Journal of the Midwest Association for Information Systems (JMWAIS)

Volume 2016 | Issue 2 Article 2

2016

Motivating Employees to Comply with Information Security policies

David Sikolia
dsikoli@ilstu.edu, dsikoli@ilstu.edu

David Biros
Oklahoma State University, david.biros@okstate.edu

Journal of the Midwest Association for Information Systems
Volume 2016 | Issue 2 Article 1

Date: 07-31-2016

Motivating Employees to Comply with Information Security Policies

David Sikolia

Illinois State University, dsikoli@ilstu.edu

David Biros

Oklahoma State University, David.Biros@okstate.edu

Abstract

Noncompliance by employees with Information Systems security policies is a serious computer security threat. An employee's extensive knowledge of the information systems, the access credentials they have been given, and the trust accorded them by their employers make them a potentially dangerous threat to computer security. The importance of this phenomenon has led to a number of research undertakings on the 'insider threat.' However, research on employee compliance with IS security policies has focused mainly on the role of extrinsic motivation. Few studies have focused on the role of intrinsic motivation. This study fills this gap by building a theoretical model using a grounded theory methodology. Concepts from High Performance Work Systems (HPWS) theory were used to develop the initial questions for structured interviews. This theoretical model provides a framework for how organizations can intrinsically motivate their employees to comply with organizational information security policies. Organizations can intrinsically motivate their employees through a supportive organizational culture, training, and job design.

Keywords: Information security, Grounded Theory Methodology, Intrinsic Motivation, Compliance with IS Policies

Please note: A prior version of this article received the Midwest Association for Information Systems (MWAIS) 1st place Best paper award at the MWAIS 2016 conference in Milwaukee, WI. The article has been expanded and subject to a second round of peer reviews. We congratulate the authors.

1. Introduction

Information security threats come from many fronts, both external and internal. Technical and non-technical measures have been implemented by organizations to mitigate these risks (Ifinedo, 2012; Siponen, Pahnila, & Mahmood, 2007). In this study, we focus on internal security risks, specifically the behavior of the trusted user or employee of an organization. We seek to understand the initiatives by an organization that lead to improved employee compliance with information security policies. Considering the consequences of data and computer systems breaches, we develop a framework for explaining how employees can be intrinsically motivated to comply with organizational information security policies.

1.1 Information Security Policies

Users of computer information systems in any organization are familiar with policies, standards, and guideline documents. A policy describes specific rules or requirements that must be met (SANS, 2014). Organizations have a variety of these policies, usually customized to fit the particular needs of the organization.

Unfortunately, cases of intentional or unintentional employee non-compliance with information security policies have been documented, with some security experts concluding employees are the weakest link in information security defenses (Acuna, 2016; Aurigemma & Panko, 2012). Although complex viruses, worms, Trojans, rootkits, and distributed botnet attacks are mounted by criminal gangs and sometimes foreign governments, the greatest t hreat of all is the insider threat, the trusted employee (Ifinedo, 2012; Warkentin & Willison, 2009). Popular media tends to headline the exploits of hackers or crackers, however evidence suggests most information security incidents occur as a result of employees' actions (Hu, Dinev, Hart, & Cooke, 2012; Karjalainen & Siponen, 2011). It has been claimed that over half of all information systems security breaches occur because employees do not comply with information security policies (Siponen & Vance, 2010). Other reports indicate that 50% - 75% of security incidents originate within the organization, perpetrated by an employee (D'Arcy, Hovav, & Galletta, 2009). Some violations might be accidental, others might be self-benefiting but without malicious intent. Nevertheless, regardless of the motivation, the end result is the same; rules are broken, possibly causing damage, or a security risk (Guo, Yuan, Archer, & Connelly, 2011).

1.2 Conceptual background and research question

Motivational perspectives have been widely used to understand human behavior in relation to information systems use. For example, Davis, Bagozzi, and Warshaw (1992) found both intrinsic and extrinsic motivational factors to be key drivers for the adoption of technology in organizations. In their research model, perceived usefulness is given as an example of extrinsic motivation, whereas enjoyment is given as an example of intrinsic motivation (Davis, et al., 1992).

