical capability research in this area includes studies on passphrases and user-interface (UI) design artifacts to control access policy. Keith et al. (2009) found that using long passphrases is effective in user authentication. Longer passphrases are more resilient against attacks and yet are easy to remember. This may mitigate employees

from using weak passwords. The UI design artifacts are special popup interfaces (like popup screens) that may include information on who in the department is online on their desktops, their access, and which files they are working on. It may also show whether the respective supervisor(s) are online and monitoring those employees. Vance et al., (2015) found that such interfaces increase online identifiability in the department, expectations of evaluation, awareness of monitoring, and the social presence of peers. All of these factors may increase the perceived accountability of the user, diminishing his intention to violate the access policy.

Review of IS Security Policy Compliance

This section is the biggest section in the security literature review of this dissertation. This is due to the large number of articles in IS security field addressing the topic of ISsec policy compliance. ISsec policy compliance and the methods to increase could well be the intersection of people and IT artifacts in the field of security. IS field has its roots of existence in studying such interactions of IT artifacts on business but also on information and employees.

The Conceptual Themes

Four major themes emerged from the literature review of ISsec policy compliance. Each theme will be defined and discussed in terms of both the negligent and malicious categories in the following section. The process through which IS management tries to strengthen the links in the security chain of the organization comprises of making every employee abide or comply with the laws or the IS policies. This dissertation identified four overarching themes depicting countermeasures for combatting insider

threats to ISsec. The themes are: Implementing different philosophies of countermeasures (of deterrence and development), applying procedural countermeasures, applying technical countermeasures, and enhancing environmental countermeasures. The definitions of each of these themes are described concisely in the following section. The following sections describe the themes in a more comprehensive manner in separate sections for each theme.

In this dissertation, the philosophy of countermeasure is defined as the philosophical approach IS management uses to ensure compliance or to decrease noncompliance among employees. There are two main philosophies regarding approaches to ensure compliance. One approach is a positive developmental one, with an emphasis on encouragement to comply, referred to here as the development philosophy. The second is a more negative one, referred to here as the deterrence philosophy, with an emphasis on creating fear in the case of failure to comply. An example of the development philosophy is explaining why compliance is beneficial for the employees (for example, because it may provide a sense of personal satisfaction). An example of the deterrence philosophy is informing employees that those who do not comply with the newly established policies will be penalized financially.

Procedural countermeasures are managerial measures taken by IS management to deter noncompliance or encourage compliance with ISsec policies. This may include forming policies and training employees on security awareness. The definitions for the procedural and technical countermeasures can be found in the literature (Guo and Yuan, 2012; Straub, 1990). The rest of the definitions are formulated for this dissertation.

Technical countermeasures are the technical means employed by IS management to deter noncompliance or encourage compliance with ISsec policies. This may include software monitoring and reviewing computer logs. Environmental countermeasures are the social measures used by IS management to deter noncompliance or to encourage compliance with ISsec policies. This may include creating a fear culture of security department by encouraging supervisors to keep tabs on employee compliance, thereby creating a heightened sense of subjective norms (the expectations of significant people, like the employee's supervisors and colleagues) or creating a more positive culture toward security by hiring those potential employees that have shown high standards of commitment and loyalty to the organization they serve.

Heretofore the themes were introduced, defined and described by giving examples. In the following sections this dissertation parades the literature along the lines of these themes in detail.

Theme 1: Implementing a Philosophy of Deterrence or a Philosophy of Development Regarding Countermeasures

There are two main philosophies in the IS literature regarding approaches to ensure compliance: the extrinsic model, which is command and control, and the intrinsic model, which is self-regulatory control (see Tyler and Blader, 2005). The command and control model is best understood in IS security literature by the term deterrence, based on seminal works of General Deterrence Theory in early 1990s. Deterrence conveys the idea that there are extrinsic measures (usually IS management) forcing policy compliance on employees. I name this deterrence approach via command and control the philosophy of deterrence. The best name to be given to the counterpart of deterrence philosophy is

what this dissertation names the “development philosophy”. The title “development philosophy” fits well with the intrinsic model of Tyler and Blader. It is self-motivated (albeit the self-motivation may still be triggered by outside measures). Thus IS management instead of using threat (or deterrence) uses development. To summarize, the deterrence philosophy threatens employees with sanctions to force them to follow IS policies. The development philosophy encourages and motivates policy compliance by by informing IS users of the intrinsic benefits and overall safe work environment they will experience (safety from outside hacking attacks) if they comply with IS policies.

Researchers who wanted to test and prove its effectiveness on one type of employees, the malicious insiders, heavily rely upon the deterrence philosophy. The malicious employees are the hired employees who for some reason want to harm the organization they work (or recently worked) in. This is the case because of the long proven history of the deterrence approach; its effectiveness has been shown in dealing with criminal acts not just in IS research, but also in governmental and legal actions throughout thousands of years of recorded human history. GDT was adopted, adapted, and contextualized in IS research in the early 1990s. There are other possible reasons why deterrence theory is widespread in ISsec research: ISsec lacks indigenous theories on security, and there are still not enough good robust developmental theories (with the exception of protection motivation theory) which has been adopted, adapted, and contextualized in ISsec research. Given enough time and good direction from ISsec editorials, our research community will adopt and contextualize more of the developmental theories to change potential malicious insiders into complying employees.

GDT focuses on the indirect (or general) prevention of crime by making examples of specific perpetrators, using the instrument of quickly inflicting a severe and particular sanction on the perpetrator. It is not surprising to see the influence of this approach in IS theory and practice, especially pertaining to malicious insiders. How this philosophy of deterrence is studied and tested in IS research is more fully explained in the following section.

Deterrence philosophy (negligent threat). To determine the effectiveness of deterrence philosophy on negligent insiders, the severity and certainty of sanctions have been tested. The severity of sanctions is the severity of the punishment that may be inflicted on noncompliant employees. The certainty of sanctions is the likelihood of being caught and reprimanded or punished, regardless of punishment severity. Research has found that sanction certainty lacked significance and severity had a greater impact than certainty in deterring IS misuse intentions (D'Arcy et al., 2009). The researchers explain the insignificance of sanction certainty by introducing the awareness of policies in a post-hoc analysis. Apparently, the certainty of sanction awareness is more significant than sanction certainty alone (ibid). Since the sanctions are in and of themselves insufficient for enforcing compliance, they must be communicated to IS users during security training, and the employees must be well informed about the penalties for breaching security (Straub & Welke, 1998).

The fear of sanctions has a deterrent effect, and since deterrence increases actual compliance (Siponen, Pahnila & Mahmood, 2010; Guo and Yuan, 2012), one of the means of maximizing ISsec is to introduce the threat of being fired upon failure of compliance (Dhillon and Torkzadeh, 2006). The existence of codes of ethics has little

deterring value if used alone, and therefore punishment is an enforcer of policies (Harrington, 1996). Sanctions affect the perceived cost of noncompliance toward IS policies, and therefore compliance intention (Bulgurcu et al., 2010). Pre-conventional moral reasoning exists when a person is abiding by ethical codes because of fear of punishment. This reasoning is the only significant moral reasoning that deters noncompliance (Myyry et al., 2009). The social conformity that makes the employee abide by the policies is called "conventional moral reasoning." The firm beliefs and principles that make the employee abide by the policies are defined as "postconventional moral reasoning." The latter two reasoning levels were insignificant in their impact on compliance with ISsec policy (ibid). Hence, the effectiveness of the deterrence approach is only *partly* dependent on the moral reasoning factor in individuals. This suggests that the perception of severity and certainty of sanctions will work best only on employees who fear punishment.

The philosophy of deterrence has other techniques besides the enforcement of severity and certainty of sanctions. The detailed formulation or specification of security policies and the periodic evaluation of the employees' behaviors based on these specified IS policies are positively associated with the individual's perception of compliance mandatoriness (see Kirsch and Boss, 2007). Thus, when employees notice that management is investing time in developing detailed IS policy documents, they will perceive the gravity and the seriousness of policy compliance.

Deterrence or fear approach (malicious threat). Regarding malicious threats, early IS literature on insider threats (Straub, 1990; Straub and Nance, 1990) found that the severity and certainty of sanctions deter computer abuse. Severe punishment could be

executed on a malicious insider such that he would be a living example to other potential perpetrators. In the case of the absence of a malicious incident, punishment threats should be regularly communicated to employees.

The deterrence research on malicious insiders is inconsistent in its results: deterrence certainty and severity had no influence on compliance behavior in one of the articles (Son, 2011), in contrast to the previous articles reviewed above that found the severity and certainty of sanctions significantly decreased IS misuse. Perhaps the fact that Son's (2011) sample comes from China could be the cause behind the differing worldviews regarding compliance (Leidner & Kayworth, 2006). For example, the deterrence effect of certain security countermeasures varies between the US and Korean cultures (Hovav and D'Arcy, 2012).

In summary, based on the research of many scholars, deterring IS misuse using the severity, certainty, and celerity of sanctions is a proven technique available to IS management to enforce compliance on the company's negligent as well as malicious insiders. Interestingly, the security studies did not differentiate among the types of insiders in their abilities and intentions (naive, opportunistic, and malicious) when they tested the deterrence approach. Their samples consisted of general users and not specific malicious, opportunistic, or naive employees. This should be remedied in future ISsec research.

Development philosophy (negligent threat). The rise of insider security incidents moved some scholars to argue that the deterrence model is not effective enough. Thus they started advocating for another approach, the development philosophy, which uses encouragement to motivate employees to comply with IS policies. Although convincing

at first glance, the argument of rising incidents cannot be firmly attributed to the ineffectiveness of the deterrence philosophy. The rising incidents could be easily ascribed to the poor implementation and appropriation of deterrence philosophy or to the rising number of IT users. Furthermore, punishment cannot be abandoned altogether. People who follow rules to avoid punishment and people with low self-control are deterred better by punishment than by ethical training (Workman & Gathegi, 2007). Perhaps the explanation of the incentive to shift the focus of some research from the deterrence approach to the development approach is of a philosophical nature: punishment in deterrence models embodies a negative approach, and any negative approach is frowned upon in a society driven by political correctness and eager to explore positive approaches to societal problems. Siponen and Oinas-Kukkonen (2007), among others, encourage researchers to explore motivational approaches to ensure IS compliance. Thus, IS researchers have recently started to explore a more positive dimension to compliance.

Bulgurcu et al. (2010) found that the perceived benefit of compliance positively influences compliance intention. In their study, the benefit of compliance was comprised of intrinsic benefit (a sense of accomplishment and satisfaction), the safety of the resources (working files being safe from virus attacks), and rewards (financial and promotional). Furthermore, the increasing awareness of the intrinsic cost of noncompliance (guilt, stress, and embarrassment) was found to positively affect intention to comply. The intrinsic cost is not a component of a deterrence approach because it is self-inflicted; it is not initiated by the organization as formal or informal sanctions are. The intrinsic cost is solely dependent on the individual character of the insider and his or her emotional makeup. Hence we do not group this construct under the deterrence

approach. The organization encourages users to comply by directing them to count the cost of potential technical and psychological harm resulting from hackers destroying work files (extrinsic) or feelings of guilt (intrinsic) upon failure of compliance.

Some studies (Kirsch & Boss, 2007; Pahnila et al., 2007; Siponen et al., 2010) reached different conclusions than Bulgurcu et al. (2010) regarding rewards, which may take the form of a pay raise, bonuses, or verbally praising IS policy compliant employees in front of other colleagues. According to these studies, rewards are not related to the enhancement of compliance. Others found only weak correlations between rewards and good practices related to password creation, storage, and change (Stanton, Stam, Mastrangelo & Jolton, 2005). This discrepancy in the results could be the natural consequence of the absence of reward systems in current IS departments. Since IS departments do not typically use rewards as an incentive for IS policy compliance, the survey questions might have been regarded as irrelevant by the respondents.

Several authors (Johnston and Warkentin, 2010; Vance, Siponen and Pahnila, 2012) tested the fear appeal, which is not induced by punishment, but is generated from an outside threat. The authors found that management should uncover the severity of an attack coming from a hacker, depicting the damage it can do to the work files of employees. This step will motivate IS users to abide by the security policies and protect their work files, thus indirectly protecting the overall organizational security. If the work files are compromised, organizational security is jeopardized.

Not just the severity of an attack, but also the efficacy of the security software in place and the self-efficacy of employees in applying the security software should be emphasized. Along these same lines, research has found that as long as employees

understand the damage of an outside threat to the company and perceive the company's security countermeasures as effective, their attitudes toward the policies will be positive and they will abide by them (Herath & Rao, 2009a and 2009b; Workman, Bommer & Straub, 2008).

Development philosophy (malicious threat). Although the encouragement approach has experienced resurgence in the case of negligent insider threats, it has yet to be explored thoroughly in terms of malicious insider threats, perhaps for a good reason: It seems counterintuitive to human logic to use a positive approach to deter abuse or criminal acts.

One of the measures of both negligent and malicious intents concurrently used the self-defense intention (SDI) construct and found that a physical security system (i.e., locks on server room doors) increases SDI, which in the study is composed of the intention to implement access control and intrusion protection software (Lee et al., 2004). Although the article failed to show SDI's impact on insider abuse, it does indicate that at least there was an attempt to measure a development approach (raising the self-defense intention). Nevertheless, the article was not clear whether it was testing the case of negligent or malicious insiders.

Practice shows that malicious insiders desire either monetary compensation from competitors who reward espionage or revenge following a salary cut or demotion (Shaw, Ruby & Post, 1998; Hunter, 2003). If this is the case, rewarding compliance financially (Dhillon & Torkzadeh, 2006) could be a promising construct to solve the problem of espionage, but it has not yet been tested empirically. It seems that deterring vengeance (sabotage) is harder than quenching materially felt needs (espionage) using a

development philosophy. Whatever the rewards of the development philosophy are, they need to be equal to or greater than the benefits of noncompliance perceived by opportunistic or malicious insiders. The perceived benefits of this criminal behavior can be lucrative. Using the organization's internet access for non-work-related activities is lucrative (convenience, saving personal time and money), and this lucrativeness negatively impacts compliance (Li, Zhang and Sarathy, 2010).

There is only one study (Peace, Galetta and Thong, 2003) that directly dealt with the theft of software and intellectual property (software piracy or copying), which is a form of espionage. Other than punishment certainty and severity, which are beneficial, a new solution was discovered. Decreasing software costs will lead to lowering the incidents of espionage or software copying. This could be a positive solution to deterrence, but it is restricted in scope and limited to software copyrights, rather than addressing overall security in organizations.

In summary, two major subcategories within the development philosophy have been studied to date, especially in studies of negligent insiders: 1) informing employees of the direct benefits of compliance (intrinsic and financial) and 2) informing employees about the indirect benefits of compliance (the security of their files). The indirect benefits include not having to undergo the re-creation of important work files upon losing those to successful outside virus attacks. We use the terms "direct" and "indirect," since the direct category of benefits is known and experienced daily by the employees. Employees only upon the condition of an attack and the unsuccessful mitigation of it know the indirect category.

Overall, deterrence and development philosophies are of little value if they are not written down and communicated to IS users. These two concepts, forming policies (writing down) and informing employees (communication) are discussed next under procedural countermeasures.

Theme 2: Applying Procedural Countermeasures

Procedural countermeasures are managerial practices that include forming policies, informing employees about them, and training employees on behavioral and technical skills to ensure that they are well aware of the threats and how to comply with IS policies, and thereby how to mitigate the threats. This section describes forming policies and informing employees, first the studies of negligent insider threats, followed by that of malicious insider threats.

Forming policies is not in and of itself a countermeasure mitigating noncompliance. But compliance cannot be assured unless there are written policies. Therefore, procedural countermeasures (having procedural policies) are the backdrop based on which the policies can be enforced or encouraged, and eventually followed or broken. Policies have two subcategories: First, the actual technical rules that increase the security of information systems (ex: not having organizational data on personal mobile devices like laptops, smartphones, iPads) and describe the punishments (or incentives) when a rule is broken (or kept). The second one constitutes the actual countermeasure or deterrence to noncompliance, nevertheless, since both are important and the first is a prerequisite for the second, both are described under the theme of forming policies. The IS policies that include the costs of noncompliance (sanctions) are imperative to deter IS misuse (D'Arcy et al., 2009), and when they include the benefits of compliance (rewards), they become

useful in encouraging compliance intentions (Bulgurcu et al., 2010). Thus, policies can serve both deterrence and encouragement approaches and will be described as such in the following section.

Forming policies (negligent and malicious threats). Among the earliest responses of IS departments to insider threats was the establishment of appropriate IS policies and codes of ethics. A security policy defines the rules and guidelines for the proper use of organizational IS resources (Straub & Nance, 1990). Yet the effects of codes of ethics have been found to be infrequent and negligible on computer abuse intention (Harrington, 1996). The same can be said of policies. Motivating compliance requires more than just framing and communicating policy to an organization's employees (Lim, Teo & Loo, 2002). Of course, we are not suggesting the abolition of written codes of ethics. Their importance lies in their legal functions, based on which organizations may take action if a violation occurs (Siponen & Vance, 2010).

User participation in policy formation directly raises the perception of improvements of security controls, which in turn increases the employees' policy compliance (Spears & Barki, 2010). When IS management makes employees aware of security risks and invites user participation in policy formation, employees realize that they have a valuable role in enhancing organization security. Thus, they will be more apt to comply with the policies they have contributed in creating. Other forms of user participation are whistle-blowing policies and technical tools. When the users are empowered and encouraged to report computer abuse in the workplace and the system or reporting procedure is anonymous, there is an increase in the willingness to report the

abuse or noncompliance, and therefore the overall efficiency of security is enhanced (Lowry, Moody, Galetta and Vance, 2013).

A small number of studies considered the implications of policy characteristics on compliance. Characteristics may include things like policy age, frequency of update, and clarity. One study showed that the degree of specificity of IS policies (detailed explanations) may increase the employees' perception of the mandatoriness of compliance (Boss et al, 2009; Kirsch & Boss, 2007). Another study found that ISsec policies' existence, longevity, updates, scope, and adoption of best practices have no significant impact on the existence and severity of security breaches (Doherty & Fulford, 2005). We think national differences could be at the root of this discrepancy. The first study was conducted in the US, but the second in the UK. Americans put a greater emphasis on punctuality than their UK peers (Fullbright Commission, 2015), which may explain why American employees are more positively affected by IS policy age, updates, and clarity than their peers in the UK. This raises the question of whether the same countermeasures are equally valid in different cultural contexts. Future research may shed light on the universality of the effectiveness of countermeasures as well as on the different philosophies of deterrence and development. Another explanation of this discrepancy may be the finding that UK policies (at least, of the healthcare sector) do not promote understanding and are not clear enough (Stahl et al, 2012).

A number of articles tested policies or codes of ethics to see their impact on IS malicious misuse. For example, guidelines and policies for acceptable system use and the dissemination of information about penalties communicate deterrence (Straub, 1990; Straub & Nance 1990; Straub & Welke 1998). Similar to the negligent insider case, these

policies may lose effect if they are not effectively communicated to employees (Straub & Welke, 1998) and followed by the enforcement of sanctions in case of a breach (Straub & Nance, 1990).

In summary, IS policies are the backbone of countermeasures to deter negligent as well as malicious threats, but only the *awareness* of IS policies, not the mere existence of them, decreases IS misuse intention (D'Arcy & Hovav, 2007). Although awareness was described superficially in theme 1 (related to the awareness of sanctions), in the next section it will be described in an extensive way, encompassing not just the awareness of sanctions, but the awareness of what to do and how to do it, in relation to policy compliance.

Informing Employees (negligent threat). This subtheme speaks about the communication of both managerial policies and technical information to users. Knowledge of managerial policies is helpful to both types of insiders but technical knowledge is specifically helpful to negligent IS users. After all, no IS department wants to send a potential malicious or abusive employee to advanced training to gain additional technical knowledge of the systems.

Employee security awareness and training may come not just from within organizations, but also from without the organization via self-education (Hsu et al 2015). Nevertheless, informing and educating the users in the organization can take many forms other than technical education or communication of managerial policies. For example, informing employees about basic security practices will make them conscious enough to not share confidential data with others on public forums (see Smith et al, 2012) or on social media. In our study, this type of education is labeled raising behavioral knowledge.

Thus, communicating behavioral knowledge may include raising *awareness* of IS policies, their related sanctions and incentives as well as good security practices at work. Communicating technical knowledge may include raising users' perceptions of self-efficacy, reducing response costs, and increasing response efficacy. These two dimensions are discussed next.

Behavioral Knowledge. Among negligent insiders, SETA programs can decrease IS misuse intention (D'Arcy et al. 2007, 2009) (SETA programs are named "cues to action" in Ng, Kankanhalli, and Xu, 2009). Bulgurcu et al. (2010) confirmed the role of IS policy awareness in increasing the perceived costs of noncompliance and the benefits of compliance. Informing employees about IS policies through SETA programs is not the only channel for raising awareness among employees. Other channels include requiring users to participate in security risk management (SRM), which raises employee awareness of ISsec risks (Spears & Barki, 2010).

Awareness campaigns do not have to include awareness about policies and procedures only; they may also include educational materials for employees on how to notice suspicious employees doing suspicious activities (Dhillon & Torkzadeh, 2006) as well as on how to be aware of social engineering techniques employed by outsiders or malicious insiders. Clicking on phishing links or responding to an email allegedly, coming from the IT department and wanting the username and password are well-known hackers' social engineering techniques to breach security. Building a robust behavioral knowledge among the employees may mitigate these types of threats.

Technical Knowledge. Self-efficacy and response efficacy comprise the technical dimension of awareness. These are technical know-hows that are different from the behavioral policies. Security compliance self-efficacy is an employee's perception of his or her technical ability to abide by the policy (Warkentin et al, 2011). The second subtheme (response efficacy) is employees' perception of software effectiveness in preserving security.

Self-efficacy positively impacts IS policy compliance (Boss et al, 2009; Bulgurcu et al., 2010; Herath & Rao, 2009; Johnston & Warkentin, 2010; Warkentin, Johnston & Shropshire, 2011; Workman, Bommer & Straub, 2008). If an employee has been trained to skillfully respond to any policy demand (ex: training on password behaviors, Stanton et al, 2005), he or she will be apt to comply with the policy more than the employee who is poorly trained. "Resource availability" is a similar term advanced by Herath and Rao (2009a) and refers to the robust training of employees who subsequently tend to perceive themselves as more competent to comply with IS policies than the poorly trained employees.