Intrinsic motivation is behavior that is driven by internal rewards. Extrinsic behavior is driven by external rewards. Intrinsic motivation refers to an individuals' engagement in a given behavior for no other reason other than their enjoyment of the process. It is the pure pleasure and satisfaction derived from a given activity (Davis et al., 1992; Venkatesh, 1999). Extrinsic motivation is behavior influenced by the value of the outcomes that are distinct from the activity itself. Such outcomes include promotions, pay raise, and improved job performance (Davis et al., 1992; Venkatesh, 1999).

Most studies on the 'insider threat' have focused on employee compliance or non-compliance with information security policies on the basis of extrinsic motivators (Guo et al., 2011). Extrinsic motivators used in these studies include perceived certainty of punishment, severity and celerity of punishment; subjective norms, cost-benefit analysis, perceived vulnerability and sanction effects. These studies have examined this phenomenon using theoretical lens that include deterrence theory (D'Arcy et al., 2009; Herath & Rao, 2009; Hu, Xu, Dinev, & Ling, 2011; Siponen & Iivari, 2006; Siponen & Vance, 2010; Straub, 1990), protection motivation theory (Herath & Rao, 2009; Siponen & Iivari, 2006) and rational choice theory (Bulgurcu, Cavusoglu, & Benbasat, 2010; Li, Zhang, & Sarathy, 2010), amongst others.

According to deterrence theory (Straub, 1990), individuals weigh the costs and benefits before engaging in criminal behavior, and choose crime if it pays. Thus if an individual comes to the conclusion that there is a high probability of being caught and the punishment is severe, then they will not engage in criminal behavior (Siponen, Pahnila, & Mahmood, 2010; Straub, 1990). Classical deterrence theory posits that certainty, se verity and celerity of punishment are factors that guide an individual's decision to commit a crime or not (Siponen et al., 2007). Celerity of punishment

refers to how fast punishment is delivered. General deterrence theory posits that the greater the certainty and severity of sanctions for a criminal act, the more individuals are deterred from the act (D'Arcy et al., 2009). General deterrence theory includes three extra factors, social disapproval, self-disapproval and impulsivity (Siponen et al., 2007).

Protection motivation theory postulates that there are three crucial components of fear appeal. These are magnitude of noxiousness of a depicted event, the probability of the events occurrence and the efficacy of a protective response (Rogers, 1975). Fear can be aroused in response to a situation that is judged threatening and thus requiring protective measures to be taken (Herath & Rao, 2009). Fear appeals have two parts; the first part contains statements articulating severity of threat and the probability of threat occurring, the second part is designed to enhance perceived efficacy by providing steps to avert the said threat and the value of averting the threat (Johnston & Warkentin, 2010). These two cognitive processes are also referred to as the threat appraisal and coping response appraisal (Herath & Rao, 2009; Pahnilaa, Siponena, & Mahmood, 2007).

Rational choice theory proposes that offenders weigh the costs and benefits of engaging in defiant behaviors before deciding to act (Li et al., 2010). Individuals are sensitive to the consequences of their behavior and make rational decisions based on a cost benefit analysis of intended behavior. The decision to act in an offending manner is a function of perceived costs and perceived benefits of the criminal behavior (Hu et al., 2011). Cost benefit analysis consists of perceived risks (detection probability, sanction severity, subjective norms and security risks) and perceived benefits (Bulgurcu et al., 2010; Li et al., 2010).

A review of literature that is based on extrinsic motivational factors has been found to be mixed or even contradictory in some instances (D'Arcy & Herath, 2011). In other efforts to understand why these extrinsic motivators are not effective, neutralization theory (Siponen & Vance, 2010) has been applied in some studies. According to Siponen and Vance (2010), neutralization positively affects intention to violate information systems security policies. Neutralization theory claims that both the law abiding and law breaking individuals all believe in the norms and values of the community in general. But the law breaking individuals engage in anti-social actions because they apply techniques of neutralization. Neutralization techniques offer the violators justification for breaking the law. In its original formulation, five techniques of neutralization were proposed: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners and appeal to higher loyalties (Sykes & Matza, 1957). Later, other techniques were added, the metaphor of the ledger and the defense of the necessity (Minor, 1981; Siponen & Vance, 2010).