"Response efficacy" explains the effectiveness of IS policies or packages to protect information (Johnston & Warkentin, 2010). A higher perception of response efficacy is associated with the intention to comply (Johnston and Warkentin, 2010) and a decrease in noncompliance (Workman, et al., 2008). Adopting and disseminating awareness about powerful security tools in IS departments seems to be promising in encouraging IS policy compliance.

Informing employees (malicious threat). Pertaining to malicious threats, all the research dealing with IS policies also deals with IS policy awareness, which includes

communicating information about sanctions upon failure to abide by IS policies (Straub 1990; Straub & Nance, 1990; Straub & Welke, 1998). SETA programs dominate a good number of the papers categorized as dealing with negligent insiders, but the literature is silent on how SETA programs help the potential malicious insiders to devise their cunning plans. The question remains, if IS management cannot differentiate between potential negligent and potential malicious employees, and they provide training for all, does this training make the potential malicious insiders more knowledgeable or more capable of breaching the security? Cronan, Foltz and Jones (2006) may shed light on this subject. The students who were aware of the university policies were more prone to circumvent these policies than the students who were unaware of the policies. Furthermore, tech savvy students had a greater tendency to commit computer misuse than regular students (Cronan et al, 2006). The question is: If tech savvy students are more prone to breach security, is this also true for tech savvy employees? In addition, how does increasing training in organizations relate to that? Future ISsec research may find out what the right answers are.

Another observation in this dissertation is the following: Why is it that "the informed and the trained" in organizations are complying, "the informed, and the trained" in universities are noncomplying? A possible explanation is the following: If the difference in the two settings is the presence (or absence) of forces such as accountability (its presence in organizations and its absence in universities), this then raises the question of whether the reality of compliance in organizations is due to the increase in awareness and the increase in self-efficacy or whether it is due to the presence of accountability. Since awareness of consequences (ex: punishment) significantly impacts attitude on

ethical decision making (Leonard et al., 2004), this could mean that awareness and training may help only in the presence of deterrence measures. Another possible explanation is that students pay (they are the customers of universities) whereas employees earn. This could mean that customers may be upheld to a lesser degree of compliance rather than paid employees.

In summary, educating employees is the fourth most widespread protection mechanism employed by organizations after the use of passwords, media backup and virus protection software (Whitman, 2004). Since SETA programs may include ethics training, it is important for organizations to understand that ethics training is beneficial only with the employees who follow the rules out of social conformity and those who exhibit high levels of self-control (Workman & Gathegi, 2007). Although the "E" (education) in SETA programs does not ensure 100% compliance, it does significantly affect a section of the employees who have certain individual characteristics.

Training is important, but equally important is the method, the context, and the situational conditions of the training. In Puhakainen and Siponen's (2010) action research, they found that the integration of ISsec training with the companies' normal daily business communication was crucial in enhancing users' motivation to comply with the ISsec policies. In the same study, the authors found that continuous training, rather than a one-time training effort, increases compliance.

Forming policies, communicating them, and educating employees are like putting "do not enter" signs on roads. These signs are sufficient for most citizens, but not enough for some: some need physical barriers blocking the entrance of the road or hidden cameras watched by police officers to monitor movement. The notion of barriers and

monitoring is the dimension depicted by our next theme: technical countermeasures that control access to systems and monitor the traffic on the networks.

Theme 3: Applying Technical Countermeasures

The theme of applying technical countermeasures in organizations to ensure compliance is one of the least studied themes regarding insider threats in the information systems literature, probably because the computer science literature may have been attracting all the technical studies and experiments. Nevertheless, the socio-technical aspect of technical countermeasures needs more attention by ISsec research because of its importance.

For example, the mere presence (or the absence) of technical countermeasures (ex. software monitoring) depicts the deterrence (or development) philosophy adopted by IS management. Monitoring the IPs of employee computers to know who failed to update the security software is a good example of a strict deterrence approach. The absence of such a strict measure could signify that IS management is less serious about deterring noncompliance or at least less serious in using technical means to achieve deterrence and sends the right (or wrong) message to the users. Another example is the impact of advance notice of technical monitoring: it seems the advance notice does not just enhance deterrence, but it also cultivates trust between the employee and the organization. The advance notice of Internet usage monitoring has been shown to build trust between employees and organizations (Alder et al., 2006). We suggest that the studies on the socio-technical dimension of compliance need not be neglected nor left to computer science field. Computer science is purely technical; the very essence of Information Systems research is to address the socio-technical side of the countermeasure's impact.

Technical countermeasures (negligent and malicious threats). An important factor of enhancing technical countermeasures to deter IS misuse among negligent insiders is user participation in the design, creation, and implementation of technical preventives and access control (Dhillon & Torkzadeh, 2006; Spears & Barki 2010) in the security risk management planning process. This technique positively influences the performance of technical security controls among users. It is true that technical controls are somehow used to deter negligent threat, but using them to deter malicious threat is even more accentuated in ISsec literature.

In the case of malicious insider threats, the studies examine computer monitoring, access control, and auditing logs as ways to control and secure the systems technically. Tracking down questionable activities on the network and the subsequent punishment of perpetrators are the direct value of preventive countermeasures (Straub & Nance 1990, Straub & Welke 1998). Another indirect albeit important deterring value in using technical preventives is that the awareness of deterrence philosophy is communicated through these technical means. Technical preventives do not just block an employee from accessing an unauthorized database, they also deter all employees from accessing unauthorized databases if, for example, the system generates a monthly report on each and every employee's accessed files and databases and sends copies of the report each month to the respective employees and to their supervisors. The key issue here is that IS users should be aware of such countermeasures (Straub & Welke 1998) (through the report, in this example) for this channel to have a deterring effect. The presence of a monitoring system is usually communicated to employees by directly informing them about the presence of such a system (D'Arcy et al, 2009; Straub 1990).

A more specific monitoring system is the community anomaly detection system (CADS), which extracts relational patterns in the patient records' access logs among work team members. Based on relational patterns, it detects a deviation from the pattern and sends a notice to security analysts to investigate the access logs of the user in question (Chen et al., 2012b).

Although the significance of increasing the awareness of technical countermeasures as a deterrence measure has been proven in the literature, we argue that past research dealt with this countermeasure in a one-sided manner. There could be side effects of making employees aware of the types of technical countermeasures used. Potential opportunistic or malicious insiders could take advantage of such information and devise their acts accordingly. Therefore we propose two layers of technical countermeasures, declared and undeclared. The declared ones may deter the majority of employees from thinking about circumventing policies, and the undeclared ones may catch those who attempted to circumvent the known countermeasure by other ways.

In summary, applying technical countermeasures provides another layer of protection. This theme is in need of further IS research to cover the socio-technical side. The journals in the computer science and engineering disciplines contain extensive research on technical countermeasures, including access controls, password mechanisms, and firewalls (Siponen & Oinas-Kukkonen, 2007). Future IS research should study the socio-technical effects of these technical countermeasures on insider behavior. We argue that this is an IS issue (socio-technical) rather than just a computer science issue (technical), because in the case of password changes for example, employees may devise ways to circumvent technical countermeasures. Therefore purely technical means should

not be addressed in IS research without studying at the same time the technical measures' effects on the employees.

Theme 4: Enhancing the Environmental Countermeasures

Environmental countermeasures constitute the fourth and final theme of this section of the literature review, after treating the themes of philosophies and procedural and technical countermeasures. The socio-organizational values, assumptions, and expectations play a role in insider threat security research (Dhillon & Backhouse, 2001). Therefore this section will address the social environmental aspect of IS policy compliance in the following paragraphs.

The social environment plays a role in channelling deterring or encouraging messages to IS users. For example, negligent employees may experience shame inflicted on them by other more compliant employees. This social embarrassment channels a deterring message to other potential negligent insiders. This overarching theme of environment includes not just shame (which is part of subjective norms), but also organizational commitment and ethical climate, among others. This theme can be grouped into two sections: external and internal. The external environment depicts the organizational characteristics, including subjective and descriptive norms, and the overall social and moral environment within the organization. The internal environment depicts the individual characteristics of the employee, including his or her moral character.

External environment (negligent threat). Pertaining to negligent threats, ethical, professional, legal, and societal environments and climates in an organization could increase or decrease ISsec policy compliance intentions (Banerjee et al, 1998; Leonard et

al. 2004; Posey, Bennett and Roberts, 2011a). The two major expressions of the external environment of organizations are subjective norms and descriptive norms.

Subjective Norms: These norms refer to the perception of the IS user regarding whether his or her immediate significant environment (managers, colleagues, etc.) expects him to perform a certain behavior (Herath & Rao, 2009). Subjective norms are the same as normative beliefs, which increase ethical behavior intention regarding IS use (Leonard & Cronan, 2001; Pahnila et al., 2007; Siponen et al, 2010). If a manager has high expectations of his subordinates, it is likely that this will affect the behavior of the majority of the manager's employees. Johnston and Warkentin (2010) named this construct "social influence" and found, like Herath and Rao (2009a), that social influence impacts behavioral intentions. Along the same lines, Banerjee et al. (1998) found situational characteristics (conventional beliefs and high expectations of managers) that increased ethical behavior intention. In an opposite result, Siponen and Vance (2010) found that the impact of shame is becoming nonsignificant when measured in the same model along with neutralization techniques used by employees. This means that the countermeasure results are not solely dependent on the message communicated from outside the person. but also on the individual characteristics from within him or her, which will be elaborated on more fully in the internal environment section below.

Although neutralization is a cognitive technique, other non-cognitive forces may neutralize shame and the effect of organizational security culture on the employees. For example, virtual status is the level and degree of business activities that an employee implements from different remote locations compared to within the organization itself (D'Arcy and Devaraj, 2012). D'Arcy and Devaraj found that virtual status increases

technology misuse intention. This misuse may be due to the absence or decrease of the effect of organizational security culture on the employees (shame or subjective norms are neutralized in this case).

Descriptive norms refer to the perception of an IS user as to whether his or her colleagues are abiding by the IS policies or not. Herath and Rao (2009a) found that descriptive norms positively affect intention to comply. Banerjee et al. (1998) included role models in their description of situational characteristics and found that good role models affect the ethical climate of the organization and channel a message of encouraging compliance.

External Environment (malicious threat). Pertaining to malicious threats, subjective norms have no significance in contrast to negative descriptive norms (bad role models), which show significance. One of the major predictors of computer crime is associating with friends who engage in the activity (Skinner and Fream, 1997). In other words, learning computer crime is primarily peer driven, which could be an echo of descriptive norms. Regarding subjective norms, Hu et al. (2011) found that whereas shame had no impact on malicious insiders, it was an effective deterrence on negligent insiders. Shame is not effective on malicious insiders, probably because, malicious minds are not deterred that they will be shamed in front of others in society.

In summary, developing and sustaining an ethical environment maximizes ISsec (Dhillon & Torkzadeh, 2006). In this review, the external environment captured organizational subjective and descriptive norms in their positive (reasonable expectations, role model) and negative (social pressure, differential association) dimensions. Whereas

the external environment deals with the issues outside and around the individual, the internal environment deals with the issues within him or her.

Internal Environment (negligent threat). The internal environment is the personal individual moral convictions of each employee, including ethics, morality, organizational commitment, apathy, denial of responsibility, neutralization techniques, individual propensity and locus of control. For example, individuals who have an internal locus of control take responsibility for their own actions, and therefore may be less inclined to omit ISsec precautions at work (Workman et al, 2008).

On the negligent level, Banerjee et al. (1998) talked about individual *ethical* characteristics that influence behavioral intent and high moral commitment that decreases IS misuse intention (D'Arcy et al., 2009). Gattiker and Kelley (1999) applied different levels of morality to the IT environment: personal (preferences and tastes), conventional (societal norms that dictate the perception of non-harmful but unacceptable behaviors), and moral (social norms that dictate the perception of harmful acts). The latter study not only found that users differ from each other within the domains of morality, but also that young male employees are more vulnerable to err in the moral domain. Cronan et al. (2006) agreed, finding that males committed more IS misuse than females. Loch and Conger's findings in 1996 may hint at a solution for the gender issue. The findings suggest that men make ethical decisions in computing acts based more on their attitude toward the ethical scenario rather than on the social norms, while woman intend to act ethically or unethically based more on the social norms, rather than on their attitude. This study tells us that men and women do not respond in the same way to the same countermeasures to the same degree. IT professionals probably need to work on the

attitudes of men toward compliance, while the expectations and pressures of the socio-organizational environment will drive women toward compliance. Social norms do not seem to significantly impact the morality of males in order for them to act ethically in computing acts (Loch & Conger. 1996). This finding suggests two things: first, the internal environment is a moderator of the relationship between procedural/technical countermeasures and employee compliance, and second, there is no one size fits all strategy toward the different types of insiders but rather strategies should be customized based on broad but different psychological characteristics. This issue needs more investigation in future research.

Siponen and Vance (2010) studied neutralization techniques and found that employees with high usage of these techniques were more inclined to violate IS policies. The scenario examples of their study include the following items: "It is not as wrong to violate a company ISsec policy that is not reasonable" and "It is all right to violate a company ISsec policy if you get your work done." This echoes what Harrington found to be true in 1996 in one of her IS ethical hypotheses: "employees with high responsibility denial have a propensity to enact computer abuse."

Along the same lines, organizational commitment was found to significantly increase intentions to comply (Herath & Rao, 2009), and apathy was found to decrease precautions taken to secure systems (Kirsch & Boss, 2007). Therefore, IS management should build the moral reasoning and organizational commitment of their employees by working on improving the internal and external ethical climates. Education has been proven successful in shaping the acceptable moral reasoning of individuals (Davis 1987; Rest 1979; Thoma & Davison 1983). Another promising way to increase compliance is

through legislation. Governmental regulations on IS policies increase individual beliefs in IS compliance (Cannoy & Salam, 2010). Thus, organizations can push governments to legislate ISsec policies. This will help increase compliance in organizations.

Internal environment (malicious threat). Regarding malicious insiders, an interesting insight comes from the canonical correlation analysis done by Shropshire (2009), when he analyzed documented stories of malicious and opportunistic insiders who were legally prosecuted in the past. The independent variables of this study were financial changes, relationship strains, substance abuse, and job changes; the dependent variables were IT sabotage (i.e., destroying data) and IT espionage (i.e., selling data). The results showed that only financial changes in the life of an employee correlated with IT espionage: financial crises moved employees to sell information to competitors. Relationship strains, substance abuse, and job changes correlated with IT sabotage. These findings may give IS management insights on the importance of scanning, profiling, and keeping a supervising eye on the changes in the lives of employees. The application of these findings is not unique to IS employees; nevertheless, IS management needs to apply these proactive methods to keep malicious insiders at bay.

One of the major predictors of computer crime is associating with friends who engage in the activity. Learning computer crime is primarily peer driven (Skinner & Fream, 1997), and peer behavior positively influences policy compliance intention (Herath and Rao, 2009b). Therefore, IS management should take heed to cultivate an IS department with the highest standards of moral and ethical behavior. This does not necessarily mean that IS departments should be saturated with the uncomfortable tension of shame, especially since shame and informal social sanctions are not promising

constructs in deterring the misuse intentions of malicious insiders (Hu et al., 2011). However, attracting and keeping a large base of ethical employees and encouraging them to expect the highest standards of IS policy compliance from their peers should deter potential malicious insiders from acting on their schemes.

A third insight of securing the environment is found in Son (2011).The congruence between employees' intrinsic values and organizational values will encourage employees to abide by IS policies. Therefore, IS management should survey potential employees and only accept those whose moral values coincide with those of the organization, although this might not be realistic in the cases of outsourcing the service where IS management has no control over the employees of the provider. Future research should investigate the best ways to implement this congruence.

It has been noted how neutralization techniques nullify the impact of formal and informal sanctions in the case of negligent insiders (Siponen & Vance, 2010). In the case of malicious insiders, this relationship may also hold true. Investigating new techniques to profile and identify malicious insiders or perhaps to empirically test the situational and behavioral characteristics or criminological settings (Banerjee et al. 1998; Willison & Backhouse, 2006) are some areas for studying malicious employees in the future.

In summary, the internal environment captures the ethical dimension, morality, organizational commitment, apathy, and neutralization strategies, all initiated within and related to the individual characteristics of the IS user. Promising countermeasures on the level of the internal environment are pre-employment screening, profiling, and training. Overall, the theme of environment covers the external (organizational climate) and internal environments (individual characteristics) that affect IS compliance. Lately, some

authors (Chen, Ram and Wen, 2012b; Hu, Dinev, Hart and Cooke, 2012) have started using the term "security culture" in organizations, which is along the same lines of what this dissertation called environmental countermeasures.

In summary, the ISsec policy compliance literature depicts the affordances of ISsec policy compliance, "its positive side", and seldom touches on the potential downsides of IS security policy compliance. The next section draws on practitioner journals (and some handful academic articles) to consider some of the downsides of ISsec policies.

Review of the Downsides of IS Security Policy Compliance Efforts

This section will describe the few academic articles that touch on the subject of the downsides of ISsec policies. The description of the practitioner journals follows. I first reviewed the abstracts and the research models of 105 peer-reviewed articles regarding ISsec policy compliance from 1990 to 2015 in the senior basket journals, as well as from Lowry et al.'s 2004 rankings of 25 top IS journals. The majority of the articles assumed that increasing ISsec policy compliance is de facto good. Only one article (D'Arcy et al., 2014) dealt specifically with the downsides of ISsec policy compliance. That article studied security-related stress caused by burdensome, complex, and ambiguous ISsec requirements.

Although there is enough indication in the practitioner journals toward the downsides of ISsec policies, peer-reviewed academic ISsec research has not studied this important dimension well. The closest IS academic literature that comes to the notion of downsides is the marginal testing of "response cost". Response cost is the employees' perception of IS solutions as being too cumbersome for daily activities. The response to

comply may impede employees from giving their best to their projects. "Perceived response cost work impediment" and "perceived cost of compliance" are the terms used for this dimension of technical awareness. These constructs significantly affect attitudes toward solutions and intentions to comply (Herath & Rao, 2009a; Bulgurcu at al., 2010). These results are few and sporadic.

If, at least hypothetically, the dimension of ISsec measures' downsides requiring ever-increasing ISsec policies increases ISsec breach risk instead of decreasing it, then academia has neglected an important and dangerous area of research. There is some empirical support for some generally negative or adverse effects of security requirements on employees. For example, a perceived work impediment increases the perceived cost of compliance with security policies, thus indirectly affecting the intention to comply with security requirements (Bulgurcu et al., 2010). Herath and Rao (2009) named the work impediment "perceived response cost." There is also evidence from the psychology discipline regarding computer monitoring negatively affecting the perception of employees of the organization and increasing adverse behavior from employees (Alge, 2001). A decrease in commitment and an increase in workplace deviance may occur (Alge et al., 2006; Ariss, 2002; George, 1996). Even though organizations may think that monitoring prevents organizational resources abuse or misuse, providing a method to evaluate user performance, deterring security breaches, and defending the institution in legal issues (Ariss, 2002; Martin & Freeman, 2003), employees may have a directly opposite and negative perception of organizational "snooping" (Dunn & Schweitzer, 2005).

Security is often not perceived as an end user task (Besnard & Arief, 2004). From the end users' perception, evaluation is directly linked to job performance (e.g., high enrollment numbers for a director of graduate program), not security performance or security policy compliance. One survey reported that employees tend to consult with their direct managers, rather than IT personnel for directions on ISsec related issues (Cisco, 2006). This make sense since an employer may consult with a manager (rather than IT department) in resuming or stopping the use of a web analytics tool designed to increase outreach and enrollment numbers in a graduate program, even if the IT department is discouraging the use of that tool for privacy and security reasons. One of the goals of IT management is to strike a balance between the need to secure information assets and the need to enable the business (Kayworth & Whitten, 2010). Many of the adverse effects of security requirements can be due to the loss of this balance. Employees often perceive of security requirements in terms of the cost and benefit of compliance (Bulgurcu et al., 2010) and understand security requirements as constraints and limitations on their job performances (Dourish et al., 2004; Post & Kagan, 2007). Siponen and Vance (2010) reported in their action research study that some employees did not follow the email security requirement in an organization because "overload, hurrying, suddenly emerging situations and unplanned assignments hindered their compliance with the email policy." Nevertheless, since the study's focus was on pre-determined goals and actions for increasing compliance through training, the aspect of overload "was not to be addressed by the action research intervention", keeping the question unanswered and the phenomenon of downsides of the downsides of ISsec measures under researched.

All of these studies regarding the adverse effects of ISsec policies share the shortcoming of not adequately explaining the mechanism and the constraints of ISsec measures. This dissertation summarizes the problem in a theoretical model describes the downsides of ISsec measures and explains the relationship among the security measures and the adverse effects on productivity and security. Why and how IS security measures negatively affect productivity and security itself are discussed next in the analysis and results sections, after the methodology of the grounded theory employed in this study is described and elaborated.

CHAPTER THREE

Methodology--Grounded Theory

Grounded theory (Corbin & Strauss, 2008; Strauss & Corbin, 1990, 1998) was chosen as the methodology of this dissertation since it is a methodology that enhances theory discovery (Martin & Turner, 1986), and no theory has been formed to date to explain the potential side effects of ISsec policy compliance enforcement.

Grounded theory does not force-fit data to a priori theory and hypotheses; rather, its aim is to derive theory from data (Corbin & Strauss, 2008). The theory to be developed in this approach is intimately tied to the data to the extent that the resultant theory is likely consistent with empirical observation (Eisenhardt, 1989). Most of ISsec compliance research involves quantitative studies assume that forcing ISsec policy compliance is good. The major objective of this dissertation is to build theory from the data (Orlikowski, 1993; Corbin & Strauss, 2008) on the topic of the downsides of IS security measures. The grounded theory has three basic components: 1) theoretical sampling and site selection, 2) data collection, and 3) data analysis and validation (Corbin & Strauss, 2008; Glaser & Strauss, 1967; Strauss & Corbin, 1990; Strauss & Corbin, 1998).

Theoretical Sampling and Site Selection

In terms of theoretical sampling, Glaser and Strauss (1967) advised that particular attention needs to be given to theoretical relevance, purpose, and similarities and differences across data sources with regard to the suitability and adequacy of the data

collected. Pertaining to relevance, a site was chosen that best capture the intention of the research.

A field study was chosen to investigate the outcomes and the dynamics of enforced security policies. The research required a site where users could exercise a significant level of information disclosure without being hindered by fear of retaliation from management. Another criterion for the site was the ability of the IT department to implement an increased level of security policy. The chosen site is a North American mid-sized university, which is *a private higher education institution* (hereafter "PHEI") where users (usually faculty, staff and administration) have considerable autonomy from IT management. Since faculty evaluations follow a different channel than organizational employee evaluation in a typical workplace, faculty (the majority of the users interviewed in this dissertation) have autonomy on their decisions, regardless what the IT department demands of them. This is important because the faculty have higher freedom to critically assess the IT department's decisions, in this case on security issues. Plus, this selected site had recently implemented an increased level of security policy, namely the double authentication Virtual Private Network (VPN), which allowed us to investigate the positive or negative impacts of this move. The following quotes from users and IT client services (which act as a bridge between the client and the IT department) depict the rigidity of the ISsec policy implementation:

> PHEI - IT security department has set the bar quite high, and I don't necessarily fault them for that, but I do think that it's a case where, because of their decision to set that bar high. . . you could argue it restricts certain business functions or business opportunities for the [name of the] school. I guess I want to be careful that I'm not saying it's necessarily... it's not unnecessary, but because the expectation, the threshold has been set so high for security that it is restrictive to business process for us as a school (Respondent 20, director of a computer center).

An IT client services staff member, who bridges the faculty solution demands and the IT department, expressed that the IT department sometimes are requiring beyond what even the banking industry requires. The IT staff who found an application from an outside solution provider, and whose solution was rejected based on some security reasons from the IT security team, complained with the following words:

> There's a product that we were looking at, and it had credit card integration, and PHEI was requiring security measures over and above what banks and retailers currently require for credit card data, and this company was like, "Well we can't support that yet." (Respondent 5, project manager in instructional technology, IT client service professional).

On a different subject, an administrator was trying to find software for a business problem he had. He approached IT department, nevertheless the IT department did not give the approval of the purchase of the software due to security reasons. Furthermore, IT department could not give adequate and viable solution to his departmental and business needs. For this respondent, security reasons blocked or hindered his productivity.

> I say that as an educated security person. Obviously, there are breaches of personal data in the news every day. Maybe PHEI knows something I don't, but when I hear that other, larger companies are able to work around this, why is PHEI taking so much time to figure this out? That's a little frustrating (Respondent 30, director of a graduate program).

This makes this site a more interestingly valid site for investigating the concrete and emotional results of ever increasing ISsec policy compliance. In order to find out the constraints (and the affordances, in order to not be biased) of the information system policies, interviewing both IS users and IT professionals was adequate to compare and contrast the enablement and constraints of different types and levels of professionals.

The Site

The site selected in which the analysis was conducted is a private university comprising ten colleges employing approximately 1,000 staff and faculty; it is a

nationally ranked research institution noted as having "high research activity" by the Carnegie Foundation for the Advancement of Teaching. As of the date of this research, the university had a range of $250 and $350 million in operating cash, with total assets between $2 billion and $4 billion (these are ranges to conceal the identity of PHEI). Thus, ISsec policy compliance is very important to maintaining ISsec. The university not only has a chief information officer (CIO) but also has a chief information security officer (CISO) position (created in 2008). Many universities have been hacked in recent years. In 2015 alone, three major high profile security breaches hit Penn State University, the University of Connecticut, and the University of Virginia (Wagstaff and Sottile NBCNews, 2015). However, at the time of this research, PHEI has never been hacked, breached, or reported in the news. The site is at the forefront of security implementations and is setting a pattern for other institutions, according to the CISO. In 2014, double authentication VPN was implemented so that those users who were overseas and or off campus who wanted to access specific systems were not able to access the network without a new authentication level (a code sent to an app on their smartphones). The trend for the coming years is that PHEI is going toward making the majority of the systems not accessible without a double-factor or double-authentication method. Since passwords are breakable, the CISO believes that this is the only secure tool currently available for the institutions to secure their information assets.

Data Collection

Data collection consisted of conducting 32 semi-structured interviews across the research setting (see Table 3.1), including two follow-up interviews. A gatekeeper who is a faculty and chairperson in one of PHEI's departments facilitated access to the site. The

gatekeeper personally knew both the author of the dissertation and the CISO of PHEI. This knowledge helped the author to gain trust and access to interview not just PHEI's most senior IT personnel but also to have almost free access to interview whomever the author wished. The gatekeeper's email and mediation with the CISO tremendously helped this research in a site and a sensitive security subject that would have been next to impossible to conduct.

Faculty members, department chairs, faculty, and administrative staff in one of the schools were among the main end users of the information systems who were interviewed in PHEI. To retain accuracy, all interviews were audio-recorded and transcribed to text. The text documents were then used in the data analysis phase of the study. Five types of data were collected: 1) interviews with the IT department, 2) interviews with end-user professionals, 3) internal documents on ISsec policies, 4) Q&A emails exchanged with IT security specialists, and 5) notes taken upon attendance of a security awareness meeting designed for end users. However, the IT management for security reasons denied the researcher IT helpdesk observation time. The average length of the interviews was around 30 min each (with lower and upper range going from 17 to 48 min). All of the PHEI's IT and IT security policies were read (a total of 43 web pages), and one security awareness meeting was attended. The interviews were conducted in 2015 over a period of four months. Each interviewee was initially contacted via email. The interview guide (See Appendix A) was developed by the researcher with the input of a panel of 5 academicians with the intention of eliciting specific opinions/observations on ISsec measures. The study was constructed to ensure the participant's viewpoint rather than the researcher's viewpoint. Nevertheless, the researcher needed to configure

appropriate follow-on questions, or in some cases, develop additional avenues of inquiry for the next set of interviews since elaboration and clarification are crucial elements of the interview process (Marshall & Rossman, 2011, p. 145). The interviews were recorded after gaining specific approval to do so from each participant. The interview questions were more semi structured in the early phases of the research with a general selection of interviewees. As concepts began to develop through open coding, the selection of interviewees and questions started to converge to the emerging concepts (Orlikowski, 1993).

Data Analysis Methodology

The units of analysis include the individual opinion (enablement and constraints) of ISsec policies and the reactions (both affective and behavioral) of the users to the new IT security policy (double-factor VPN authentication), as well as opinions about IT security policies in general. Nvivo 10 software was used to code the data, following qualitative data coding procedures (Miles & Huberman 1994; Myers, 2009). With the emergence of themes through data analysis, interviewees and questions were selected based on the emerging themes (Orlikowski, 1993). The analysis of the data followed the lines of three coding phases: open coding, axial coding, and selective coding (Strauss & Corbin, 1990, Gasson, 2004; Orlikowski, 1993; Strauss & Corbin, 1998). The following paragraph concisely describes the three phases.

Open coding is a content analysis technique to classify data into concepts emerging from the data rather than forcing concepts on the data from outside sources. Axial coding seeks to group the concepts into an umbrella theme; it finds connections or

Table 3.1.

Descriptive Interviewee Sample Pool

Position	# of Interviews
Advanced Technology Repair Specialist	1
Assistant Director, Academic and Research Computing Services	1
Assistant Professor – tenure track	1
Assistant Vice President & Chief Information Security Officer	2
Assistant Vice President for Client Services	2
Associate Librarian	1
Coordinator, Academic Support Services in a School	1
Desktop Configuration Specialist	1
Director of a Computer Center	1
Director of Budget Management	1
Director of IT Client Services	1
Director of Communications & Marketing	1
Director of Hardware Support & Technology Systems Consultant	1
Director of Online Teaching and Learning Services	1
Director, Client Support Services	1
Director, Graduate Business Degree Programs	1
Director, Undergraduate Programs	1
Office Manager 1	1
Office Manager 2	1
Professor 1	1
Professor 2	1
Professor and Chair 1	1
Professor and Chair 2	1
Project Manager, Instructional Technology	1
Senior Academic Consultant	1
Senior Academic Consultant, Faculty Technology	1
Senior Analyst/Programmer	1
Software Support Specialist 1	1
Software Support Specialist 2	1
Temporary Full-Time Lecturer	1
Total:	32

relational meaning among the concepts that emerged in the axial coding phase and puts them in a comprehensive scheme (Kock, 2004, Orlikowski, 1993). This phase allows the researcher to focus and narrow the analysis (Glaser & Strauss, 1967). After conducting

open and axial coding, selective coding is implemented, which is a grounded theory technique that draws relationships among the emerged themes (Strauss & Corbin, 1998). The theoretical relationships between the six themes are detailed in the findings. Examples of grounded theory research in information systems are found in the studies of IS development projects (Gregory et al., 2013), the role of IS in competitive actions and firm performance (Vannoy and Salam, 2010), the enhanced use of IT (Bagayogo et al., 2014), and the characteristics of software development team members (Siau et al., 2010). An example of research in ISsec is found in the dissertation work regarding managerial effectiveness in ISsec (Knapp, 2005).

During the open-coding process, emerging concepts in the data were constantly compared with previously identified concepts to identify patterns in the data. The point of saturation for data collection and analysis was achieved whenever no new concepts emerged from the data and when identified concepts repeated themselves in the data (Glaser & Strauss, 1967). At this point, the identified concepts were grouped in themes through axial coding. The goal of axial coding is to create themes to represent various concepts identified in the transcribed manuscripts. In terms of data analysis, the researcher used constant comparative analysis to guide the effort. This form of analysis allows for an evolution of themes, concepts, and categories from the data collected (Sarker & Sarker, 2009). Furthermore, this dissertation follows the interpretive method drawing on adapted from the methodological guidelines of Sarker and Sarker (2009, p.445), which is a seminal work in interpretive methods. For the detailed illustration how the interpretive method was employed see Appendix B.

Validation

The author conducted the validation process in two phases: a comparison of the themes with the extant literature and validation by participants. Following Eisenhardt (1989), the findings (the relationship among the themes) were compared with the extent literature (as much as they were tested in the extant literature) in the areas of enforced ISsec policies (Straub 1990; Chen et al., 2012a), ISsec awareness (D'Arcy et al., 2009; Diven & Hu, 2007; Karjalainen & Siponen, 2011), the policy sabotage of IS users (Guo et al., 2011), frustration with technology (De Guinea & Markus, 2009) and technology use (or lack of it) and its impact on productivity (Franzten 2000; Kleis et al.,2014; Quatraro, 2009). These types of comparisons enhance generalizability and provide an additional level of theoretical relevance by observing similarities and differences that are characteristic of the resulting theory versus the extant literature (Eisenhardt, 1989). In the second phase of the validation, six of the study's participants (almost 20% of the total interviewed) reviewed and legitimized the findings. It is important to notice that member checking technique is the "most critical technique for establishing credibility" (Lincoln and Guba, 1985; Creswell, 2007).

Furthermore, this dissertation applied the method of source triangulation: the interviewees were of different sources. Directors who are faculty members, directors who are staff, faculty who are at the same time chairpersons and faculty who are not holding any administrative role, all of them gave their input. Some staff members interviewed were administrators, others were not, some ITS were senior staff members, others were junior in their position. Some ITS worked as a bridge between the IT department and faculty/staff/admins, other ITS staff members worked purely for the IT department. There

was a triangulation of strategic, managerial and operational levels in the organization. This technique is important to establish credibility and enhance the validity of the results, since the results will not be skewed in one experience or other (Creswell, 2007).

CHAPTER FOUR

Analysis, Results and Discussion

This section describes the adverse effects of IT shortcoming regarding IS policy compliance. This first section of the analysis summarizes the definitions as well as the results of this dissertation. The following sections dive into the detailed analysis.

Definitions and Summary of Findings

In this dissertation, the IT department shortcoming is defined as increased security measures (SM) without adequate justification (AJ) in the eyes of the users (U) (hereafter, increased SM w/o AJU). The analysis section traces the probable increased security risk to the vicious cycle of increased security measures without adequate justification for the user, which leads to increased non-malicious voluntary security violations.

Inadequate justification in the eyes of the users in this dissertation is the lack of any or all of the following: 1) IT department's communication reaching out to the user informing an additional increased security measure is needed and justifying the existing ones 2) IT department's explanation in lay lexicon and understandable jargon why the increased security measure is needed and crucial, 3) user – IT department dialogue on the implications of the increased security measure and whether it can be prevented and 4) the IT department's administration of a survey, questionnaire or focus groups to make to make sure the majority of the users are seeing the same threat, therefore seeking the importance of the solutions advanced by the IT department. If one or all of these steps are

missing, or if the results of the questionnaire or focus groups are not positive, the IT department is still in the phase of increasing security without adequate justification in the eyes of the users (increased SM w/o AJU). The IT department should not assume that once it sends an email informing of an increase in a security measure, the security measure is already justified in the eyes of the user. The adequate justification is important because the IT department cannot automatically assume the user will comply once informed about the security measure. The adequate justification including the four steps need to be present in order to ensure the user will not volitionally violate the security policy whenever and wherever it is viable for him to violate it.

Increased security measures without adequate justification for the user also leads to increased mistrust between the users and the IT department. This mistrust may also feed the non-malicious volitional security violations among users. Other adverse effects of increased Security measures without adequate justification for the user are increased technology use avoidance and negative feelings, which may decrease user productivity. Lower productivity in this dissertation is defined as the general hindrance to work and productivity and creativity (directly or indirectly) caused by security requirements.

The analysis also expounds on how the user faces three options when faced by security measures without adequate justification for the user. Three scenarios are open for the users: 1) If the IT department does not or is not able to monitor, control, and enforce the policy, the majority of the users will circumvent the policy (NMSV). 2) Whenever the policy is enforced and controlled, the users will avoid the usage of the technology linked to the enforced policy. 3) Whenever the policy is enforced and controlled AND the users

for any reason cannot avoid the technology use related to the policy, the users will experience negative emotions and mistrust toward IT management.

This chapter also stresses the vicious cycle that begins with increased security measures without adequate justification for the user, leads to non-malicious volitional security violations (NMV-SVs), leads to increased security risk, and in the case when the increased risk or the NMV-SVs are discovered by the IT management, comes all the way back to increased security measures without adequate justification for the user. The discussion section gives some solutions regarding how to escape the vicious cycle as well as how to curb all the described adverse effects of increased security policies.

Drivers of IT Shortcoming

In this dissertation, the "IT shortcoming" is a formative second order construct (see Figure 4.1). A formative second order construct is a construct in which 1) it does not make sense apart from its formative components and 2) all the components need to be present to make the construct valid and meaningful. An example of a second order formative construct is a good security policy. A good security policy is a policy that is clear, understandable by lay users, concise, and relevant. A good security policy does not exist unless these four components are there. In addition, each one of the construct components is indispensable. They are not mutually replaceable. Thus, *clear* is different from *concise*. In this dissertation, the IT shortcoming is defined by its 3 formative constructs: the IT shortcoming involves a) increased security measures by IT on the users b) without communicating ample techniques in terms of how to follow the policy and c) without building adequate justification for the increased security measures in the eyes of the users. Let us give an example along the line of these three points: Consider the

example where the IT department decides to enforce the changing of the password every six months (point #1, increased security measure). In this case, the IT department should give tips and techniques on how to manage the 40–50 usernames and passwords of an average user (whether to use (or not) third-party password managers, how to create memorable but robust passwords, how not to use all or parts of the non-work related passwords in the passwords of the work, etc.) (Point #2, adequate communication). Then the IT department should build the case to justify the twice a year change of the password and explain why it is needed, if there are enough reasons to demand it, and what those reasons are (point #3, adequate justification in the eyes of the user). If either point number two or three or both is missing, the users will use parts or complete sections of their non-work related passwords into their work related one, or even worse, they will use weak passwords easy to remember. This example shows how an increased ISsec policy can increase the security risk rather than decrease it.

Applying double authentication for VPN for the user to remotely access institutional systems or applications or files is an example of an increased security measure. A new policy can be considered to be "without appropriate justification" in the eyes of the users when there is a lack of communication or a less than ample explanation for why this additional level of security is required. For example, the IT department may say passwords are easily broken by hackers (on average in 30 seconds by brute force), the hackers are able to act as employees when they acquire the password of an employee account and consequently gain access to the most sensitive systems (social security numbers, bank account numbers, etc.). Under all this threat, it needs to be explained to employees that double authentication is an additional impermeable layer of security,

which means that hackers must do more than simply cracking a user's password to gain access to an account.

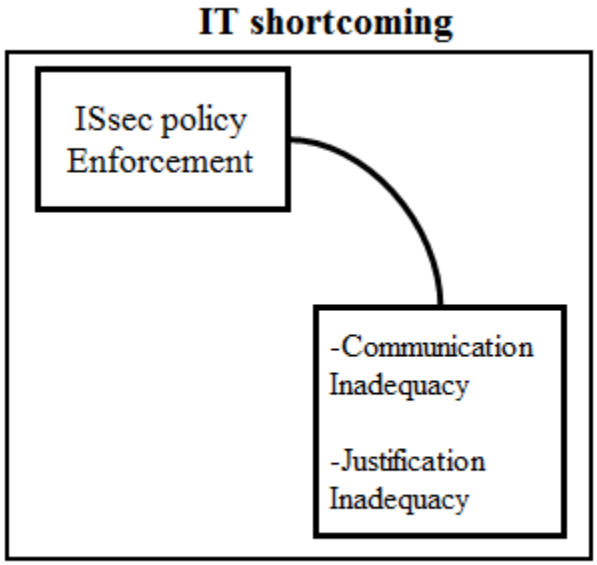

Figure 4.1. IT shortcoming: A formative construct

Numbers should back up these explanations. For example, "30% of systems are hacked into because they do not use double authentication, and this number goes down to 1% whenever the systems use double authentication." This type of detailed information can satisfy employees and amply convince them of the importance and the justification of the increased security measure.

The following paragraphs will give concrete examples and quotations from the users of the research site, showing how the users are not convinced of the added value of increased security measures. That does not mean that there is no ample value and deep need for that security measure. It only means that the value was not well communicated, explained, and justified by the IT department. This could perhaps be the result of a lack

of communication from the IT toward the users regarding the security measure and why it is needed. It could also be the result of an inadequate or generalized explanation for why the measure is needed. It also could be that the measure would still not be justified in the eyes of the user even after an alleged ample explanation. This dissertation cannot speculate on why the IT department does what it does regarding increased security measures. Nevertheless, I find that the safest route for the IT department to demand an increased security measure is by clearly explaining why the measure is needed. The IT department cannot and should not assume that the users will blindly follow the increased security measures or policies. Below are some examples of how the users in the site do not understand the value behind some security measures.

One user questioned the value of more security measures. She even doubts that the measures are there to actually improve security. She believes increased security measures serve to justify the existence of security personnel.

> So there's all these new security things, and my observation is it creates more work for the help people because now we have to call for questions with this kind of stuff, and then too it creates more work for us, and *I personally haven't seen the value yet* (Respondent 19, senior professor).

Respondent 28 wanted to know why he needed to change his password every six months or why he needed to have double-factor authentication to access his systems via VPN. He described the process of changing so many passwords so frequently as painful. He needed all of the explanations or justifications of rigorous security measures to be backed by actual data and statistics:

> I would like them to justify the pain that I go through with actual data . . . . So the real question is, could they somehow communicate to everybody the fact that yes it's a little over the top for what you do, but we do this over here which requires us to do this? (Respondent 28, assistant professor).

Even IT service staff members do not understand why some security measures are applied. The following quote is from an IT service staff member who finds solutions and applications in the market, reviews their features and security, and makes recommendations to the IT security section. The solutions are meant to meet the needs of staff, faculty, and researchers. The specific quote below came after one of the suggested systems was rejected by the IT security, although it was widely used in the marketplace. Even the informed guessed answer is not justifiable in the eyes of this IT service staff.

> All the other universities that use this system, and it's a widely used system, none of them are having any problems with it that we know of. They're allowing students to pay for it directly, and they're using a credit card system that follows all the rules laid out by banks or visa or whoever, but PHEI [IT security] is requiring something more. And we were just surprised by that, and I don't really know why. They're trying to get out ahead of it and require what's going to be standard in a few years, but why we're requiring it now I have no idea. . . . Okay, if it's the standard in the industry and everybody's okay with that, why are we not? I don't understand it (Respondent 5, project manager).

Another IT service staff member expressed his frustration about not finding a good justification for why the students' credit cards are so meticulously protected by the institution. Some of the faculty approached the IT services wanting a certain application to be used in their classrooms. This application needs the students to pay a certain fee with their credit or debit card to be able to register. The application is a brilliant one and can be used for all the students in PHEI, nevertheless only those few classes are benefitting from it for security and cost reasons. PHEI's IT department wanting to protect the cards from any compromise while using this outsourced system, PHEI is paying the fee on behalf of the students (for each student for example US$15). The cost is tolerable for few classes of 40 students each. Nevertheless, PHEI is not willing to pay the cost of that application for 10,000 students (the numbers are concealed), just because the cost will go up to US$150,000 for one application. It is an enormous expense. Therefore,

PHEI is not making a beneficial application available for security reasons, trivial and unlikely ones according to one of the IT staff. The following is the comment of the senior academic consultant bringing faculty needs to the IT department.

> PHEI is paying that bill because we don't want students to put their credit card in there because we don't think what they're doing, say in their PCI compliant, is enough. We want them to be held to a higher standard. *I don't see any real justification of that.* If what is good enough for the banking industry is good enough for the banking industry, it should be good enough for us too. *I don't know why we need to have a higher standard than that.* Plus, we're not talking major financial transactions here. We're talking a $20.00 proctoring fee on a credit card. I use my credit card at Home Depot. Home Depot had a breach. Okay. That's no big deal. You get the credit monitoring. You go on with life (Respondent 8, senior academic consultant).