As a research community, in our pursuit to understand why employees fail to comply with information security policies, we have not explicitly examined the role of intrinsic motivation. This is the gap we hope to fill by asking ourselves the following research question:

> *RQ: How can organizations help their employees to be intrinsically motivated to comply with organizational information security policies?*

The rest of the study is organized as follows. The next section describes the research methodology. This is followed by our findings, a discussion of the findings, and finally a section on the implications for research and practice.

2. Research Methodology

In this study, a grounded theory methodology (GTM) is applied. This method is applied because the generation of theory with explanatory power is a desired outcome (Birks & Mills, 2011). As depicted in Figure 1 below, the process began by identifying ideational or seed constructs, which were used to develop the initial interview questions. Data analysis proceeded from open coding (identifying categories, properties and dimensions) through selective coding (clustering around categories), to theoretical coding (K. Urquhart, 2012).

2.1 Ideational constructs

A characteristic of grounded theory is that there is no prior formulation of hypothesis or expectations by the researcher to be confirmed by the data. The goal of grounded theory is not to verify or falsify existing theory. However, a researcher cannot approach a study with an empty head, rather he or she is required to be open minded (C. Urquhart, Lehmann, & Myers, 2010). A priori specification of constructs can help guide the initial design of data collection of grounded research. It must be noted that these constructs are tentative and none is guaranteed a place in the final theory (Eisenhardt, 1989).

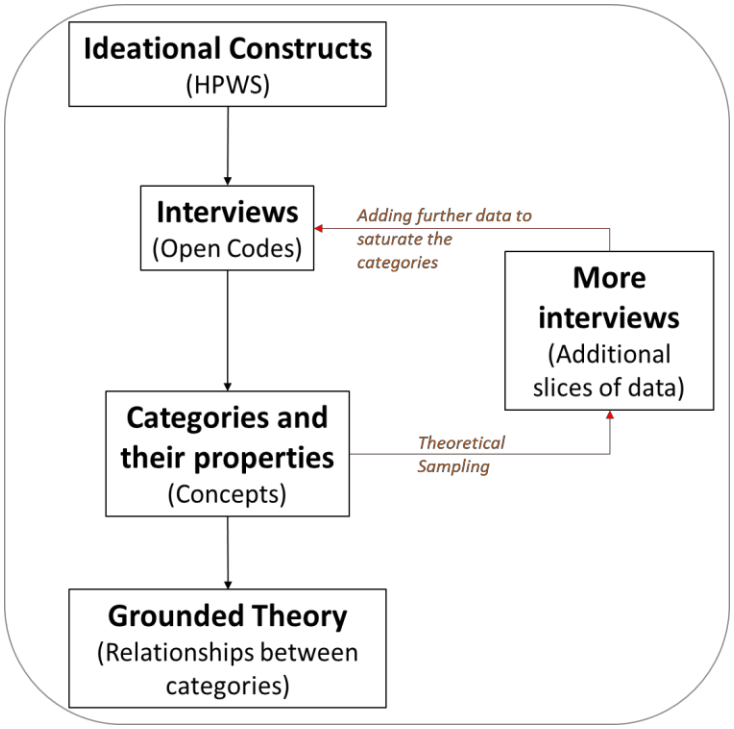

Figure 1: Cycle of Data Collection and Analysis

The seed ideas for how organizations can help their employees be intrinsically motivated to comply with information security policies came from the human resources literature. Specifically, we looked at the role of high performance work systems in motivating employees. High performance work systems (HPWS) are a set of distinct but interconnected human resource practices designed to enhance employees' skills and effort (Messersmith, Patel, & Lepak, 2011; Patel, Messersmith, & Lepak, 2013). There is no specific set of practices in the human resource (HR) literature, but traditionally it has included recruitment and selection, pay and compensation plans, information sharing, performance appraisal processes and training. These HR practices have been linked to factors such as productivity, voluntary turnover, profitability, growth, innovation, and customer service (Messersmith et al., 2011; Patel et al., 2013).