Another quote comes from a user who needed to buy an analytics system to deploy in his department in order to use it to attract prospective students, but his request was denied. He says that he understood all the explanations of why the analytics system should not be used by one of the marketing departments, nevertheless he still does not find it justified we hear him saying:

> I took computer science a long time ago. I triple majored and one of my majors was computer science. And the company that I used to work at was a computer company. And so I'm not easily intimidated by computer speak. And so it's definitely understandable as far as how they [IT department] write it [denial of a request] but I'm not sure it's defensible. . . . It's understandable, it's not justifiable (Respondent 25, position concealed, as extra anonymity was requested by the respondent).

All of these quotes prove there is an IT shortcoming. This shortcoming is comprised of either a lack of ample communication, or a lack of justification, or both. Specifically referring to the last quote, analytics track people's website behaviors and clicking patterns. If a prospective student is interested in a specific program that PHEI does not have, PHEI can learn via that analytics tool which university websites the prospective student is visiting and on which program is clicking or lingering more than the others (reading the webpage of the program). That could mean that he or she is interested in that specific program. PHEI can therefore create such a program in the near

future to cater to such prospective students. This tracking of personal computer's clicking patterns via cookies or a software code borders on ethical issues and may or may not be solely dependent on IT department's decision. Higher administration (e.g, provosts and vice presidents) may have their say in such matters. Therefore, explaining and justifying decisions definitely include what type of decisions is coming from their spheres, and which decisions are dictated upon them from strategic management. This may decrease the friction between the IT department on one side and the end users on the other side.

IT Shortcoming Leading to User Non-Malicious Security Violations (NMV-SVs)

The author noticed an insufficient explanation is a construct in which IT services (ITS) knowingly or unknowingly does not explain in a plain way the reason behind the new (increased) security requirement. The "why" is important. If users do not understand why they are required to perform an extra level of work to implement an extra security policy, they may respond in a negative way.

This IT department shortcoming will lead to user volitional non-malicious violations for security requirements whenever they are able to circumvent the policy. This latter part—whenever they are able to circumvent—is important. In the case when they are not able to circumvent the policy, other results will show up (technology use avoidance or frustration; both are discussed below). Therefore, if a user does not have an adequate explanation of "why," one of the results will be that he or she will circumvent the security measure.

We see this positive relationship in the following interview quotes related to password policy in particular and not complying with ISsec policies in general. Regarding password policies, non-malicious volitional security violations are in the form

of 1) using the *same passwords* across personal and work accounts at the same time, 2) *using similar* passwords (or parts of the same passwords in different work accounts), 3) writing the password on *unsecure devices*, and 4) *generally not complying* by the policy.

Using same or similar passwords across personal and work-related accounts. Whenever we witness the enforcement of a security requirement, the users, if they are not satisfied with an explanation, will circumvent the requirement if they are able to. This is most evident in the interviews regarding password requirement circumvention. The users are using the same or similar passwords across work-related and personal accounts. This may lead to an increased risk rather than decreased risks, although the password policy really aimed at decreasing risk in the first place. The following are some quotes from the users regarding the use of the same or parts of the same passwords among the personal and work-related accounts of the user.

> I'd say 50% to 75% percent do reuse passwords (Respondent 29, director of a program).
> I may change little things, like adding the @ sign in replacement of an A or something as opposed to really getting creative and trying to figure out a whole new set of passwords. Like I said, I'm probably not as secure as I should be (Respondent 31, office manager).

A director of an administration went to a great length explaining how she is embarrassed in using similar passwords across her 30 plus work-related and personal accounts. This show how difficult is for any user to handle so great number of passwords and lead to willing or unwilling compromise of security measures by using similar passwords across sites. A typical example of how increased security measures do not necessarily means more security. It might be exactly the opposite as the following two quotes suggests us to believe:

> I have been in the habit of setting that as the same ID as my PHEI ID, whether that's good or bad. . . . I got to go back to my snazzy little page, here, and add the account, and the user ID and the password, right there. *And, the sad thing is, if you go through a lot of*

> *these, the passwords are very similar, you know?* So, they are similar consecutively, but also similar throughout the systems? . . . Yeah, I'm very embarrassed. User ID and name. I mean, it's embarrassing. (Respondent 17, director of a sensitive administration[1]).

The reuse of passwords pushed the IT department to implement a more rigorous strategy. The increased measure enabled the systems to remember up to the last four or five passwords used to access the systems. Thus, the increased measure forced the user to not be able to use old passwords, or in other way to use a "family of passwords" (which could mean the same passwords added 1-2-3… ect. at the end of the on password. The number is chosen based on the month of the year the password is being changed in). The following quote shows the overwhelming nature of such security enforcement.

> That's part of what creates this difficult situation where I might use a similar set of passwords or kind of a family of passwords, but now if I've used a number of those passwords already. Then you're getting into a system that's remembering four or five deep then; again, that gets to be kind of overwhelming (Respondent 20, director of a computer center).

The users are weary of remembering frequent changes of passwords and they try to circumvent that pain via creative ways. This leads me to conclude that increased security measure (in this case frequent password change) does not necessarily lead to increased security. Unfortunately, oftentimes, it means the exact opposite!

Writing down passwords on non-secured places. Another example of circumvention is storing passwords in non-secured places (sometimes on paper forms, but usually in digital form) on smartphones that are usually non-encrypted and not protected by antivirus programs. We find many quotes from users telling us so.

> Yeah, yeah. I mean it's very important. Just about every—as a department chair, I probably have about 18 different administrative systems that I have to use to do my job, which is really a lot. I actually—I keep a little—[he shows me a note card where he has all the usernames and passwords]. And I have to—it seems like whenever I get on that,

[1] By sensitive administration, I mean dealing with sensitive data (e.g., payroll, social security number, health care reports, financial data or any other sensitive information of these sorts).

> which isn't every day, I have to change my password. And so it's—to me, it's just way, way – it's overkill. And so I literally have—I have a password written down in pencil, and I'll erase it and I'll write the new one down. That's a bit intrusive. (Respondent 3, professor and chair)

An office manager was confident telling me that although she writes passwords on paper nevertheless she protects the paper in a secured locker. Right in the middle of the talk, eyes dropped on a sticky note put on the wall next to her computer. She acknowledged, to her surprise, that she does put passwords on non-secured places. In her own words, she said:

> Yeah, I probably do a bad thing. They're all, somehow, connected in one way or another, and I write them down, on paper. I don't put them on my phone [after pausing and gazing at the wall full of sticky notes] Yes. I have my one, it's a—Yeah, I do have a password [on the wall] (Respondent 26, coordinator of an academic support services).

Passwords are usually written down in digital formats on smartphones. Not all of the users we asked who put their passwords on their smartphones have encrypted smartphones. The following quote from Respondent 17 shows why he registered around 50 accounts' username and passwords on his mobile phone. The respondent shows the "note" document on his smartphone where he preserves his passwords.

> Well, I did this because—out of fear that I would not be able to log in when I went overseas, when I went anywhere, that I would not be able to log in [to any system]. So, out of fear, I did this, because I need to be able to access all kinds of systems. Five or six inside of PHEI, and then many outside of PHEI, so I write these [usernames and passwords] down out of fear. Because what if I can't go find my reservation for my cruise or something, because I can't remember my ID number [and password] ? (Respondent 17, director of budget management)

Consumer Reports (Tapellini, 2014) gives the above-mentioned chart (see Table 4.1) regarding how smartphone users secure their mobile: The majority of users do not follow security practices on their smartphones. It was noticeable how there was a significant difference between the IT staff and the non-IT staff/faculty regarding best practices of password management.

Table 4.1.

Security of Smartphones

How Smartphone Users secure their phones	Percentage of smartphone users
Set a screen lock with a 4-digit PIN	36%
Backed up data (to a computer or online)	29%
Installed software that can locate the phone	22%
Installed an antivirus app	14%
Used a PIN longer than four digits, a password, or unlock pattern	11%
Installed software that can erase the contents of the smartphone	8%
Used encryption	7%
Took none of these security measures	34%

The IT department does not practice all of these unhealthy password behavior patterns. All the IT-related or IT-services-related staff 1) never put any work related password in writing (neither on paper nor in digital form) 2) never use the same or similar or parts of passwords in between their work-related and personal accounts, and 3) manage the sheer number of their personal passwords by storing them in password management apps. The researcher wondered why the IT department is "betraying" the users by not helping them learn how to navigate a password saturated world. The password management policy specifically mentions that "the passwords can be written in a secure place" but does not elaborate on what is a secure place. Thus, in this case and for good reasons, the users are circumventing policies because they are not given ample instruction and tips by the IT department on how to remember work-related passwords, or at least how to secure their smartphones (by encryption and strong antivirus), and how to manage personal accounts on password management software. Only two of the non-IT users were aware of password management software like Dashline or Lastpass. The reason why users are writing down their passwords or using similar passwords is

understandable: They are incapacitated by the sheer amount of passwords! The IT department was absent. In a private email session about password management apps, an IT security specialist said, “PHEI ITS does not recommend and/or support any password management software; therefore (with my apologies) officially I cannot recommend any of them” (private email conversation in the October 2, 2015).

With this type of communication, awareness and justification are not provided in the ISsec policies. No user is aware that the IT specialists themselves will not use customized app for their work-related passwords, but only for their personal accounts, and that only if the app uses either encryption or double authentication or both. This piece of information was gathered during a personal conversation with the CISO of the institution.

Not abiding by ISsec policies in general. Yet another example of circumventing security requirements is using software that is not supported by the IT department for use. This following example captures well how the user wants to cling to her productivity level and wants to non-maliciously but voluntarily circumvent a security measure. There is a tendency among users that when they are faced with a threat to their productivity, they try to go underground. They try to non-maliciously but volitionally counter some security requirements. In the following paragraph, the respondent is a director of a program and is using software to facilitate her work:

> We are able to collect our own data, maintain our data, pull our data, communicate directly with our people, and do what we need to do on our small scale. (Respondent 30, director of a graduate program).

The context of the following quote is that in 2008, there was software being used by the marketing department of a school. The marketing software tool was approved in

2008. Yet, when the institution created the position of a CISO, they increased the security measures; that particular tool is being disapproved in the other departments. The department that first used it, wants to remain under the radar so that the IT department will not [quote] "come after" the user.

> I think they go overboard on security. That's another thing. We didn't have any problems using our software, but that was before. I've been using it since 2008. I know another department is trying to add the same software we're using, and PHEI is giving them fits. I got lucky. Security, they go above and beyond. That would be my only thing. Do we really need as much security as they're telling us we need? I don't have details of that. I try to stay under the radar with this program we use so they don't come after me, since it was implemented with PHEI's support, but implemented before some of these extra security layers have been added (Respondent 30, director of a graduate program).

This is a clever move from the user. This example could be considered a clear case of a non-malicious volitional security violation. Another example of the general non-malicious circumvention is the general non-compliance with one of the ITS policies. The program director said he just does not comply with the IT policy in the matter of FERPA code. FERPA code, which is enforced by the IT department, says that writing down student grades in email communications are prohibited and jeopardizes good standing of the university in front of the government:

> It's almost impossible not to include grades, but they really don't want us to do that because it's so easy to break in to our stuff. . . . We just don't comply [with ITS policy]. We really have to [write the grades in our email correspondence with the students] because it may be right before they go to class and take a final. You never know what the situation is (Respondent 29, director of aprogram).

Recently, some studies started identifying this connection between security measures justification and intention to comply. The lesser the freedom restrictions of new ISsec policies (behavioral freedom, e.g., unrestricted access to the Internet in a work environment), the lesser end user computer abuse (Lowry et al., 2015), and the threat to freedom will decrease the intention to comply with ISsec policies (Lowry and Moody, 2015). Thus, this dissertation proposes the following:

PROPOSITION 1: Security measures without sufficient justification in the eyes of the users increases non-malicious volitional security violations.

User Non-Malicious Voluntary Security Violations (NMV-SVs) Leading to Increased Security Risk

The abovementioned examples show that increased non-malicious violations increase security risks. Ironically, when the ITS wanted to increase security, it did encounter decreased security and increased risks.

In 2013 alone, the number of smartphones lost or stolen was 1.4 million and 3.1 million, respectively (Tapellinni, 2014). We saw that 93% of smartphone users do not encrypt their data. The same is the case for laptops, of which more than two-thirds are not encrypted (Schwartz, 2011). When an unencrypted smartphone or laptop is stolen, even if it has a password, the hard drive can easily be accessed and all the files on it disclosed. If the majority of users in PHEI are writing their passwords on a file on their smartphones (or on a Word document on their laptops), there is a high risk of a hacker who recovers the hard drive of a stolen or lost device to access all the passwords written on the mobile device.

The usage of similar passwords across work-related and personal accounts puts the system at high risk. If one of the personal accounts (like Hotmail or Gmail) is hacked and the hacker knows the password, the same password can be used by the hacker to increase his chances to crack the work-related password. That is why the majority of IT staff interviewed in this dissertation abstained from reusing passwords or parts of passwords from their personal accounts. Nevertheless, this ill practice is widely adopted by the users.

The user NMV-SV leads to an increased risk. We see this positive relationship in the following interview quote related to passwords:

> Yeah that is, to me, kind of the ironic thing, is that in an effort to make systems more secure, in some respects we could be making them less secure due to the vulnerability of either writing the passwords down or leaving passwords somewhere where they're discoverable, whether it be on a sticky note on a monitor or on a smartphone or some other place that someone else could learn what that password is. So I do think that there's got to be, hopefully there's a better way to where we're not trying to—we don't have this overwhelming number of passwords so that we create actually a less secure situation (Respondent 20, director of a computer center).

The above mentioned quote from a computer center director confirmed the researcher's fear that NMV-SV increases security risks. In the words of this computer expert, IT departments, in their endeavor of making systems more secure, "ironically" create a "less secure situation". Thus, this dissertation proposes:

PROPOSITION 2: Non-malicious volitional security violations are positively related to an increased security risk.

Increased Risk Relationship Toward Enforced ISsec Requirement

Once the IT department discovers the increased risk, or the non-malicious volitional violations of the users, the IT department will increase security measures. At the research site several years ago, when the IT department discovered that users rotate the same two passwords, all over again, thus increasing security risk, they added a patch that reads four passwords deep. This new procedure that has been in effect for several years, forces the users not to use up to four old passwords used in the email system.

The literature review of ISsec policies in the beginning of this dissertation gives ample evidence that this proposition is true. We reiterate that proposition to complete the

picture of the vicious cycle discussed in the next proposition. Thus, based on the literature review section, this dissertation reiterates the proposition in the following way:

PROPOSITION 3: Increased violations of security measures, once discovered by an IT department, will increase security measures by the same IT department.

The Vicious Cycle of Security Measures

We find in Figure 4.2 the vicious cycle of how increased security measures sometimes decrease security in organizations. The key problem as to why increased security measures may lead to increased risk is in the highly probable and widespread approach of IT departments in dealing with users in their organizations. IT departments sometime either lack the knowledge that they need to justify why a security measure should be implemented, or in the case of awareness, they lack the means to reach their thousands of users in an effective way to explain to lay people the "why" and the "how" of the security measure.

The analysis until this section has shed light on how security measures, if not adequately justified, may lead to NMV-SV by users. These security violations may increase the security risks, as we saw was the clear case with password management. The IT department, once alerted to the increased risk, will impose further security enforcements. The full cycle is complete and is repeated unless there is a clear explanation for 1) why the security measure is important, 2) why the violation of that security will lead to breaches, and 3) how to better comply with the policy (e.g. tips of password management). Once the IT department accomplishes this part and once the user

understands the "why," they may be more willing to adopt more difficult but healthier password management habits than the ones encountered in this research.

In the case of password management, the IT department needs to explain first why the same or similar passwords should never be used across work-related and personal accounts. Second, it should explain that work-related passwords should be robust and never be written down on any digital or paper form (including some tips on how to create memorable but strong passwords), and finally, it should explain how personal accounts' passwords can be managed with the help of digital apps. Unless the IT department does its role (or the users reach out to the IT department for an explanation and tips on the how and why of the security measures), the vicious cycle will remain effective. Thus, this dissertation proposes the following:

PROPOSITION [1-3] ^{prime}: Increased security measures increases security risks if unaccompanied by justified security in the eyes of the users.

IT Security Shortcoming Hinders Productivity

Security measures usually have some level of hindrance regarding productivity. This level of hindrance is sometimes insignificant, such as in the case of changing the password twice a year. Each time, the entire process of password change may take up to 5 min, an insignificant amount of time. Other times, there is a significant level of hindrance, for example, in the case of putting a new IT artefact (e.g. a software solution) in place with reviewing it for security purposes before integrating it with the existing servers in an organization.

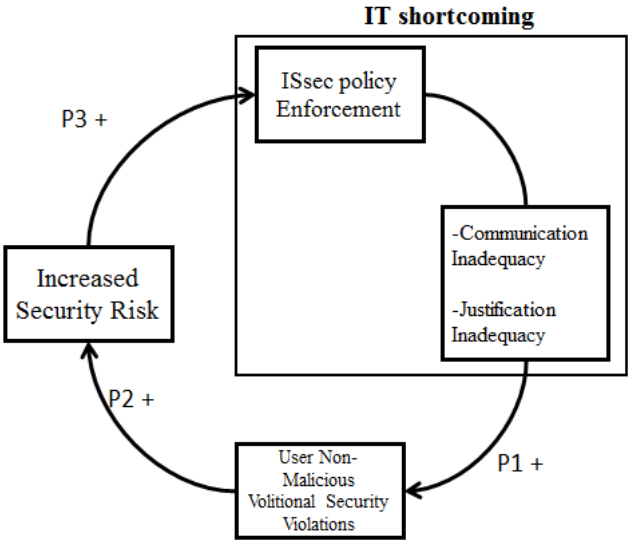

Figure 4.2. The vicious cycle of security measures

Although an IT artifact is there to increase productivity, the security reviews on them almost always hinder productivity simply by absorbing a significant amount of time before employing the system. According to IT service staff members who help faculty and staff in an institution to find solutions (software applications), they spend months and months of review before they send their report to the security team in the IT department. This time negatively affects the productivity by simply postponing the employment of a solution for months. If the security team needs other upgrades on the capabilities related to the software solution or the IT artifact (e.g. deleting capabilities for videos immediately rather than after 90 days), this may add another time delay for the software provider to upgrade the solution to meet the security needs of the purchaser (PHEI in this dissertation). Security is there not to increase productivity, but to secure the increased productivity that will come with the implementation of the new technology or software. Thus, security measures usually take time and effort, and at some level or at least for a while, they hinder or postpone productive work.

Security measures do not just usually absorb time and postpone productivity by postponing the deployment of a technology, but they create hindrances to the users in terms of inconvenience. Simply changing passwords or getting online training about how to use double authentication may take some time from the users and may be inconvenient during work time. We will call this the "necessary" level of inconvenience and time consumption. The CISO of the institution did not deny this "necessary level" of inconvenience:

> People are like, *"That's inconvenient." I'm not saying it's not inconvenient. I'd never make that claim.* But what I'm saying is that the risk is so high that we have to take *some additional action*. Most of our, what I would say, changes that we do, absolutely come into place because there's evidence to back up why we're doing this (Respondent 21, CISO).

This section does not deal with the "necessary" level of inconvenience but rather an "UNnecessary" level of hindrance to productivity. This dissertation links the unnecessary level of hindrance to productivity to the result of the IT shortcoming and failure to invite the input of the users regarding the increased security measure and and/or adequately justify it in their eyes.

In PHEI, some departments 1) lost the ability to acquire or use a system (thus they lost productivity) because of unnecessary security tightness; others 2) lost their decision-making ability because of unnecessary tightness in access control or in the use of decision-making tools; yet a third group 3) lost countless time (thus productivity) because of many extra steps pushed on them to report a security problem or just because the password changes were an unnecessary extra hassle; and a fourth group 4) complained about getting a B level product instead of an A level one (in terms of productivity) just because the B product had tighter "extra" (read "unnecessarily" extra) security.

The following paragraphs will unfold examples of these unnecessary losses of productivity. It is important to mention that these grievances are only perceived "unnecessary" loss of productivity in the eyes of the users rather than actual unnecessary losses of productivity. It could be as well a "necessary" loss of productivity. It could be that a faculty member wanted to use a solution that would have greatly enhanced the learning skills of his students, but the security team in IT department saw a tremendous risk in the software and therefore rejected the solution. The faculty lost productivity, but it is not a loss that is unnecessary because, according to the IT perspective any productivity with a real compromise of security will backfire, usually in the short run if the solution can be exploited by hackers. This debate and decision regarding "necessary" or "unnecessary" loss of productivity and where to draw the line or who decides what is necessary or unnecessary may only be settled by constant, ongoing, systematic, and frank Q&As and inputs between the users and the IT security team regarding the necessity (justification) of the security measures.

Denial of use of a system because of "unnecessary" security tightness. More specifically, one of the marketing departments wanted to target potential students, but it was denied for security and privacy reasons the use of the free Google Analytics software The director of the department explained in his words:

> So we've been trying to make a case for why we need to have analytics. Everybody has them and I understand Google Analytics is easy to use and free, even though it's not really free because they're probably using all of your data. They're probably collecting that and using it somehow. But there needs to be some way that we can get web analytics because how can we do anything—you know, this is what we teach in the [anonymous] school. You try to make data-driven decisions. Anyway, we get—I get real frustrated with all of that. It's very difficult to try to do our job and keep up with everybody else and have all these obstacles put up. And it's either because of—they say it's either because of security or because of privacy (Respondent 25, position concealed, as extra anonymity was requested by the respondent).