It has been found that HPWS are associated with higher levels of job satisfaction, commitment to the organization and psychological empowerment of the employees. This positive attitude has been found to be positively correlated with better organizational citizenship behavior (Messersmith et al., 2011; Patel et al., 2013). Such behavior may include compliance with organizational information security policies. The relationship between organizational HPWS and two individual-level employee attitudes, 'job satisfaction' and 'affective commitment' were found to be fully mediated by organizational level concern for employees (Takeuchi, Chen, & Lepak, 2009). HPWS have been found to facilitate a climate of concern for both employees in an enterprise and its customers which resulted in employees engaging in positive behavior towards customers and fellow employees (Chuang & Liao, 2010).

HPWS have been shown to have an effect on employee motivation. Two motivational constructs, psychological empowerment and perceived organizational support have been shown to have an impact on individual employee performance (Liao, Toya, Lepak, & Hong, 2009). Psychological empowerment refers to individuals' self -motivating mechanisms and consists of meaning, competency, self-determination and impact. Psychological empowerment reflects an individual's innate intrinsic task motivation (Liao et al., 2009).

We propose that these HPWS by an organization can lead to improved employee compliance with information systems security policies. This would be through psychological empowerment of the employees or the activation of their innate intrinsic motivation (Liao et al., 2009). Therefore, these HPWS practices were the seed ideas or ideational concepts that informed our first set of interview questions.

2.2 Interviews

Data collection was through semi-structured interviews. The interview questions were adjusted accordingly based on the feedback of initial responses during the interview as well as over the course of the data collection period. As mentioned, the initial interview questions were developed around concepts identified in the High Performance Work Systems (HPWS) (Boxall & Macky, 2009). The interviews were semi-structured and therefore new questions were asked whenever new ideas were presented by the interviewees. Additional questions were also asked to probe deeper into the responses received or to get clarification on some issues raised. This allowed us to tailor our interviews to the people and context we were in.

The purpose of this research was to understand employee compliance with information security policies in an organization. First, we were interested in understanding from the employees why they fail to comply with information security policies. And second, we wanted to understand from the employees how their employer can intrinsically motivate them to comply with information security policies.

Therefore, we identified individuals who met the basic criterion of being employed in an organization, either public or private. Towards this end, the first round of interviews was with administrative employees at a business school (7 interviews). This was followed by a second round of interviews at a private information technology company (6 interviews). All the interviewees at this technology company were with management personnel. A year later, we carried out a third round of interviews with employees working at a health center (4 interviews). The fourth round of interviews was carried out over the phone with Chief Executive Officers or Chief Information Officers of med ium sized private companies. These companies were from a variety of industries including aviation, healthcare and consumer electronics.

We carried out 23 interviews, 17 of them face to face and recorded on an audio device. The rest were carried out over the phone and notes were taken during the interview. On average, each interview lasted a little bit more than 30 minutes. In total there were 670 minutes of interview audio. The interviews were then transcribed word by word, resulting in more than 200 pages of a single spaced Word document for analysis.

2.3 Data analysis

Each interview was followed by open coding, selective coding and theoretical coding (K. Urquhart, 2012) in that order. A memo describing the core message from each interview was also written at this stage. Open coding was performed on each of these transcripts and the process repeated multiple times. The next step was selective coding.

From the open codes identified in each interview, we selected core codes. These core codes explain user compliance with information security policies. These memos on each interview transcript were followed by a search for similar themes across interviews. We began looking for themes that appeared in more than one interview. These were aggregated into categories or super-categories. At this point, we used a software tool, NVivo, to help us manage and organize the textual data.

2.4 Trustworthiness of the study

In this study, credibility was established through respondent validation. From the second round of interviews, interviewees were asked confirmation questions. This was accomplished by repeating a summarized version of their response, and then they were asked to confirm if that is the message they were communicating. Secondly, subsequent interview questions reflected the responses received in earlier interviews. This was in line with participant guidance of the interview questions.