In order to provide an explanation for this case, the researcher contacted the CISO. He said there is a more secure but costly solution for analytics, a paid version of free Google Analytics that does not collect consumer data such that it is sold to or used by a third party. Nevertheless, this version was out of reach at the time because of the high cost of the solution and the tightness of the IT department budget. This answer was not a good justified argument in the eyes of the user, who is the head of a department. It seemed to him that IT security was having the cake and eating it too; it was not providing a solution, and it was unnecessarily putting the department (and the school) at a competitive disadvantage in the marketplace. Respondent 25 continued in expressing the grievance:

> I think probably more of how we bump up against IT security in my department is that we're trying to market—do marketing. And we run into roadblocks with what we can and cannot do. And we're told by IT that we can't do it because of security reasons. Like, for instance, when we're doing marketing online and we're not allowed to retarget people—all the things our competitors do every day. We're not allowed to target people. We're not allowed to track where they're coming in from or—and this is not even as much maybe security-related as what they see as a privacy issue. But, I mean, there's just *lots of obstacles put in our way when we're just trying to do what everybody else is doing, our competitors* . . . I came from a different—I worked at a company—a multinational company for 15 years before I came here. And when we would go to our IT department and say, "We want to do this campaign where we have personalized websites and we want to track their data and qualify them—send their leads to the salesmen," they'd say, "Great, we're going to help you do that" because everybody was interested in making it easier for our sales people to make some money and make profit for the company. *But here it's like it's an adversarial dance*. Every single time you try to get anything done you bump up against that every time. *I don't feel like they make our jobs easier at all. And I feel like they go to a lot of trouble to not make it easy. Like they would rather spend an hour saying all the reasons they can't do something instead of a half hour figuring out how they might be able to do it* (Respondent 25, position concealed, extra anonymity asked by respondent).

This incident shows how a security concern from the IT department may impede not just the productivity of a business unit, but also may intervene and hinder the unit's core business functions. A denial of a the use of a system without adequate alternative solution is only one way in impeding productivity. Another way security can hinder

productivity is through the limitations it can put on the decision making of the departments. This is the subject of the next subsection.

Loss of decision making ability because of unnecessary security tightness. The use of innovative software like Google Analytics is hindered by IT department according to some users. Nevertheless, another type less related to specific software, and more related to the core of business decision making of departments is also affected by security and privacy. The following quote shows how the business process and decision making is hindered by some security measures.

> Another example is, what—well, sending email. So if we send mass email we have to go through the PHEI CMS system, the one that they built themselves. It's their content management system for the web, but we have to use that to do our mass emails. We would like to not do that because we can't track anything other than how many people clicked on the links. And we don't know who those people were or anything about them or—all we know is how many people—how many links got clicked on or, excuse me, how many clicks there were on a link. And so we're not allowed to use any outside email vendor to do that service for us…It's hard to take data and make decisions here; it really is because the data's just not available. (ibid) (Respondent 25, position concealed, as extra anonymity was requested by the respondent)

Hindered decision making surfaced in other forms too albeit for the same reasons: security and privacy. A chair of a department who is not able to access the grades of all the students who come take his advice in academic matters complained about this restriction.

> And so it's someone who's, in their mind, they're doing exactly—I don't want to say someone sitting in an ivory tower, but they're making decisions—someone is making decisions about, well, a department chair should only have information on so someone was making those arbitrary decisions without really understanding my role (Respondent 3, chairman of a department).

The decision making process of a chair is directly related to the sphere of the access he has in order to efficiently be able to advise students on taking additional or specific courses or not. Currently chairs only see his department's students details and

only by permission the students of his school. Nevertheless, it is not uncommon for students from different schools wanting to take courses in the chair's school. Productivity in the form of decision making is hindered, but also productivity in other forms, including loss of time discussed in the next paragraph, are also hindered by security measures.

Loss of work-related productive time because of unnecessary security tightness. In addition to the decision making hindrance, time constraints work inconvenience and time-consuming measures emerged as some problems of increased security measures. .Password changes demand brainpower and becomes a time consuming burden according to this office manager.

> We have to—this takes brain power you just have to sit and remember it. And if you forget it, then you have to or I have to get up and go to that folder look it up and come back and re-log it in. And sometimes I've run into situations where you know the right password but it's just not working so you have to go through the process of you know, I forgot my password and re-create that and then that takes time away from doing stuff that's a major inconvenience. Oh, the only thing it really is, it just makes it tedious to have all those different log-ins. (Respondent 18, office manager).

Another respondent says that the ticketing and tracking system of IT helpdesk requests are just another form of dumping work on the user. It is not honest to demand extra steps from the customer and call it customer help or orientation. It is basically, according to the respondent, an outright diminishing pressure from the IT department and dumping work on the user. The quote says:

> If you're trying to serve people and make them more productive, why give them extra steps, when meanwhile you've got this person paid to sit there and log information. Well fine, let the IT person give them the information along, that's fine with me. But why make me do it? So I know, that's kind of an industry thing too where more and more has been pushed on the consumer. It's like, you have to do all sorts of things before you can talk to somebody or you have to, so it's this, they call it—they pretend like it's a customer orientation, but it's really just dumping the work on you. And again, if it's something you don't use a lot, you don't remember that secondary password and you're also tied now to two devices [for the VPN double authentication]. And so there's all these new security things, and my observation is it creates more work for the help people because now we have to call for questions with this kind of stuff, and then too it creates

> more work for us, and I personally haven't seen the value yet (Respondent 19, faculty member and director of a program).

This is another form of work impediment and hinders productivity. In the words of the respondent's words the IT department instead of making the job less tedious on the user, is making it more tedious along with creating the job positions of the helpdesk staff members and ensuring they have enough tickets or job pressure to justify their existence. Hindrance of productivity is emerging in different forms. Password management re-occurs in the following quote along with the word hassle, which occurs four times in one small paragraph. Interestingly, the user is accusing PHEI in creating this mess of password management.

> It's more that than it is a loss of time. It's more like, I gotta stop, I've gotta track this email, I've gotta track this password to everywhere I go, fix what it goes, whatever. It's a hassle. Definitely a hassle. Passwords are a friggin' hassle, and PHEI is a part of that problem. Now, if you look here in these passwords, most of them are gonna be not PHEI passwords, they're gonna be—these passwords, an electric bill, AT&T, my phone bill. Blue Cross/Blue Shield, my medical bills. . . . Those are all PHEI things, all different passwords. It's a friggin' hassle. It's a hassle, and I could be left out to dry if I haven't kept track of the password here, correctly, or if I don't know it there, and I've gotta ask for it— (Respondent 17, director of a department).

Still others complained about losing time in every step of password change. He said it takes five to ten minutes in every password change and that is loss of productive time. Notice the desperate tone at the end of the quote hoping for some type of a solution.

> I just keep making it up until I get one that works. There are a couple of systems where I think I change my password every time I log in. That's five or ten minutes if you have to change a password. Besides the fact that you did it about six times with other passwords before you realize that you don't know what it is. So yeah. That's hard. I don't know how you guys are going to come up with a new password authentication system. That would be nice (Respondent 13, director of a service).

Other respondents noted the time consumption when their laptop was broken. This time consumption is not in an obvious area of productivity. Several years ago, PHEI demanded all the laptops to be encrypted. Nevertheless, whenever a laptop is broken and

needs some fix, it needs to be decrypted first. This adds another day or two on the fixing time, delaying giving back the laptop to the user. The director of the laptop services explains:

> I think the one thing the faculty really did not like was that we required, five years ago, I think we started requiring all laptops to have encryption. And, that seemed to create some issues, because even reimaging a system was no longer easy to do, because you had to spend hours decrypting, before you could work on the computer. (Respondent 16, senior leader of IT services).

Up until this part of the analysis, the reader noticed that increased security measures hinders productivity, by 1) loss of the use of productive systems, 2) loss of decision making and 3) loss of productive time. One final example of productivity loss is discussed next.

Loss of capabilities of an A product (or A service) because of unnecessary security tightness. An A level product (in this case a software application or a solution) is a product that is distinctive and has competitive advantage over a B level product. Based on a conversation with an IT client service staff member who finds solutions for the faculty academic or administration business needs explains how increased security measures sometimes hinder the choosing of an A product and leads to a less efficient B product. This B product, albeit has more security features may lower the quality of service.

> It is one of those that the better product didn't have the ability to take those videos offline right away. We ended up with what I personally feel is a second-best product because the first-best couldn't meet that particular security concern in a way that we felt was adequately addressed. . . . They do, functionally, almost the same type of thing. It was just a cleaner interface, simpler to use, a more long-term reputable company, larger customer base, better support. It was kind of like comparing large corporation A to large corporation B, kind of a Coca-Cola to Pepsi kind of thing. Pepsi is good. It can do most of the same stuff, but it's not Coca-Cola kind of a deal. We would have liked the Coca-Cola of this particular product. It seemed like it was a better fit for our institution, but Coca-Cola didn't have the ability to do this one thing we want it to do as far as going in,

> and deleting videos immediately without a 90-day waiting period (Respondent 8, senior academic consultant in the IT services).

In the above-mentioned quote, the faculty and the students using the B product lost a cleaner interface, ease of use and a better customer support. The A product had all these features but it was not purchased nor deployed because of extra measure of security reasons.

The IT department did not make available one the software solutions introduced and explained earlier in this analysis. Instead of making students pay his or her share of the cost of the proctoring software, PHEI wanted to protect the students' credit cards, and lifted the heavy financial burden of covering all the cost of the registrations. Nevertheless, the majority of the students were denied that access. A project manager complained about this beneficial software not being made available to all of the students because of unjustified security reasons:

> I mean it was small charges, but basically if they used this system, they could use their credit card and $5.00, $10.00, whatever, to access this system. Now PHEI is just like, 'Okay, it's going to be free to the students,' which it's a good deal for the students, granted, but they're having to limit who can use it. There's only certain students who are going to be able to use it because PHEI is having to pay for everything, and that's basically business decisions that are all being driven by the fact that our credit card data requirements were too stringent. . . . The drawback, I think, at least in my mind, was that *they only gave that access to a few classes*, Okay, you three *professors that requested this, your classes can have access to this, but nobody else can because it would cost PHEI too much money*. So those students got it for free, but it couldn't be used by any other professors, at least not yet (Respondent 5, project manager)

One of the IT client service staff members, himself an academic consultant representing IT department, summarized well his and his colleagues message to the IT department regarding a the subject of solutions and software applications that are being denied for "unnecessary" security reasons. The consultant said in the following quote:

> In general, what I would tell IT is to just be aware that the very nature of teaching and learning with technology and higher education is a dynamic thing. And that sometimes, erring on the side of innovation is more important than security sometimes and to just

> keep that in mind. To not always say no. To not let no be your first answer. To really listen to what's going on and try to provide a service, which is what we really try to do. Even when we have to say no, we try to come up with compromises and other solutions to help them out. Again, ITS I feel like is in the position where they can just say no, and that's the end of the conversation, and we get to clean up everything (Respondent 10, senior academic consultant in the IT services).

In summary, IT security department may knowingly or unknowingly, and in the eyes of users (and some IT client service staff members) may unnecessarily and unjustifiably hinder business productivity in areas like 1) loss of the use of productive systems, 2) loss of decision making, 3) loss of productive time and 4) loss of the capabilities of an A product or a service. Overall, this loss of productivity was expressed in carefully selected cautious words by one of the computer center directors, who said the following:

> My sense, in this particular area, is that PHEI ITS security has set the bar quite high, and I don't necessarily fault them for that, but I do think that it's a case where because of their decision to set that bar high, it has restricted the, you could argue it *restricts certain business functions or business opportunities for the business school*. I guess I want to be careful that I'm not saying it's necessarily, it's not unnecessary, but because the expectation, *the threshold has been set so high for security that it is restrictive to business process for us as a school* (Respondent 20, a computer center director).

The witness of an IT expert, in this case a director of a computer center, is a strong one to the soundness of the conclusion this section reached. Based on this sections' analysis of productivity this dissertation proposes:

PROPOSITION 4: Security measures without adequate justification in the eyes of the user decreases user productivity.

Figure 4.3 describes the downsides of ISsec policies in the case of IT insufficient communication and justification of increased security measures. These are: 1) increased non-malicious volitional security violations, 2) increased technology use avoidance, 3) increased frustration, 4) lowered productivity and 5) increased mistrust of users toward

the IT department. Heretofore the chapter covered increased NMV-SVs and lower productivity, the rest of the downsides follow in the next sections.

Security Measures without Adequate Justification for the User Leading to Technology Use Avoidance

When the user does not see a justification for the increase in a security measure and when user input is not invited in the dialogue, whenever possible, the user will avoid the technology use involved in or related to the increased security measure. The choice of this option is only valid when the technology use avoidance does not significantly harm the overall output or routine of work (although it may harm the extra productivity level that may only come with and through the usage of the technology; more on this in the next section). The best example in this dissertation regarding this observation is the usage of the VPN after the IT department enforced double authentication. Following is the background of VPN usage in the current site of study.

VPN is the secure and private connection that employees of the organization can use to get to their files and systems while they are off campus. Up until one year ago, the VPN was secured by a username and a password. Since the passwords are easily broken, the IT security team decided to implement double authentication (users get an extra code on a special app to be downloaded on their smartphones) to doubly authenticate access on the VPN. This extra layer of security makes it hard on hackers to access the same systems of the institution even if they can crack the password of one of the employees. Although this makes the systems more secure, those users whose jobs are not critically related to the use of VPN tend to opt out of using VPN. That means only those staff members and employees who are systematically absent from their offices' desktops continued the use

of the VPN. By absence from their offices I mean, they do not have on campus access to their files because of frequent travel abroad, or just live far from the campus.

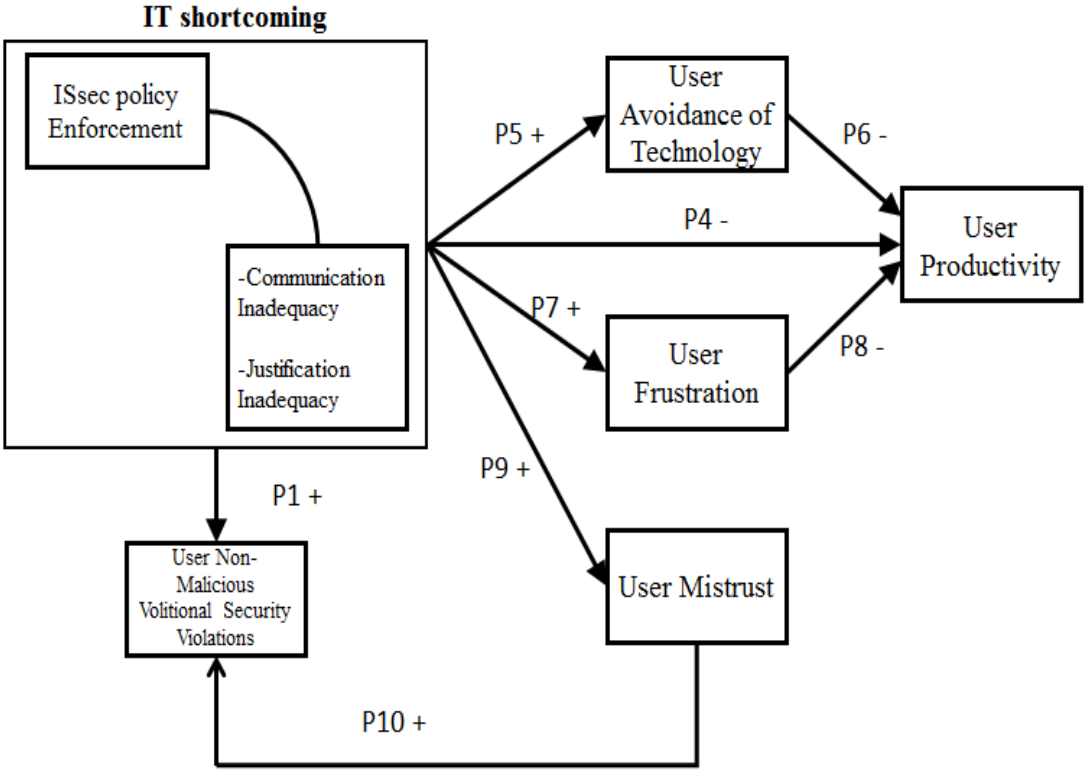

Figure 4.3. The downsides of IT shortcoming

Those who opted out from the VPN usage were most commonly among those who were frequenting their offices on campus every day of the week. Thus, those who opted out of the technology use were those who could afford opting out (i.e., canceling work from home via VPN and opting in to go to work from the office on campus). The most common reason cited was the cumbersomeness of the extra layer of security. This observation was obvious in the following quotation by an interviewee:

> I don't think I've used it since then. I always had a hard time at home getting it set up in the VPN, but I always had instructions from the computer center, or technology center now is what they call it. But not always was I able to get it to go into that VPN. But I haven't used it since there's a double authentication. Yeah. Because I don't have to—I

> don't want to use it any more than what I have to. I'd use it more if it was easier for me (Respondent 26, coordinator of academic support services).

Usually extra layers of security come with a price on the user. That price could be in the form of a learning curve to do how to use the system, spend an hour or two reading extra manuals and deploying an additional software (like in the case of double authentication), or contact the IT helpdesk in the case of support, troubleshooting or just understanding the use of the new system. This extra price led another user describe her case to me and give me the reason why she opted out of the VPN use:

> It seemed like every time I went back into it [VPN], it changed. It looked different. It changed the way it did it. It was asking me to put in a different password. I was always having to go online and read the rules to use it again. I just stopped, and just said it would be more productive for me to do it at work where I don't spend all the time getting that set up to use it than trying to use it at home. I quit using it. . . . I used to be the one who could explain to everybody how to do it at home. Now I don't even know how. I don't think anyone in our office uses that to answer questions at home . . . It just got that much more complicated to do (Respondent 29, Director of a program).

Technology Use Avoidance (Institutionally Owned Technologies) Because of Encryption

Another example of technology use avoidance is an employee not wanting to use an institutionally owned laptop because of encryption. PHEI started enforcing encryption on any laptop given freely to its employees (faculty or staff) to protect the data on the mobile device in case of its lost or theft. Nevertheless, encryption service does not come without a cost. Encryption adds at least two additional burdens on the user. In case the laptop had technical problems and was sent to the repair services on campus, the encryption repair significantly adds to the repair time because decrypting a device with mirroring technology takes time (this information was given by the director of the repair services). The user is left without the mobile device for two or three more days. The other additional burden is remembering a passphrase unique to the encryption. Only the owner

of the device knows the passphrase. The majority of users have up to 50 work-related user and personal accounts and passwords. Adding another passphrase is critical because the user will not be able to get any repair service in the case of forgetting the encryption passphrase (if all the data is wiped out, it is another burden since it adds an additional day or two to reinstall all the applications and software accumulated over the years). One of the IT staff members expressed why he avoids using the laptops provided by PHEI. The reason he gave is related to the encryption of the laptops, which may create additional hassle for the user. He is satisfied with using his own personal laptop.

> Like one of the things that ITS wants is if you have a laptop, your hard drive has to be encrypted. That's the rule, which is one of the reasons why I don't have a laptop (Respondent 4, senior IT analyst).

The laptop that this IT analyst avoided is an institutionally owned work related laptop. Albeit th laptop is a more secure one and recommended by the IT department, nevertheless the user chose the available option of not using an institutionally owned laptop. The reason he gave was related to security (i.e. encryption in this case) and the hurdle the security measure creates. Another leader in a senior position in the IT department confirms this same phenomenon and gives the reason why:

> I think the one thing the faculty really did not like was that we required, five years ago, I think we started requiring all laptops to have encryption. And, that seemed to create some issues, because even reimaging a system was no longer easy to do, because you had to spend hours decrypting, before you could work on the computer. So, it slowed us down, basically. It slowed the turnaround time to fix problems, and that kinda thing. The PGP password is different from any other password you have. So, that meant that the user had to remember yet another password. The PGP password is much more sensitive, it has a lot more requirements than any other system that we have. . . . Yeah. So, their way of circumventing that policy is not to use a laptop at all That was really their only way around it (Respondent 16, senior leader in IT services).

Some users either opted out from using a laptop and were satisfied using their desktop, or they continued using their personal laptop. In the first case, they avoided a technology use, the ramifications of which will be discussed in the next section. In the

second case, they avoided a secure technology in favor of a less secure option (the ramifications of this were discussed under the NMV-SVs section). Thus, this dissertation proposes the following:

PROPOSITION 5: Security measures without adequate justification in the eyes of the user will increase technology use avoidance.

The Relationship between Technology Use Avoidance and Productivity

The extent literature describes how technology and innovation increase productivity (Franzten 2000; Kleis et al., 2014; Quatraro, 2009). In our cases described in the previous section, we know that VPN is there to increase productivity by facilitating working from home on a project or accessing a file at work from home. However, users either go directly to their office if they live nearby, or they postpone work for the next day or for a couple or several days or so over the weekend or over a holiday. In the first case, the user is losing time by commuting, and in the second case, the user is losing time by postponing the work. In both cases, the user is losing time in working on files from home. The same case applies for not opting for a laptop owned by the institution. The laptop or a mobile device is there to increase productivity.

As discussed earlier, technology use avoidance of any sort may not necessarily diminish the productivity level of a user to a significant degree. The employee may be able to finish the task at hand the next day or after the weekend. The tasks may not be so urgent that the employee needs to work from home using a VPN or from the airport using a laptop. Alternatively, the employee may stay in the office an additional hour or two to finish a task. Nevertheless, technology provides an added value for additional

productivity, and holding everything else constant, employees equipped with technology will be more productive while out of the office (e.g., with a laptop and a VPN) than an employee not equipped with these advanced mobile technologies. Thus, this dissertation proposes:

PROPOSITION 6: Technology use avoidance will decrease user productivity.

Security Measures Without Adequate Justification for the User Leading to Frustration

This dissertation shows that there is a relationship between unexplained or in the eyes of the users unjustified security measures and lingering negative feelings of the users. These frustrations are due to several sources in PHEI:

Frustration regarding security additions on a system. Any incremental implementation of security measures will have its own share of negative feelings and frustration among the users, sometimes because there is a new constraint on the user in terms of learning tasks (e.g., learning how to use double authentication for VPN). The following is the response of a user after trying to use a VPN when its access process was changed for security reasons (double authentication). Her frustration is expressed in terms of the element of surprise in a dire situation to use the system and in terms of the lack of clear and timely communication from the IT department regarding the upgrades of the system:

> If any system is going to change security wise, it would be nice if we knew that was going to happen. . . . It'd be nice if we had some prior notification… "next time you go into that, you may need some more time because the look of it has changed, and the ability to do it [has changed]. You've got to get double certification". That would have been nice to know. It's *very frustrating* because I needed to do it fast. It has to be done on a certain day, so I needed to do it fast that day (Respondent 29, director of a program).