Transferability in this study was enhanced through clear descriptions of the research methodology, peer de -briefers and an audit trail. The study also provides a systematic recording and presentation of information about the material gathered and the processes involved. A record of the research process as well as the theoretical, methodological, and analytical choices made by the researcher are provided. This is an audit trail. These measures improved the transferability of this study.

Confirmability in Grounded Theory Methodology means another researcher confirms the findings when presented with the same data. Confirmability tests the ‘objectivity’ of research. An audit trail provides the necessary materials for confirming research (Brown, Massey, Montoya-Weiss, & Burkman, 2002). In this case, confirmability in this study is reinforced by the audit trail. We provided a transparent description of the research steps taken from start to the end of the project.

3. Findings

The framework for improving employee compliance with information security policies in organizations is depicted in Figure 2. The concepts, formed from selectively coding and categorizing the open coding labels, are clustered into four main categories: organization, information technology, employee, and outcomes. The framework represents a cycle with each of the categories impacting all the other categories.

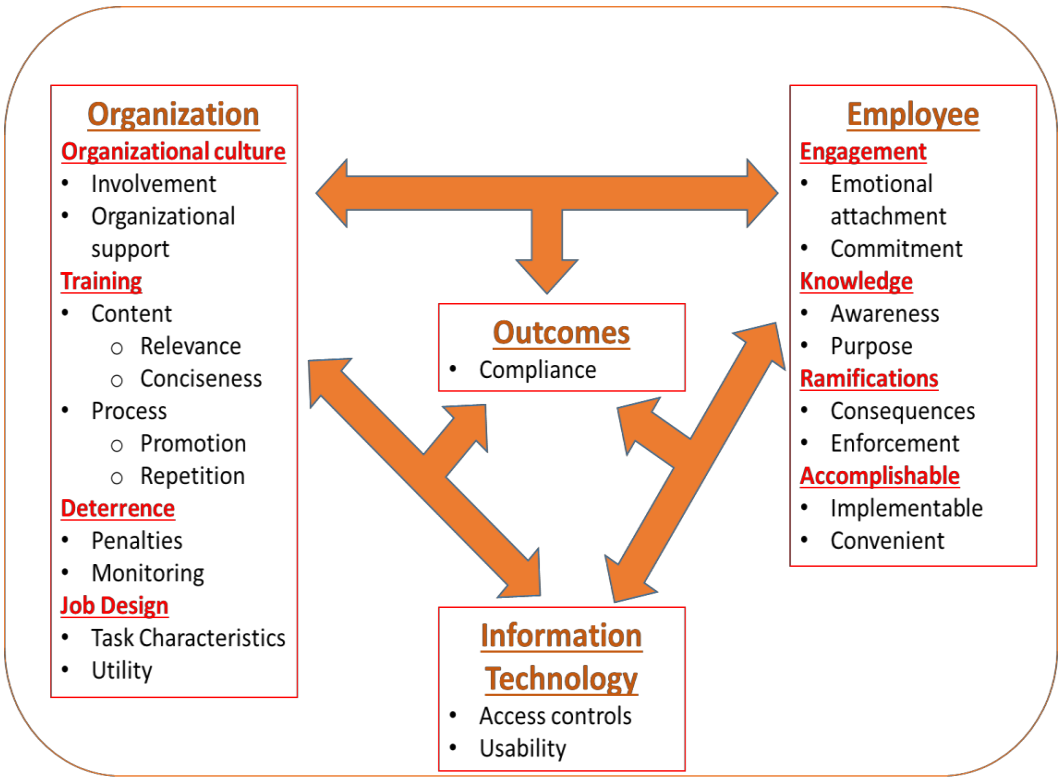

Figure 2: Framework for improving employee compliance with information security policies

The rest of the section gives a detailed description of each of these main categories and the concepts. Evidence from interview data is also provided to support each concept. For each concept, we provide description of the concept, an example interview except verbatim, and a table of open codes and sub-categories. Each of these concepts was a theme appearing multiple times in a given interview. Furthermore, the theme must have appeared in multiple interviews from more than one organization.

3.1 Organization

The category 'organization' consists of four sub-categories, organizational culture, training, deterrence and job design.