The background of this latter quote is that the user accesses from home his regular work related software applications. For that reason, he uses VPN on a regular basis. In the timeframe during which the VPN was being upgraded from one authentication (password) to double authentication (password and a code sent to the mobile), the instructions of accessing VPN changed. This change included downloading specific additional software. The IT department did not communicate these changes in a timely manner, and this user wanting to access his system on a weekend, in an urgent case, could not do it successfully thus was frustrated from the upgraded system. The frustration came from security additions on a system. This frustration can also come from the password management case.

Frustration regarding password management. The feelings of frustration are also expressed in the practice of password management. A pool of respondents were vocal that the password security measures are too tight and that they were having problems in remembering their frequently changed passwords. They have hard time to keep track of all the frequent changes in the password lists. What follows is a sample of the users' expression of frustration regarding password policies in the institution:

> When you get the email to say that you have to reset your password, I always put that off. I grumble because I can't remember every password that I've used, so it takes—it's one of those cost of being here and doing business. We know we have to do it. *It's not fun* (Respondent 29, director of a program).

According to the respondents, the password management is not fun, but also is a painful process. The following respondent, out of his frustration said, "it is a pain in the ass". He uses many work-related systems because of his position. For him password change is an endless journey.

> It doesn't automatically accept the PHEI ID. A lot of systems do, some don't. So, I have to do this syncing. Which is a *pain in the ass*. . . . It's more like, I gotta stop, I've gotta track this email, I've gotta track this password to everywhere I go, fix what it goes, whatever. It's a hassle. Definitely a hassle. Passwords are a friggin' hassle, and PHEI is a part of that problem. . . . Those are all PHEI things, all different passwords. It's a friggin' hassle. It's a hassle, and I could be left out to dry if I haven't kept track of the password here, correctly, or if I don't know it there, and I've gotta ask for it. Yeah, it's a hassle. Little bit more than just a time problem. Because how could 15 minutes a day or ten minutes a day be a problem? It's not. But, the hassle, yeah. Yeah. And, PHEI is a big cause of that. . . . It's an endless journey to change a password (Respondent 17, director of a department).

Frustration comes out of security additions in a system (and the following learning curve that may be required), out of continuous password management but also out of IT objection of using some productive systems and the overall bureaucratic system imposed by the IT security department. The former two reasons were discussed above; the latter two are described in the following paragraphs.

Frustration related to the IT objection of using a specific system. Marketing departments had special clashes with the IT security team. The departments wanted to use some analytics software, but the security team vehemently opposed the installation and use of the marketing systems for security and/or privacy reasons. Respondent 25 has a major in computer science, and he understands the technical background of the IT answers given to him, but hhe is still not convinced that the IT denial of using the analytics system is justified. Realize the tone of frustration in the following quote:

> *Here [in PHEI] it's like it's an adversarial dance*. Every single time you try to get anything done that you bump up against that every time. *I don't feel like they make our jobs easier at all*. And I feel like they go to a lot of trouble to not make it easy. Like they would rather spend an hour saying all the reasons they can't do something instead of a half hour figuring out how they might be able to do it. (Respondent 25, position concealed, as extra anonymity was requested by the respondent).

Even an IT services staff member who is technically savvy did not justify the fact that the IT security team was "treating everything with the same microscope." He said the

security team is holding academic solutions/software to the same level of financial software. He said that the faculty members were frustrated when they learned one of the software capabilities was denied because of an unwarranted high standard security scrutiny that was used. The context is the following. The exact software capabilities are changed in order to keep anonymity. Certain faculty members use a software application e.g. that contains all the grades of students in particular class. There is another application that administers online assignments to the students and automatically grades the assignments. The faculty liked the idea of these two applications to communicate with each other (e.g. the assignments grades migrating from the second application to the first). For that capability, the IT department needed to integrate the two systems. Since the first system is on the main server that contain the grades, the IT department refused giving the assignment application access to the first application. The integration was denied. The faculty needed to manually type the grades back on the first application. This process was tedious and unnecessary specifically because the owner of the second application is a well-known established publisher, a long time provider supplier of PHEI. The following quote explains the frustration of the faculty members:

> Frustrated. They were frustrated. I guess that's the easiest way to describe it. They wished they could do it. They still can use those tools on their own. They just can't have that link between the learning management system and those tools. I think they were annoyed and frustrated with that (Respondent 8, director of an office).

Overall bureaucratic control of the IT security team. One of the faculty members expressed her frustration about the control system of the IT department. The policy of submitting a helpdesk inquiry is through submitting an online ticket (or making a phone call to the IT helpdesk extension). Even when you know who is responsible for laptop repair, the policy says you need to go through the helpdesk. This adds more time for the

users, who must explain all the issues with the device in writing or on the phone. The faculty member felt this was counterproductive, and she said that if she knew the staff member in the hardware repair department, she should go directly to him. Read her frustration toward the bureaucratic control in her own words:

> So it seems to me that either they just have a huge backlog of stuff, or all the stuff that they're doing for control and for their security is taking an enormous amount of time and productivity. But I guess for them it's their job, but for me it's like, "Why does it take so long?" So yeah, I get frustrated . . . why do we have these layers? Why can't I go directly to the person I know can solve the problem? . . . And it's all so they can tick box, that they solved this problem. So if your problem doesn't have a number associated with it, it doesn't get solved. . . . Why would I go through 4357 [the extension number of IT helpdesk] when I know she's the Outlook person? I mean, I know this. So I don't understand that, and I think for them it's about logging it. I'm like, well, they're welcome to log it. I've got the email. She can forward the email to whoever, they can log it and give it a number . . . let the IT person give them the information along, that's fine with me. But why make me do it? They pretend like it's a customer orientation, but it's really just dumping the work on you (Respondent 19, director of a program).

In summary, frustration and overall general negative feelings are the results of increased security measures without clear justified reasoning behind them. This can be seen in a variety of security measures or policies, from specific password management, to a VPN upgrade, to denial of using some systems, to the overall "control philosophy" of the entire IT department regarding any support they may provide. Thus, this section proposes the following:

PROPOSITION 7: Security measures without adequate justification in the eyes of the user will lead to increased user frustration.

In summary, this section described how and why users get frustrated from increased ISsec measures. This frustration is not without negative consequences, especially on productivity level. The next proposition development advances the notion that frustration lowers productivity.

Frustration Leading to Lower Productivity

A *New York Times* article entitled "Do happier people work harder?" says that there is a correlation between the inner work life and workers' creativity, productivity, commitment, and collegiality. The authors of the article base their argument on research they conducted by collecting 12,000 diary entries from 238 professionals at seven different companies (Amabile & Kramer, 2011). Employees who feel happier are more likely to excel in their productivity level in terms of having creative ideas. It follows that non-happy days (due to any sort of frustration) may decrease the optimum level of creativity and productivity.

The previous section proposed that an increased SM w/o AJU may increase frustration among employees. Frustration, in its turn, may reduce the overall quality of the inner work life, at least on the day that the frustration happened due to some level of hassle, hindrance, or constraint. Cumulatively, if 10 incidents happened in a year for each employee in an institution of 2,000 employees, that equals 20,000 days of lower quality of inner work life. Future research may try to quantify in dollar terms how much productivity is affected by frustration; nevertheless, there is enough indication in the field of psychology that there is some correlation between the two. Thus, this dissertation proposes the following:

PROPOSITION 8: Frustration induced by security measures without adequate justification in the eyes of the user lowers user productivity.

Security Measures without Adequate Justification for the User Leading to Mistrust of Users toward the IT Department

The SM w/o AJU may lead to an array of mistrust between users and the IT department. Whenever the IT department does not explain why they are increasing security measures, why they are centralizing their services, or why they are establishing significant control over some procedures, it runs the risk of fostering distrust with users.

This mistrust toward the IT department is obvious in several of the user interviews. Two obvious issues were that of arbitrary decisions and not understanding the role of the faculty. A faculty who was not able to see the students' records and grades outside of his school because of access control from the IT department accused the IT department of not understanding the role of department chairs:

> I think someone has made an arbitrary decision, and it's someone that doesn't understand the role of a department chair. And so that's—so I think security needs to be—there needs to be more of a partnership. . . . And so someone was making those arbitrary decisions without really understanding my role. . . . And I just think a lot of these decisions are being made in a vacuum, and they're probably clueless that it really is negatively impacting faculty (Respondent 3, chairman of department).

One IT service staff member expressed some doubts about the soundness of some of the decisions made by the IT security review team regarding a solution he proposed. The following is an excerpt of his way of not justifying the IT decision:

> Some of the reasons I get. Some of the reasons I understand. Some of the reasons are completely, totally justified. . . . *At the same time, some of the reason for questioning it is sometimes a little silly*. For example, there was a concern over one product that we were looking at using that was a publisher material, but it would have the ability to write quiz grades back into the learning management system. It needed that level of access to write grades back. . . . A really obscure, unlikely type scenario . . . That obscure, unlikely scenario was primarily one of the main justifications for saying, 'No, you can't do this integration with this publisher because there's this off chance that somebody there might do something unethical like that.' That seems a little *silly and unlikely*, but that was one of those scenarios where we didn't get a chance to really do that (Respondent 8, Senior Academic Consultant).

A third respondent used the words "a little bit ridiculous" (Respondent 28, faculty) regarding one of the negative decisions of the IT security reviews on one of the programs. A fourth respondent, a faculty member expressed her opinion regarding the fashion of security software that is driving ITS to do what it does. In other words, she is referring to the security measures in the institution that are driven by software capabilities in the market.

> Is it because companies are more worried about being hacked, or is it because there's new security products on the market and the consultants are all getting them to buy? Is it because there's nothing else right now? There was ERP CRM knowledge management and social media. What is there now? If you've already done the social media stuff, what do you do now? …So high profile hacking incidences then leads to new software available to help curb hacking and then once software is available, you feel like you have to use it or maybe it becomes a feature of security software you already have, so an added feature, and just like with Word and everything else, a new feature comes out and everybody tends to, 'Oh, we've got to do it.' So some of it is definitely not that the university IT people say, 'Oh, we should do this.' I think some of it is driven by the capabilities of the software (Respondent 19, senior professor).

Others expressed doubt on the necessity of double authentication for the VPN system and the password changes every six months. "Do we really need as much security as they're telling us we need?" said respondent 29 (director of a department). Assumptions of taking pleasure in controlling the lives of other people were among the expressions of mistrust. The following quote shows different assumptions and skepticism about security measures going from 1) control to 2) majoring in minors to 3) IT showing off that they are on the top of security.

> So yeah, I get frustrated, and I think at least in my case that the approach they take to this over control, you tend to develop just the impression that they over control because of the way they handle their security and other things. And so then *they have this reputation for over control [1], and not being there to really serve you . . . they have this whole thing where it's all about control* . . . You've got to release a little bit of control, because people are going to bring their own stuff and you should let them. They should be able to buy their own laptop if they want to. It doesn't have to all be the property of the university. *You should be more concerned with focusing on the areas that are the biggest threat than focusing so much on the devices and securing the devices and stuff like that* [2]. The simple side is you've got people, it's their job and *they take pleasure in just*

> *making rules that other people have to follow [1]*. So that's the cynical side . . . So yeah, my own feeling is some security they do because they feel like they need to do it *to demonstrate that it's state of the art security [3]*, even without reflecting on who it's helping and what problem it's solving (Respondent 19, senior professor).

Only careful scrutiny and a prolonged open dialogue with sincere questions and answers between the users and the IT department can fully give the real intentions behind the IT department's security decisions. Nevertheless, mistrust among the users will flourish whenever there is increased security measures by the IT department without a clear and justified explanation from the IT department toward the user. Thus, this dissertation proposes:

PROPOSITION 9: Security measures without adequate justification in the eyes of the user will lead to increased mistrust from the users toward the IT department.

User Mistrust Leading to Non-Malicious Volitional Violations

The mistrust that the interviewees expressed may lead the users to justify their non-malicious volitional violations of security policies. Trust in the organization and perceptions of the procedural justice were key factors regarding favorable attitudes of the employees toward security monitoring (Workman, 2009). Alder et al. (2006) found that justification of Internet monitoring and trust between employee and organization play key roles in determining the organizational commitment of employee. We may induce that the trust between two entities, the organization and the employee in the aforementioned article, and the IT department and the employee in this dissertation, play a major role in determining the commitment of the employee toward the organization in the aforementioned study and the compliance of the employee toward the IT department directives in this dissertation. A trusting compliant employee will be less prone to commit

NMV-SVs, and it can be safely concluded that a suspicious employee toward IT decisions will be more prone to commit NMV-SVs.

Furthermore, if the justification of the organization for its Internet monitoring increases employee organizational commitment, this may imply that the IT department justification of every increase in its security measures may positively impact the organizational commitment of the employee. However, if the justification is not presented, there may be less commitment by the user toward the organization. Earlier, we saw how some users voiced their need for justification of security measures. "I would like them to justify the pain that I go through with actual data," said Respondent 28 (a faculty member). Therefore, the lack of justification is conducive to further mistrust, and further mistrust may lead some users to commit NMV-SVs. Thus, this dissertation proposes the following:

PROPOSITION 10: Mistrust from the users toward the IT department will lead to increased non-malicious volitional security violations.

Different Results from "ITS Perceived Unexplained Enforcement"

This dissertation finds that there are three main techniques users use to cope with perceived unjustified enforcement procedures by the IT department. Whenever there is enforcement, circumvention is available, and the work is inevitable, users choose NMV-SVs. Whenever there is enforcement, but the circumvention is not available nor the work necessary, the user may choose the technology avoidance option. If both the enforcement and the work are necessary, but the circumvention possibility is not there, they will get

frustrated. Table 4.2 is the matrix of the different user response mechanisms when facing increased security measures.

Table 4.2.

Matrix of User Coping Mechanisms Facing Increased SMs

Enforcement	Circumvention Available	Work Necessary	Outcome
Yes	Yes	Yes	NMV-SV circumvention
Yes	No	No	Technology use avoidance
Yes	No	Yes	Lingering frustration AND mistrust

Toward the "TURSAP" Theory: A Critical Analysis

Heretofore the study discussed the relationships among themes and constructs and developed propositions. This section will define TURSAP theory and will summarize its relationships. Then the theoretical contribution and validity of TURSAP is discussed in the lens of the seminal work of Whetten (1989) "What constitutes a theoretical contribution".

TURSAP stands for Theory of Unintended Reversed Security Action and Productivity (see Figure 4.4). This theory explains how and why a good intention of an IT department wanting to increase security compliance by increasing security measures may turn into an unintended trigger for non-compliance. Thus, this IT department move led to 1) a reversed security action: employee non-compliance rather than a security action (compliance) and 2) this reversed security action was unintentional: the IT department did not want to increase security risk or increased non-compliance or non-malicious voluntary security violations (NMV-SV). TURSAP also explains why

increased security measures may directly end up decreasing employee productivity or by the mediation of technology use avoidance and frustration.

Whetten (1989) in his seminal work explains what the building blocks of theory development are. He explains the "What", the "How" and the "Why" are the crucial elements of a theory. Then he expounds that the limitations of a theory are important to be mentioned to put it in a context of "Where", "When" and "Who". The following paragraphs 1) define these terms, 2) show how TURSAP are meeting the first three building blocks and 3) explain what is the right context for TURSAP.

What: The "What" of a theory defines what are the constructs, variables and factors need to be included in the theory as part of explaining the social phenomena. Then Whetten adds the constructs of a theory should be both comprehensive and parsimonious at the same time. Comprehensiveness ensures all the relevant factors are included. Parsimony ensures that all the non-important constructs are deleted from the theory because they add little additional value to it. TURSAP explains the downsides of an increased security measures in a parsimonious way (eight constructs only). It includes the security dimension (increased security risk), security compliance dimension (NMV-SVs), the IT artifact (technology use avoidance), the emotional dimensions (mistrust toward IT and frustration) and the day to day impact of security measures on employee work (productivity levels). Quantitative tests of this theory in the future will display the variance explanation of this theory, in order to shed more light on its comprehensiveness and parsimony.

How: The "How" element of a theory explains the causality among the constructs. There are the relationships, the arrows that link the constructs or the boxes

together. It is a way of explaining causality. The ten propositions advanced in TURSAP meet this criteria of theory development.

Why: The "Why" of a theory, Whetten explains, gives the logic underlying the theory. Why other researchers "should give credence to this particular representation of the phenomena?" (p.491). The answer Whetten says, lies in the logic and the reasonableness of the proposed explanation. In TURSAP, the 20% of the interviewees who gave inputs on the theory in the validation phase of the findings expressed their consent with the logic and the reasonableness of TURSAP. More specifically, It seems logical that increased security measures by the IT department without adequate justification from the same may lead to increased NMV-SVs which in turn will increase security risk. An average employee in this dissertation has somewhere between 30-50 usernames and passwords to manage (enforced partially by IT department security measures). That alone may lead employees to use the same personal passwords across the work-related ones and vice versa. This phenomenon may lead to increased security risk.

The other logical component of TURSAP is the impact of security measures on productivity. It is becoming widely known that security measures are hindering productivity. Up until now, there was a lack of a theoretical explanation on how and why this hindrance operates. TURSAP is a promising theoretical development toward this goal. Whetten continues on giving the elements that may restrict the applicability of a theory. These are the "Who", the "When" and the "Where". These three constraints limit the range of the theory.

Who: TURSAP is concerned with the employees in organizations. This theory does not relate to the individual level, but only on the organizational level. It also

involves the IT department (in the construct called "IT department shortcoming") and the interaction of the employees with the IT department (in the construct called "mistrust toward IT department"). Furthermore, this theory is not valid, when the IT department is explaining adequately and justifying the reasons for extra security measures and when the employees are agreeing about the need of the extra security measures.

When: The "When" of TURSAP is clearly articulated in the construct "IT department shortcoming". It explains that the development of the employee mistrust toward the IT department is correlated with the inadequate explanation (or the lack thereof) of the IT department why it is implementing an additional security measure that will most likely impact the employees' daily work.

Where: TURSAP is generated based on North American data. Although I believe that this theory is widely valid across cultures and countries (because of the underlying logic and reasonableness), nevertheless, this generalizability needs to be tested across cultures.

Heretofore in the section, the study went through a theoretical analysis of TURSAP using the Whetten (1989) framework elements for the building blocks of a theory. The study finds that TURSAP meets all of the criteria of Whetten (the what, the how and the why), as well as gives the limitations on (the who, the when and the where).

Post-Hoc Analysis: The Perspective of the Chief Information Security Officer

After my analysis of the perspectives and perceptions of users as well as IT client service staff members on the constraints and downsides of IS security measures, I requested a conversation with the Chief Information Security Officer at PHEI, in order to

understand his perspectives on some of the concerns mentioned above. In a fast paced forty-five minutes interview time we were able to touch and clarify only *some* of the questions and concerns raised by the users and the results of the analysis section that led to TURSAP. Future research may focus on the IT department to have a fuller, deeper and richer picture of its perspective on the above mentioned security issues. Nevertheless, this post-hoc analysis is a significant start on knowing what the perception of IT department's senior leadership is.

The CISO starts with explaining why security measures are important and how they are implemented in PHEI based on careful reading of the evidences in the security world rather than following a fashion or a trend in the security industry. He emphasizes that the faculty, staff and administrators' accounts are entry points to PHEI sensitive data and resources. Once the accounts are compromised, they can be used to exploit PHEI data. This is why increased security measures are crucial. He highlights that he is aware that the average user usually does not understand the importance of his or her account, may not appreciate the security measures and may only see them as pain and hindrance.

The CISO states that he does not follow market's whims in implementing the latest fashion and trend in security. The following quotation also describes his frustration regarding employees' attitude toward IS security policies:

> I think what you have found, or what you will find, is that anything that inconveniences a user, they knee-jerk, right? So it's, "You guys are ridiculous." Many times what I have found is when I sit down and explain why we're implementing two factor authentication on VPN to protect your information, those conversations tend to all of a sudden make people take pause, right? A researcher out there in a department does not necessarily always have that vision of what is going on. They have, "Hey, I'm dealing with my data and you're making it a pain," but they do not realize that just their account even is very powerful in what it represents, because it represents access to PHEI resources that can then be exploited… Most of our, what I would say, changes that we do, absolutely come into place because there is evidence to back up why we are doing this. They are not just based off, "Everybody else is doing it," or those kinds of things. I tend to avoid security

> bandwagons because this is a business where if you listen to vendors, it is all over. They will have you doing all kinds of crazy, wacky stuff… Now for us, why do we do that on VPN? Because VPN is no different than if you're plugging into our campus network. You have significant access to our network when you do that, and so when that extends beyond the university, that is a concern, knowing that user IDs (and passwords) are compromised. And so if somebody falls for a fishing attack, do we want somebody in China, Russia, whatever, to be able to literally act like they are part of our university network?

It is noteworthy to see how the CISO's one of the phrases resonates with TURSAP findings. He mentioned, "when he sits [with a departmental chair or users] and explains *why*" the IT department is implementing a security measure (in this case double authentication), he found that "those conversations tend all of a sudden make people take pause." The CISO is much aware of what we named adequate communication and justification in the eyes of the users. It could be that these "conversations" are not taking place on a wider, longer, more frequent, deeper, richer and systematic ways with the wider employee community of PHEI.

I wanted to address the carefully planned security measures based on evidence. Therefore, I asked one of the obvious and much repeated concern about the frequent changes of the password in PHEI (every 6 months) and that several users complained that they do not change their banking password this often. Therefore, PHEI was unnecessarily going beyond the security measures of the banking industry.

The CISO explained the importance of the positions of a banking employee (and by extension of a university) and that of a customer:

> I do not know what examples there would be of that. I mean I know the banking sector very well. I am unaware of us going beyond the banking sector anywhere… So [regarding the password change] as a personal bank individual that is correct [you do not change your password every 6 months]. If you are an employee at a bank, absolutely [i.e. you do] . So you've got to remember what the perspective is. So as a consumer of that, yeah, the bank's not going to force you to change your password. That is your personal information that you are accessing. As an employee of the bank, who has access to broader information, they absolutely.

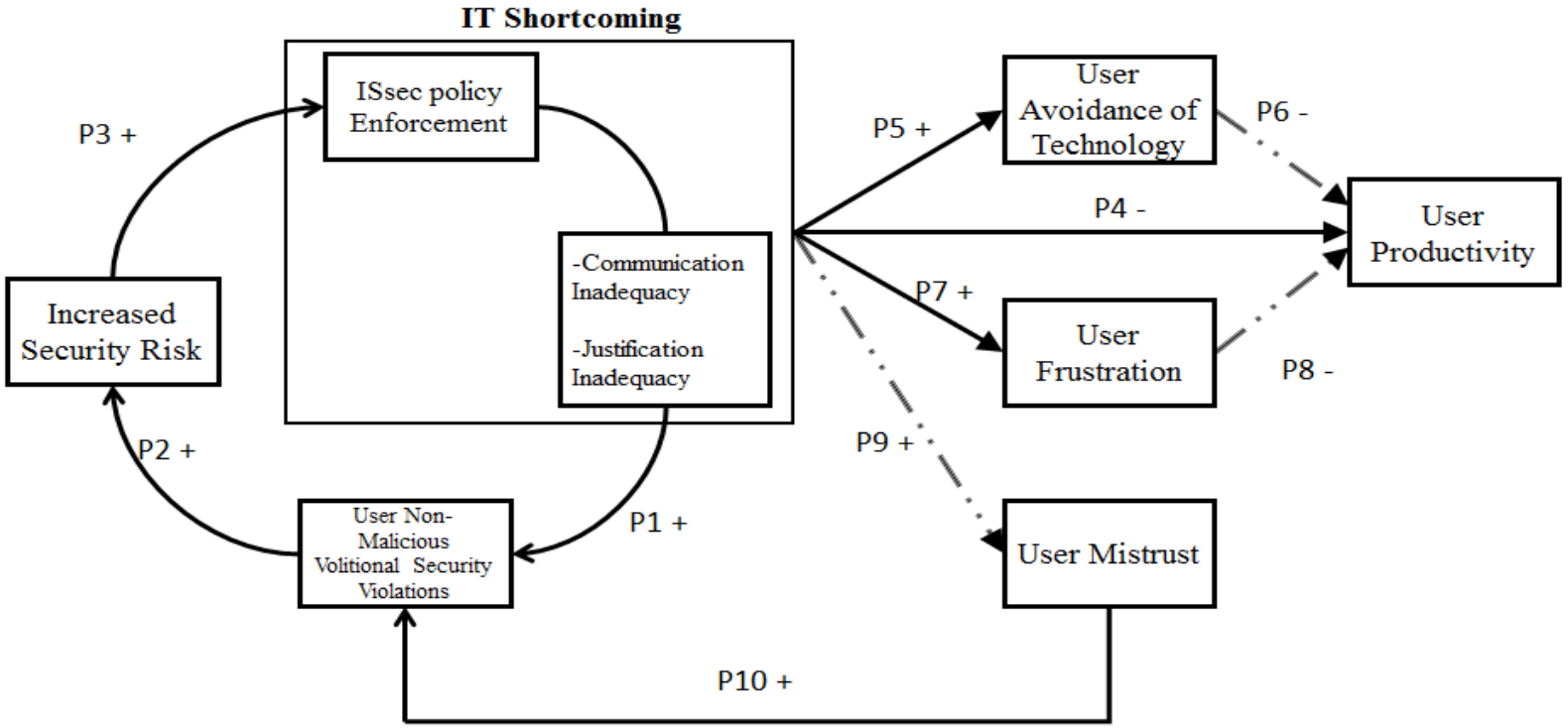

Figure 4.4. The Theory of Unintended Reversed Security Action and Productivity (TURSAP)[1]

[1] The dotted lines are to show the propositions supported by the extant literature, not by the dissertation data.

> And here's what I will argue, honestly. I do not mandate that. You want to know who mandates that? Our external auditors. Our external auditors that come in and do our financial audits, those are the folks that mandate what our changes are for password changes. I would agree. I think probably doing once a year would probably be more secure and I could up the requirements of what a password is, but the auditors require that we have it at 180 days, and so that is what it is, but I think the other thing is perspective, right? And so when you compare it it's like, "Okay, what's your role with that organization? Does it map to the risk?" And so for the risk for a faculty member, if their account gets compromised, that's FERPA information. That is student grades. You see what I am saying? That is more than just their personal information at risk. Whereas when they access the bank, to be honest, it is just their personal information. It is no more. So it is really understanding what is that perspective and role that you are playing when you are interacting with those accounts.

This above mentioned quote made me think how could the users' perspective may change by just learning that at least some of the security measures are not dictated by the IT department, but by the external auditors. How the users' trust toward the IT department may positively be affected when the users hear that the IT department sometimes [in this case regarding the frequency of the password change] does not agree with the outside auditors, without even be able to alter the security measure by the power of a senior security expert at the level of a CISO. This example, may raise all kinds of questions regarding the power of not just the IT department by that of the external IT auditors. Nevertheless, this confirms once again the importance of the free, unhindered communication between the user and the IT department.

After the example of the bank, the CISO continued his elaboration on his views on security measures, users' perceptions of these security and what all of these mean in the bigger picture. After the reader goes through the following quote, she might realize that as much as the users were ready to express their frustrations with the IT department, to the same extent the IT department might be willing to express their assumptions and frustrations about the users. This IT frustration may manifest itself in a situation where

the user for some reason, unnecessarily makes the work of the IT security department more difficult and painful.

> Let us just be honest. Security is basically trying to prevent the bad. It is insurance. It is, "Oh, that won't happen to me." Until it does. And if you look nationally, when do people generally come in and really want to have these conversations? When something bad happens, or when something almost bad happens, and sometimes that is the case when I end up getting involved on campus. A department has what I call a near miss and boy we got lucky, and all of a sudden oh, they want to talk to me all day long, right? Oh come on in, tell us what's going on, tell us what we can learn. Go look at what happened at Rutgers in the last week. Denial of service attack literally knocked them off, gone. You go and see some of the things where university presidents' email accounts have been spoofed and all of a sudden, somebody is doing a wire transfer, right? Saying, "Go ahead and transfer this money to this account. It's for this that we're doing." Boom, gone. And so the stories are out there, but it feels kind of like that, "Oh, it's okay. It never happens to us." And that's where I get sort of, it's difficult, right? Because I cannot really go and say, "Hey, this person on campus did this and yeah, it does happen here." Now can I say it more generally? Do we have people that fall for fishing and spearing scams? Absolutely. Absolutely. And so because of that, I sort of give – I'm not as likely to do that in writing, as you can imagine, but we do give the in person stories and explaining, "When you click on that email link, this is what happens. They go and start abusing your account, sending spam messages. They go and see if you have personal information. They go and see what access you have. They go and access your personal payroll." Right?
>
> I think people, let us be honest. Most people will say they care but, in practice, they do not really give a rip about the university's information. I am not going to lie, that's just the facts, right? It is about convenience, it is about getting their job done, it's not about making sure that things are protected all the time. I understand that. But when you make them realize that it's their information, sadly it ends up changing the view a little bit. It is like, "Well yeah, I don't want my social security number out there floating around." Oh, now you're interested, right?

Although the denial of service attack example that the CISO gave resonates more with the users' compromised accounts, the president's example is not helpful for the conversation at hand and for a good reason. The virtual majority of the users do not hold a powerful and sensitive positions like that of a university president or an organization's CEO. Nevertheless, the soundness of the analysis in TURSAP continued to be confirmed by the CISO's saying "when you make them realize that's their information" they become "interested". Realizing the CISO's full healthy grasp of the situation, I urged him to disclose what are the practical steps his department undertook in the past in order to

promote adequate justifications for the security measures. He mentioned his efforts in advancing communication and awareness campaigns via 1) the training of the new faculty and new staff orientations, 2) the social media awareness campaigns and endeavors on Twitter and Facebook and 3) the one on one explanation, council and advice for departments whenever they experience a security breach. Nevertheless, he was quick to mention that with the training of new faculty and staff he is probably reaching only 2% of the university users, the enrollment of the social media was low and mainly concentrated among student population. I realize the third option is an after-a-fact strategy that could not be ideal in preventing security breaches from happening in the first place.

Among the options the CISO iterated a mandatory online security training for staff and faculty was the last one. After clearing the secondary hindrance of culture the problem boiled down to budget (PHEI's culture for so long did not encourage mandatory trainings since it is a private institution, but now after some federal and state level legislations in place, this culture started to be more accepting of mandatory trainings). Professional online security engaging trainings need platform and a huge budget, which the IT department lacks.

I continued addressing some of the most contended subjects on security measures and comparing and contrasting the perceptions of each of the IT and the user sides on the subject. One of the main the concerns of a marketing department in the analysis section, was that the marketing department's program is put at a competitive disadvantage among its competitors because of PHEI's IS security constraints. In the past, the IT department has denied the access and use of a free google analytics tool that could have helped the

program in targeting and recruiting prospective students in a smarter customized way. The user perspective was that this issue is an adversarial dance, and that the IT department "would rather spend an hour saying all the reasons they can't do something instead of a half hour figuring out how they might be able to do it" (Respondent 25, anonymous). The following is the answer that I could get form the CISO on this hotly contended subject.

> Do you want somebody to track where you go with a mouse as you go through our website? That's the types of technologies that we start talking about. And here's the deal, if those technologies are free, guess what they're doing. They're aggregating that stuff. So the perfect example, if you've ever gone on Google, you search for something, "Hey, I'm looking for a new pair of shoes." And next thing you know, next site you go to, all of the advertisements are for new shoes, right? That's what's happening. Everybody's using the free Google analytics, and the result is that AdWords is very specifically able to target you as a user. So that's the problem with the analytics piece. There is, go out and look. *Schools are considering making admissions decisions based off of how you interact with their website.* That's where we're at, and I'm not going to lie, I'm a privacy guy, right? I believe that there is a right to privacy when it comes to your online interactions. There's competitors that don't have the same ethical and moral standards as [PHEI] University. Does that mean that we're going to go and do those things? Right? So that's more the statement is who do we want to be? Do we want to be the school that has a higher moral ethical standard and respects people's privacy and uses vendors who don't sell out privacy of people who just visit our website or want to apply to the university, or are we going to go ahead and try to give that away? That's a choice. That's a real key choice, and it's a struggle. Because they're right, other people are doing it. Absolutely. Amazon has been doing it for years. Google has been doing it for years. But is that who we are? And that's a key question and that's a competitive environment question that's been happening more and more here on campus. We're careful, because our privacy policies that are written today really don't allow individual user tracking. They don't for any purposes beyond security. Does that mean that it can't be done? No, but really, what do you need? Do you need to know this information in aggregate, or do you need to track a person? If you need the information in aggregate, that can be done, right? That can be done with purchased solutions. They aren't cheap, and at the end of the day when you look at it, departments have to make hard fiscal decisions. So that's one of the reasons why this becomes a contentious point.

This was a difficult subject to grasp. Both sides have valid arguments. I wanted to bring both sides on one table in order to continue the discussion just to avoid the "tis for tat" accusations. One may think tracking a user is bad. Another may say admitting students based on their interaction with the university website is not wrong if the metrics,

indicators or measurements gathered on the website are good indications of a genuine interest in an educational program, making the prospective student a valuable one to be admitted to the program . I went back to do some research on the topic of the website metrics. Baltzan (2015) mentions several of them. Website metrics could include a) "length of exposure" which measures how long does the prospective student stay on a page of PHEI, presumably an indicator if he is reading and is genuinely interested in the program, b) "page exposure", which is the average number of pages that an individual exposes himself to c) "click-through" is when a user click on a highlighted link (usually an advertisement for businesses, or important additional detail on the university program) and d) abandoned registrations (the number of times an abandoned registration process to a program may indicate the student's hesitation and ambivalence of joining the program). These types of website metrics may be used in the decision making process of admitting a person to an educational program, beyond her high GMAT or GRE scores and the richness of her Curriculum Vitae. Apparently, there are still no federal legal rulings if such tracking of users (or admission of students based on his website behavior). Amazon and google do such personalized tracking according to the CISO. Nevertheless, he does not want to take the university down that path. That is what kindled the fire of contention between the user and the IT.

The question that should be asked here is who wrote the "privacy policies that are written today that don't allow individual user tracking" (a quote mentioned above by the CISO). The user has all the right to know if the IT department is the sole responsible behind such policies or that the higher administration (president, vice presidents) are aware and approving or commanding such practices. If it is the latter, then the user might

change his attitude toward the IT department. If it is the former, then the question remains if the IT is trespassing on the productivity of the business units. Although the phrase “I’m not going to lie, I’m a privacy guy” may betray that the IT could well be behind pushing stricter security and privacy measures, nevertheless the situation is far from being clear in PHEI how the decisions are being made, and if the business units and the IT need to sit together for negotiated decision making. One thing is clear, that constant, ongoing, systematic, and frank Q&As and inputs between the users and the IT security team regarding the necessity and justification of the security measures are not a secondary matter. The feasibility of this type of dialogues and conversations between both parties should be the focus of future research in IS security.

CHAPTER FIVE

Implications and Conclusions

Theoretical and Managerial Implications

The analysis demonstrates what may happen when an IT department enforces increasing security measures without an adequate explanation. The study shows how and why security measures may increase security risks if they are not justified and well explained in the eyes of the users. This dissertation has several implications both on theoretical and managerial levels.

Theoretically, this is the first study that uses a grounded theory methodology to create and advance a theory of reversed action in security compliance effectiveness. To date, virtually all the theoretical advancements on security compliance assumed the inherent desirability of increased security measures toward compliance, but this dissertation shows that there is a strong caveat to pressing that argument too far too soon without taking into account the reverse effect of ever-increasing security measures. If the security measures are not well communicated and well justified in the eyes of the users, there will be unintended and negative effects on user productivity and overall organizational security.

The TURSAP theory seems to resonate well with Technology Affordances and Constraints theory (TACT). Technology affordance points to what are the potential uses of a certain technology in the hands of a user or an organization (Majchrzak & Markus, 2012). According to TACT a potential use or affordance can also be a potential constraint or a hindrance. A potential constraint inherent in the use of a technology may limit or

prevent a user or an organization from attaining the purpose behind the technology use. Taking the TACT's theoretical lens to its logical conclusion may allow us to see that IS policies and security measures also posit affordances and constraints. To illustrate the concept of affordances and constraints I will give a couple of examples related to technology and then give a parallel example related to the affordances and constraints of increased ISsec measures. After describing the parallels, I highlight the differences between TURSAP and TACT.

On the national and international levels, the information age and social media and the Internet have acted (at least partly) as catalysts to depose some dictatorships throughout Middle Eastern countries by exposing the crackdowns of military units on peaceful protestors. Western democracies had the chance to closely follow the "secret" crackdowns (affordance). Dictators in Tunisia, Egypt, Libya, Yemen, and Syria were unable to control the social media (Facebook and Twitter) exposing their atrocities in front of a watching world. At the same time, the Islamic State in Iraq and Syria (ISIS) is using these same social media tools to recruit thousands of European and North American born Muslim citizens to go join their fight or their state. Western countries are not able to track down or to halt the exodus of the recruitment of the male and female youths joining ISIS via social media (constraint). The same technology (Facebook and Twitter) has been a source of affordance and constraint for liberal democracy.

On the organizational level, allowing a bring-your-own-device (BYOD) policy is an affordance that enables students, staff, and faculty to bring their own devices to a university and communicate freely with each other. This same policy posits a constraint on the push of technical antivirus or patch updates. The policy constrains the ITS from

owning the different devices and systematically pushing security updates on it. On a more relevant note to our topic, as our study shows, ISsec policies can be affordances and constraints at the same time: affordances on the level of increasing security, constraints on the level of lesser productivity, increased NMV-SVs increased mistrust and sometimes increased security risks.

These results are compatible with the reasoning behind TACT in one hand but it differs from TACT in some important measures in the other hand. According to TACT, technology provides both affordances and constraints to the user or the organization. This dissertation shows that security requirements provide affordances and constraints at the same time. This may contribute in expanding the TACT into ISsec policies instead of keeping it just in the technology dimension. Nevertheless, TURSAP is different from TACT in two important dimensions. First, TURSAP explicitly describes what are the downsides or constraints. TACT does not do that. It is too general. TURSAP describes that the primary negative consequences of increased security measures are "decreased security and productivity" and the channels toward these negative consequences are clearly accounted for in the theory (i.e. user non-malicious volitional security violations, user frustration, user mistrust and user technology avoidance). TACT mentions affordances and constraints (in general terms) but does not describe what are these specific affordances and constraints. Second, TURSAP explains the specific reason of the negative consequences, mainly the IT shortcoming. TACT does not do that.

One thing TACT surpasses TURSAP, is its ability to account (in is theoretical model) for both the positive (affordances) and negative (constraints) sides of technology. TURSAP's strength in its explanatory power in accounting the detailed mechanisms of

the *constraints* of ISsec policies, limits the theory in expressing the *affordances* of the same. There are strengths and limitations of any theory, TACT and TURSAP have their shares of both.

On the managerial level, this dissertation shows there are important security aspects for IS managers to take heed. Any security measure to be implemented without enough communication and justification in the eyes of the employees will lead to counterproductive outcomes. There are sufficient signs pointing to increased frustration, increased security circumvention, increased technology use avoidance, decreased productivity, and increased security risk. CISOs can no longer afford to think that users will automatically and blindly follow whatever security requirements IT department implements. Reusing same passwords across work related and personal accounts increase security risk. Since reusing passwords across sites is strongly discouraged by the IT department, the users need tools to remember (or let the software do the memorizing) their ever increasing number of complex passwords. A solution could be the adoption or creation of password storage and management software solutions by IS departments. Current IT departments are still fearful of recommending the available third party solutions (ex: LastPass). I suggest that each organization develop its own password storage website for its employees to use. Thus, the organizational user passwords could remain inside the secure firewalls instead of being written on papers, saved on unsecured smartphones prone to be lost or stolen, or saved on third cloud computing outsourced servers like LastPass.

More importantly on the managerial level, the IT department faces the challenge of humble acceptance of the questions raised by the end user practitioner. IT departments

need to embrace critic in a gracious way, and try to win the user on its side rather than dictating the rules to be followed. The debate and decision whether the a certain security measure is necessary or unnecessary, justified or unjustified may only be settled (at least in the minds of the users) by constant, ongoing, systematic, and frank Q&As and inputs between the users and the IT security teams. Where to draw the line in the debate and who gives the final decision on what is necessary or unnecessary is open to debate and is part of the managerial implications of this dissertation and ground for future research.

Limitations and Conclusion

This dissertation began studying the security literature in light of increasing security breaches and violations. Although more than 25 years of academic research in IS security has been conducted, the study found that the majority of research assumed ISsec measures and policies are a panacea. That assumption is proving to be incomplete, and a small but an increasing number of studies are shedding light into the darker side of ISsec measures.

The importance and implications of this research were discussed earlier. Nevertheless, as with any exploratory study, the present work is not without its share of limitations. The following discussion identifies some of the limitations and suggests some remedies that future research can adopt and apply.

First, this research is conducted at one site. Some may argue that the validity of one site is questionable. Nevertheless, Sarker et al., (2013) analyzed 98 qualitative articles and found that 52% of them used one case-based research. Indeed, case study methodologists have been asserting that one case-based studies are adequate (Lee and Baskerville, 2003; Walsham, 1995).

Second, the results are drawn from one industry type, namely, education. This issue, it may be argued, limits the generalizability of the findings. It is true that limited generalizability is a threat to any qualitative research; nevertheless, we can prove that the educational site where this dissertation chose to conduct the research is a good proxy of other industries, particularly in terms of security breaches and research. Universities are the second most targeted sector (on a par with the retail sector) attacked by hackers after the healthcare sector. In 2014, 37% of reported security breaches involved the healthcare sector, and 11% and 10% of all the security breaches were related to the retail and educational sectors, respectively, as reported by Symantec and NBC news (Wagstaff & Sottile, 2014; NBC News, 2015). In 2015 alone, three major high profile security breaches hit Penn State University, the University of Connecticut, and the University of Virginia (ibid). The reason that hackers target universities is to steal personal data (Thompson, 2014). Finally, TURSAP theory is still in its exploratory stage. The research on the downsides of ISsec measures is still young and evolving. There is a need for confirmation of the theory advanced in this dissertation with quantitative test research. Nevertheless, the data in the analysis and results sections are robust and clear.

Future research can improve this dissertation and extend the application of the results. This exploratory research provides a basis for future research to study the adverse effects of ISsec policy implementation. Several suggestions are advanced in the following paragraphs.

First, more detailed research must be conducted to understand why the IT behaves how it behaves, unilaterally in the security policy decision making that affect the productivity level of employees, and what are more elaborate answers on all the

assumptions of the users regarding the IT department. Second, future research needs to study whether the IT department will be able and willing to take the advice, approval and the consent of the end users regarding the implementation of security measures that affect the users. IT departments' security experts may altogether dismiss even the hint of sitting with "end users" to "negotiate" the terms of security measures. Only future research can explore the findings. How the IT security understands justifying its security measures in front of the users is still unkonwn that needs to be investigated in future research.

Second, how should the IT department increase its efficiency and effectiveness in justifying the increased security measures? What are the theoretical and practical resources that the IT department can employ in order to adequately explain and justify the increase of security measures? Third, questions still remain and need to be addressed regarding the validity and success of Q and A open panels between faculty and users on one side and IT department on the other side, understanding debating and arguing for the validity of some security measures. Research is still absent on such endeavors and it is too early to pass judgement if such revolutionary outlook on how to approve security policies and measures will be successful in the future. Fourth, and finally, to further prove the validity of the propositions advanced in TURSAP theory, a quantitative test of the theory must follow this dissertation.

In conclusion, I highlighted increased ISsec measures and the paralleled steady amount of NMV-SV of employees. In this dissertation, it is argued that ITS shortcomings in terms of the lack of communication and inadequate justification of advanced ISsec measures are the reasons that many organizational employees circumvent ISsec measures. To reach this conclusion, many employees in a higher educational firm were

interviewed, and were found to be complaining about ISsec measures by the IT department. IT department employees were also interviewed to establish their perspectives on things. The results showed that the IT department has increased ISsec measures coupled with its shortcoming in not justifying the increase may lead to an increase in NMV-SV from the employees, and thus lead to an increase security risk. Thus, ISsec measures may increase security risk rather than decrease it. This is counterintuitive, but very insightful if all the intricacies and dynamics are observed in the process of implementing increased security measures. The results further show that increased ISsec measures may lead to increased frustration, mistrust toward IT departments, increased technology use avoidance, and ultimately decreased productivity. All of these potential effects need to be considered by IT departments prior to implementing security measures. The managerial implications were discussed, and a theory was advanced (TURSAP) to explain the dynamics of how and why the downsides of increased ISsec measures can happen and be understood. The TURSAP theory is the main theoretical and research contribution of this dissertation.