3.1.1 Organizational culture

Organizational culture emerged as a determinant of employee compliance with information security policies. Two dimensions were identified in organizational environment, employee involvement and organizational support. Employee involvement refers to employees feeling they are part of the team making decisions impacting them. They feel liberty at work. The opposite of this is feeling like they live under the law, dislike for rules, rules that are inhibiting, and excessive restrictions.

> *"But I would hope that people that are the employees that are using this information are involved in making those policies with the administration …"*

Organizational support refers to the perception by employees that the organization has in place structures to help them succeed in their job. This ranges from compensation, the work environment, in-house technical support, and the relationship with the management.

> "*The easiest way to stop that individual from doing something stupid is provide them a working environment that is comfortable, that is as stress-free as you can, while you are working and you pay them…"*

Sub-Category	**Open codes**
Involvement	▪ Negative side of policies ▪ Living under the law ▪ Dislike of rules, Inhibits ▪ Involvement ▪ Persuade ▪ Liberty at work ▪ Restrictions
Organizational support	▪ Computer Technician ▪ In-house expertise ▪ Central office ▪ Local-higher-up connection ▪ Distance ▪ In-house ▪ Internal experts ▪ In-house IT ▪ Dis-connect from central ▪ Work environment ▪ Compensation

3.1.2 Training

From the data, training is the equipping of organizational employees with skills, competencies and knowledge to comply with information security policies. Training consists of content, (relevance and conciseness) and process (promotion and repetition). The actual information security policy could be long, but for training purposes, only the important areas need to be emphasized. The content should be concise enough to allow the employee to read and comprehend all the content.

> "*Yeah it is a long paragraph; I probably don't even read all of it to be honest with you…"*

The relevance of the training is another idea that emerged. Relevance refers to both training method and content. Organizational employees have varying information technology skills and therefore training for the various employee categories should take this into consideration. Hands on training, especially from fellow employees or immediate managers is more effective for some employees.

> *"But I am sure if it had to do with policies in our department and what's relevant to us then that may make a difference"*

Publicity and refresher training are other ideas that emerged in relation to training users on compliance with information security policies.

> *"A recommendation I would say for the university and departments would be to conduct annual at least every other year just refresher training maybe a 15 minute online course"*

Regular reminders of compliance with information security policies are perceived as helpful. Scaled down refresher training covering old material and any new materials are also seen as important.

> *"Actually send out emails every so often saying "this is a reminder"*

	Sub-Category	**Open codes**
Content	Relevance	▪ IT skills level ▪ Hands on training
	Conciseness	▪ Bullet point ▪ Emphasize ▪ Ranking ▪ Apathy
Process	Promotion	▪ Publicity ▪ In your face ▪ Verbal communication ▪ Reminders
	Repetition	▪ Once a year ▪ Repetition ▪ Refresher course ▪ Yearly ▪ Training period

3.1.3 Deterrence

Deterrence refers to measures that discourage non-compliance behaviors which are clearly articulated in the information security policy. These include monitoring and penalties. Monitoring is the employee awareness that management and information technology staff are watching or keeping an eye how the information technology resources are being used. It is the awareness that one of the ramifications of not complying with information security policies is that the authorities will find out. This could be the websites that an employee visits.

> "*They probably, they might flag it, I am sure they can track the faculty and staff and what we do by our IP address but it is not blocked….*"

Penalties refers to what will happen to the employee should they not comply with information security policies. This might include breaking State and/or Federal laws and thus the possibility of facing the criminal justice system. Penalties also include the possibility of losing one's job or paying fines.

> *"Well I think certainly when you hear about somebody who flagrantly violated the policy and she got sent to jail I mean certainly if you are doing something similar, you would think twice about continuing that practice because you will get caught."*

3.1.4 Job design

Job design refers to the putting together of tasks or elements to form a job. These include what tasks are done; when and how the tasks are done; how many tasks are done; in what order the tasks are done; factors which affect the work and the organization of the content and tasks. It is easier to comply with IT policies if they are in-built in the work process. For example, employees are required to destroy social security numbers as part of their work. If this was part of an IT policy, then compliance would almost be guaranteed. It clarifies what tasks are done, when and how the tasks are done. For example, the interaction between a nurse, patient and the information technology (computer hardware and software applications) is clearly stated step-by-step. Job design is seen as the acceptable task characteristics and utility of the procedures and limitations imposed by the systems. Procedure in this case refers to who, what, where, when and why a job is done in a given way. Some of the words and phrases used to describe procedure include protocol, accounting rules, departmental login process etc.