APPENDICES

APPENDIX A

Semi Structured Interview Guide

Interview Duration:

Job Title (Faculty, non-IT staff, IT staff, student); College (----------); Department (-------)

Introduction to Informant: Hello. Thank you for agreeing to sit with me today and answer a few questions about the security policies here at _____. I want to remind you that everything we talk about will remain strictly confidential, and your own personal answers and identity will never be revealed to anyone. Only summarized answers from the entire group will appear in our research articles. Please be honest and complete in your answers, and please let me know if you need any clarification. Finally, remember that you can decline to answer any question, and you can quit at any time. Let's begin …

For IT Team Members

1) Reflecting upon the last 10 years of computer security policies, what are the things that changed? What are the things that remained the same? How have new security measures affected your own work?
2) How is the IT department able to chase a moving target (ever-changing security threats, therefore ever-changing security policies)? How often are the policies updated?
3) How does IS policy compliance increase IS security effectiveness? What in your opinion is IS security effectiveness?

4) How do you know your policy is effective?
5) Can you give me an example of a security policy your users may think is over-the-top but that you feel ITS has to do for reasons other than security – such as maintaining an image of being on top of things, or because everyone else is doing it, etc…;
6) Have you ever faced a situation in which security policies have hindered your own ability to work effectively in your role as (insert job title)? How did you deal with them?
7) Describe what you see as the biggest threat to IT security of the university? How about to individual faculty, staff and students?
8) How do you set policies? How do you communicate these policies?

For Employees/Users

1) How important is computer security in your professional work? How do you handle or manage data that is sensitive or important and might be threatened by loss or theft? Is this more important now than it was five or ten years ago? Why?
2) Describe what you know about your university's IS security policies.
3) How do security policies enable and constrain your work practice? In what ways do IT security policies make you more effective in your role as (faculty, staff, administrator…)? Are there ways that you feel the security policies constrain your work? If so, can you give me an example?…
4) For you personally (not for your unit or department), what the most important security concerns you have regarding IT (including your desktop, laptop, personal data on the University systems, mobile devices etc)? In the last 10 years, have

you been facing some difficulties in order to comply with security policies? What did you do about them?

5) Why do you think ITS does what it does regarding security policies?
6) Are there specific IT security policies that you feel are intrusive or overly demanding?
7) Are there areas where you feel there should be more security than there currently is?
8) What is your perception of ITS?

APPENDIX B

Interpretive Methodological Guidelines
(Adapted from:Sarker and Sarker, 2009)

Aspect of the study	Methodological considerations	Additional description	Illustration (where applicable)
Organization choice and entry	Selecting suitable organization to study intensively.	The goal was to study a "representative" organization in terms of the phenomenon or the research topic, that is, the downsides of the IS security policies; at the same time, to study a critical case in terms of the quality/reputation of the organization, so that normative implications for future practice could be derived (Patton, 1990; Flick, 1998)	PHEI was chosen because it: a) had a robust security policies relative to other higher educational institution and b) belongs to a sector (education) that is constantly witnessing high profile security breaches, second only to healthcare and on par with retail industry. The access was also facilitated by a gatekeeper who knows the author as well as the CISO of PHEI.
	Entering the field with credibility	"Expert approach" resulting in immediate legitimacy and credibility of the researcher.	Official email from the gatekeeper who is a chairperson and faculty, introducing the research project and setting up initial meeting/interview with CISO.
		The researcher is not only the "observer" but also the "observed," i.e., organizational members tend to scrutinize researchers' actions, particularly in the initial stages (Patton, 1990).	I consciously endeavored to cultivate and present independent academic identity by: a) maximum readiness and preparation for the interviews and b) preserving confidentiality and anonymity at all costs (Myers & Newman, 2007)

Aspect of the study	Methodological considerations	Additional description	Illustration (where applicable)
Data collection	Choice of interviewees	Suitable respondents were suggested by the CISO and one of the IT administrators who also helped set up some of the interviews.	I sought to diversify both the width and the depth of perspectives by interviewing respondents with variety of roles, projects, levels and backgrounds.
		"Snowballing" technique used to recruit respondents among users i.e. faculty, staff, admin (Patton, 1990)	Other respondents also identified and suggested relevant respondents.
	Conduct of the interviews	Being sensitive to principles of: (1) "flexibility" (2) "non-direction" (3) "specificity," and (4) "range" (Flick, 1998)	1) I adapted the schedule of the meetings (rescheduled or shortened them) to accommodate the busy lifestyle of IT department staff members. 2) I maintained a non-directive style of conversations. 3) I asked specific questions for clarification. 4) I slightly changed the interviews conducted, based on the ability and willingness of respondents to elaborate on security issues.
	Maintaining empathetic neutrality	"Nonjudgmental form of listening" (Walsham, 1995; quoting Zuboff, 1988); empathizing with interviewees' frustrations but simultaneously maintaining distance (Patton, 1990)	Patience and sympathy were the main characteristics shown when respondents expressed frustration with security policies, while restraining the probing of "juicy" stories elaboration that were not relevant to the downsides of the security policies.

Aspect of the study	Methodological considerations	Additional description	Illustration (where applicable)
Data analysis and representation	Unearthing and refining concepts through constant comparison	In Holton's words (2007, p. 277), "the purpose of constant comparison is to see if the data support and continue to support emerging categories. At the same time, the process builds and substantiates the emerging categories " The process is consistent with the notion of the hermeneutic circle, and involves not just "induction," but also "abduction" (Bryant and Charmaz, 2007).	In vivo codes were used (open, axial and selective coding) according to Corbin and Strauss, 2008. Induction was heavily used in the initial analysis, nevertheless abduction became pertinent in the Development of the different dimensions/subdimensions of the adverse effects of security and its relevant consequences.
	Triangulation	Primarily "source triangulation" (Corbin and Strauss, 2008); comparison of responses Across respondents and their levels, and administrative roles. Lack of agreement in triangulation not seen as indication of invalid category necessarily, but as an opportunity to include/explore differing perspectives and unearth additional contingencies (Flick, 1998).	Whenever possible, we asked the same specific question (ex: VPN, password policies, encryption rules…) to different respondents in different departments and roles, in order to get a variety of perspectives. In some cases, disagreement emerged among respondents regarding the validity of some policies. I did not treat these differences as problems but as opportunities to investigate more and have a richer understanding of the results.

Aspect of the study	Methodological considerations	Additional description	Illustration (where applicable)
	Being suspicious about evidence	Sensitivity to possible biases in interviews (Klein and Myers, 1999).	I was aware that individuals in the IT department may have a more favorable views to the IS policies but the users, especially those who have high administrative roles and many systems may be inclined to a more critical position. This bias was balanced when a good amount of IT service staff who serve the needs of the faculty and staff, also complained about some security policies.
	Member checking	Validating/checking researchers' interpretations with interviewees (Flick, 1998).	Figure 4 (TURSAP theory) was presented to 20% of the respondents. I evaluated the validity of the results by their reaction, thoughts and inputs.
	Being sensitive to ethical	1) Balancing anonymity and disclosure (Flick, 1998).	1) I ensured that the following were concealed: (a) organization's identity, (b) the respondents and their gender, role, departments and schools and (c) the actual technologies and projects that were being used.
		2) Ensuring that the transcripts and otherdata were kept secure (Myers and Newman, 2007).	2) I ensured only the author and transcribers had access to the empirical data.
		3) Treating respondents, their knowledge, and their time with respect (Myers and Newman, 2007).	3) Readily shortened or rescheduled meetings according to the schedules and needs of respondents.

REFERENCES

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of internet monitoring on job attitudes: The mediating role of employee trust. *Information & Management, 43*(7), 894-903.

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology, 86*(4), 797–804.

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extra-role performance. *Journal of Applied Psychology, 91*(1), 221-232.

Amabile, T., & Kramer, S. (2011, September 3). *Do happier people work harder?* Retrieved November 23, 2015, from http://www.nytimes.com/2011/09/04/opinion/sunday/do-happier-people-work-harder.html?_r=0

Anderson, J. M. (2003). Why we need a new definition of information security? *Computers & Security, 22*(4), 308-313.

Andriole, S. (2015, October 30). *Top ten CIO concerns for 2016*. Retrieved January 5, 2016, from http://www.forbes.com/sites/steveandriole/2015/10/30/top-ten-cio-concerns-for-2016-its-deja-vu-all-over-again/

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

Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2010). An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure. *Information Systems Research*, *21*(1), 115-132.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS quarterly*, *30,* 413-438.

Bagayogo, F. F., Lapointe, L., & Bassellier, G. (2014). Enhanced use of IT: A new perspective on post-adoption. *Journal of the Association for Information Systems, 15*(7), 361-387.

Baltzan, P. (2015). *Business driven technology, 6th edition*. McGraw-Hill Education.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quartarly, 22*(1), 31–60.

Besnard, D., & Arief, B. Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253–264.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Bryant, A., Charmaz, K. (2007). *The sage handbook of grounded theory*, Sage Publications, London.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM*, *53*(3), 126-131.

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

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49-87.

Chen, Y., Nyemba, S., & Malin, B. (2012a). Detecting anomalous insiders in collaborative information systems. *IEEE Transactions on Dependable and Secure Computing, 9*(3), 332-344.

Chen, Y. R., Ramamurthy K & Wen, K.-W. (2012b). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

Cisco Systems. (2006). *Perceptions and behaviors of remote workers: Keys to building a secure company*. White Paper, Cisco Systems, San Jose, CA.

Cisco Systems. (2011). *Cisco connected world technology report*. San Jose, CA, 2011.

Corbin, J., Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications Ltd., United Kingdom.

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches (2nd ed).* Thousand Oaks, CA: Sage.

Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, computer crime, and IS misuse at the university. *Communications of the ACM*, *49*(6), 85-90.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, 50(10), 113-117.

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

D'Arcy, J. & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model, *Decision Sciences 43*(6), 91-1124.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.

Davis, L. F. (1987). *Moral judgment development of graduate management students in two cultures: Minnesota and Singapore*, unpublished doctoral dissertation, University of Minnesota, Minneapolis, MN.

De Guinea, A. O., & Markus, M. L. (2009). Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *MIS Quarterly*, *33*(3), 433-444.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*, 293-314.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breach61es: An exploratory analysis. *Information Resources Management Journal,* 18(4), 21-39.

Dourish, P.; Grinter, R.E.; De la Flor, R.D.; & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing, 8*(6), 391–401.

Dunn, J. & Schweitzer, M.E. (2005). *Why good employees make unethical decisions: The role of reward systems, organizational culture, and managerial oversight*. In Managing Organizational Deviance. Thousand Oaks, London and New Delhi: Sage Publications (Kidwell RE and Martin CL, Eds), pp 39-68, Sage, Thousand Oaks, CA.

Eisenhardt, K. (1989). Building Theories from Case Study Research. *Academy of Management Review,* 14(4), 532-550.

Flick, U. (1998). *An introduction to qualitative research*. Sage Publications, London.

Frantzen, D. (2000). Innovation, international technological diffusion and the changing influence of R&D on productivity. *Cambridge Journal of Economics, 24*(2), 193-210.

Fullbright Commission. (2015). *Cultural differences*. Retrieved August 24, 2015, from http://www.fulbright.org.uk/pre-departure/us-culture/cultural-differences

Gasson, S. (2004). Rigor in grounded theory research: An interpretive perspective on generating theory from qualitative field studies. In M. E. Whitman & A. B. Woszczynski (Eds.), *The Handbook of Information Systems Research*. Hershey, PA: Idea Group Publishing.

Gattiker, U. E. & Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research, 10*(3), 233–254.

George, J. F. (1996). Computer-based monitoring: Common perceptions and empirical Results. *MIS Quarterly, 20*(4), 459-480.

Glaser, B. & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Publishing Company, New York, NY.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567-594.

Gregory, R. W., Beck, R., & Keil, M. (2013). Control balancing in information systems development offshoring projects. *MIS Quarterly, 37*(4), 1211-1232.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, *49*(6), 320-326.

Guo, K., Yufei, Y., Archer, N., & Connelly, C. (2011). Understanding non-malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, *20*(3), 257-278.

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

Herath, T., & Rao, H. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Decision Support Systems, 47*(2), 154-165.

Holton, J. A. (2007). The coding process and its challenge. A. Bryant, K. Charmaz, eds. *The Sage Handbook of Grounded Theory*. (p. 265–290). Sage Publications, London.

Hovav, A. & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea, *Information & Management, 49*(2), 99–110.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policy: The critical role of top management and organizational culture, *Decision Sciences, 43*(4), 615-659.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6-48.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54-60.

Hunter, P. (2003). Computer espionage. *Computer Fraud & Security*, *7,* 16.

Johnson, M. E. (2008). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems*, *25*(2), 97-124.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518-555.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive*, *9*(3), 2012-52.

Keith, M., Shao, B., & Steinbart, P. (2009). A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems*, *10*(2), 63-89.

Kirsch, L. & Boss, S. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. Paper presented at the International Conference of Information Systems, (pp.1-18). Montreal, Canada. http://aisel.aisnet.org/icis2007/103

Klein, H. K., & Myers. M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67–93.

Kleis, L., Nault, B. R., & Dexter, A. S. (2014). Producing synergy: Innovation, IT, and productivity. *Decision Sciences*, *45*(5), 939-969.

Knapp, K, J. (2005). *A model of managerial effectiveness in information security: From grounded theory to empirical test* (Doctoral Dissertation), Retrieved from ABI/INFROM in August 2015.

Kock, N. (2004). The three threats of action research: A discussion of methodological antidotes in the context of an information systems study. *Decision Support Systems, 37*, 265-286.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in Information systems research, *Information Systems Research, 14*(3), 221-243.

Lee, S. M., Lee, S.G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Leidner, D. & Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, *30*(2), 357-399.

Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association of Information Systems*, *1*(12), 1–31.

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions - planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143-158.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems,* 48(4), 635–645.

Lim, V. K. G., Teo, T. S. H., & Loo, G. L. (2002). How do I loaf here? Let me count the ways. *Communications of the ACM*, *45*(1), 66-70.

Lincoln, Y.S & Guba, E. G. (1985). *Naturalistic inquiry.* Beverly Hills, CA: Sage.

Loch, K. D., & Conger, S. (1996). Evaluating ethical decision making and computer use. *Communications of the ACM, 39*(7), 74-83.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

London, M., & Bray, D. W. (1980). Ethical issues in testing and evaluation for personnel decisions. *American Psychologist, 35*(10), 890–901.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal, 25,* 433-463.

Lowry, P.B., Moody, G.D., Galetta, D.F. & Vance, A. (2013). The Drivers in the Use of Online Whistle-Blowing Reporting Systems. *Journal of Management Information Systems, 30*(1), 153-189.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal, 25*(3), 193-273.

Majchrzak, A., & Markus, M. L. (2012). Technology affordances and constraints in management information systems (MIS) in E. Kessler (Ed.), *Encyclopedia of Management Theory*, CA: Sage Publications.

Marshall C. & Rossman G B. (2011). *Designing Qualitative Research*, 5th Edition. CA: Sage Publications.

Martin, K. & Freeman, R. E. (2003). Some problems with employee monitoring. *Journal of Business Ethics, 43*(4), 353-361.

Martin, P., Turner, B. (1986). Grounded theory and organizational research. *The Journal of Applied Behavioral Science, 22*(2), 141-157.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* (2nd ed.). CA: Sage Publications.

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research*, *26*(3), 565-584.

Myers, M. D. (2009). *Qualitative Research in Business & Management.* London, UK: SAGE Publications Ltd.

Myers, M. D., & M. Newman. (2007). The qualitative interview in IS research: Examining the craft. *Information & Organization, 17*(1), 2–26.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

NBC News. (Thompson 2015, May 15). *Penn State Hit by China-Based Hacker, University Says*. Retrieved November 4, 2015, from http://www.nbcnews.com/tech/security/penn-state-hit-china-based-hacker-university-says-n359631

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective*, Decision Support Systems, 46*(4), 815-825.

Orlikowski, W. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS Quarterly, 17*(3), 309-340.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In 40th Hawaii International Conference on System Sciences (HICSS 07), Hawaii, USA.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*, (2nd ed). CA: Sage Publications.

Peace, A. G., Galletta, D., & Thong, J. Y. L. (2003). Software privacy in the workplace: A model and empirical test, *Journal of Management Information Systems*, *20*(1), 153-177.

Ponemon Institute (2012). *2013 State of the Endpoint*. Traverse City, MI (available at http://www.ponemon.org/blog/2013-state-of-the-endpoint).

Posey, C., Bennett, R. J., & Roberts, T. L. (2011a). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes, *Computers & Security, 30*(6), 486-497.

Posey, C., Bennett, R. J., Roberts, T. L. & Lowry, P.B. (2011b). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, *7*(1), 24-47.

Post, G. V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security,* 26(3), 229–237.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study, *MIS Quarterly, 34*(4), 757-778.

PWC, PricewaterhouseCoopers (2013). *Global state of information security survey 2013*. New York, 2013.

PWC, PricewaterhouseCoopers (2015). *Managing cyber risks in an interconnected world: Key findings from the global state of information security survey 2015*. Retrieved from http://www.pwc.com/gsiss2015.

Quatraro, F. (2009). Innovation, structural change and productivity growth: Evidence from Italian regions, 1980–2003. *Cambridge Journal of Economics*, *33*(5), 1001-1022.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121-139.

Rest, J. R. (1979). *Development in Judging Moral Issues*, University of Minnesota Press, Minneapolis, MN.

Richardson, R. (2011). *15th Annual 2010/2011 Computer Crime and Security Survey.* Computer Security Institute (available at http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

Rosenberg, P. (2000, April). Facility security: Video monitoring-part 2. *EC&M Electrical Construction & Maintenance, 99*(4), 64.

Sarker, S., & Sarker, S. (2009). Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context. *Information Systems Research*, *20*(3), 440-461.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Qualitative studies in information systems: A critical review and some guiding principles, *MIS Quarterly, 37*(4), 3-18.

Schwartz, M. (2011, April 21). Lost Laptops Cost $1.8 Billion Per Year - *InformationWeek*. Retrieved November 22, 2015, from http://www.informationweek.com/mobile/lost-laptops-cost-$18-billion-per-year/d/d-id/1097314?

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.

Shaw, E., Ruby, K. G. & Post, J. M. (1998). The Insider Threat to Information Systems.[pdf], *Security awareness Bulletin*, *2*(98), 1. Available online at www.pol-psych.com/sab.pdf

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management and Computer Security*, *17*(4), 221-234.

Siau, K., Tan, X., & Sheng, H. (2010). Important characteristics of software development team members: An empirical investigation using repertory grid. *Information Systems Journal, 20*(6), 563-580.

Siponen, M. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information Management & Computer Security,* 8(5), 197–209.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The DATABASE for Advances in Information Systems*, *38*(1), 60-80.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-512.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64-71.

Skinner, W. F. & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research on Crime and Delinquency*, *34*(4), 495–518.

Smith, A. L., Baxter, R. J., Boss, S. R., & Hunton, J. E. (2012). The dark side of online knowledge sharing. *Journal of Information Systems*, *26*(2), 71-91.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow is security policies. *Information & Management*, *48*(7), 296-302.

Spears, J. & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal*, *22*(1), 77-94.

Stanton, J. M., & Stam, K. R. (2006). The visible employee: Using workplace monitoring and surveillance to protect information assets without compromising employee privacy or trust. *Library* Review*, 57*(9), 746-747.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1), 45-60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. CA: Sage Publications.

Strauss, A., Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* CA: Sage Publications.

Tapellini, D. (2014, May 28). *Smart phone thefts rose to 3.1 million in 2013*. Consumer Reports. Retrieved November 22, 2015, from http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

Thoma, S. J. & Davison, M. L. (1983). Moral reasoning development and graduate education, *Journal of Applied Developmental Psychology*, *4*(3), 227-238.

Thompson, C. (2014, August 21). *Hackers target colleges to steal personal data, university research*. NBC News. Retrieved November 4, 2015, from http://www.nbcnews.com/tech/security/hackers-target-colleges-steal-personal-data-university-research-n185866

Tyler, R. T. & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *The Academy of Management Journal*, 48(6), 1143-1158.

Vance, A., Lowry, P. B. & Eggett, D. L. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS* Quarterly, *39*(2), 345-366.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory, *Information & Management 49*(3), 190-198.

Vannoy, S. A. & Salam, A. F. (2010). Managerial interpretations of the role of information systems in competitive actions and firm performance: A grounded theory investigation. *Information Systems Research, 21*(3), 496-515.

Verizon. (2013). *Data breach investigations report*. Verizon Enterprise (available at http://www.verizonenterprise.com/DBIR/2013/).

Wagstaff, K. & Sottile, C. (2015, September 20). *Cyberattack 101: Why hackers are going after universities*. NBCNews. Retrieved November 4, 2015, from http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821

Wall, D.S. (2011). Organizational security and the insider threat: Malicious, negligent, and well-meaning insiders. *Symantec Research Report*, Mountain View: CA.

Walsham, G. 1995. Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*(2), 74-81.

Ward, M. (2015, September 23). *Does China's government hack US companies to steal secrets?* BBC News. Retrieved November 4, 2015, from http://www.bbc.com/news/technology-34324252

Warkentin, M., Johnston, A.C. & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*, 267-284.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of management review, 14*(4), 490-495.

Whitman, M. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*, 43-57.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403-414.

Workman, M. (2009). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information & Organization*, *19*(4), 218-232.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, *58*(2), 212-222.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24,* 2799-2816.

Young, E. (2014). *Get ahead of cybercrime.* (Ernst & Young's 2014 Global Information Security Survey).

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. Basic Books: NY.