Sub-Category	Open codes
Monitoring	▪ Flag it ▪ IP address ▪ Monitor ▪ Open access ▪ Filters ▪ Monitoring
Penalties	▪ Federal law ▪ State law ▪ Monetary fines

"…we have to sign into so we have certain rules associated with passing passwords around like FTD passwords and things like that. Instead of just emailing those we have certain protocol that we use for managing passwords…"

Utility refers to the convenience, enabling, unobtrusive information security policies. Being required to change one's password too often is seen as inconvenient, for example. Or in some cases having information security policies that are too restrictive slows down the pace at which a job is done. Or information security policies are sometimes perceived as a hurdle as they go about their day to day business.

"I would say doing everything you can to not make the security policies and practices a hurdle for someone to get over to do their business on a day to day basis. Be as unobtrusive as possible,"

Sub-Category	Open codes
Task characteristics	▪ Protocol ▪ VPN policies ▪ Social Security numbers ▪ Accounting rules ▪ Departmental logins
Utility	▪ Convenience ▪ Inhibitor ▪ Unobtrusive ▪ Security vs. performance

3.2 Employee

This study specifically looked at cognitive factors with regard to the individual employee. The category 'employee' consists of engagement, knowledge, ramifications, and accomplishable.

3.2.1 Engagement

Engagement has two components, emotional attachment and commitment. Employees who demonstrate engagement comply with the information security policies with a passion and understand how important their behavior is to the organization. They feel a strong emotional bond to the organization and demonstrate a willingness to encourage fellow employees to comply with the information security policies.

"Most of my training was hands on so like I said Julie is very hands-on she helped us and there are documents that we have like for example,"

"I don't know if it is the determining factor for somebody doing whatever they want to do. It is just like the secret service, they know they are not supposed to do these things, but that is not going to stop them from doing them. That individual has to consciously say, I am not going to do these things. Most people are not going to things because a piece of paper told them, it still comes down to the person and their willingness to follow the rules to a t. I still come down to the person…."

3.2.2 Knowledge

Knowledge is defined as the employees' awareness and understanding of information security policies and why it is important to have these guidelines in place. Knowledge refers to an awareness of what is wrong or right. The familiarity, awareness, knowledge of formal or written down policies is not emphasized, but rather a general awareness of IT policy. The employees understand the purpose of the information security policy willing to comply with it. In a way, they are persuaded they understand it. Knowledge can be internalized to the point of being perceived

Sub-Category	**Open codes**
Emotional attachment	▪ Individual fulfillment ▪ Persuaded ▪ Inhibits ▪ Involvement
Commitment	▪ Quality of employees ▪ Living under the law ▪ Restrictions ▪ Responsible

as obvious for example, or seen as common sense, or as a rule of thumb.

> *"The general use policy is pretty much common sense and for me the only reason to have this policy is for legal ramifications…"*

> *"I think the rules that have specific purposes are far as protecting us our protecting our clients, rules that in the long run ensure that we are safe as a business and can keep doing business without fear of legal entanglements or anything like that I think is very important."*

Sub-Category	**Open codes**
Awareness	▪ Obvious ▪ Basic ▪ Common sense ▪ Rule of thumb
Purpose	▪ Protection ▪ Continue functioning ▪ Guideline ▪ Accountability ▪ Legal reasons ▪ Safety ▪ Orderliness

3.2.3 Ramifications

Ramification here is defined as what the employee perceives as the consequences for non-compliance and their skill ability to comply with the information security policies. Ramifications refer to the most likely outcome or consequence for not complying with the information security policy. It is the knowledge that both monitoring and penalties are actually enforced. Awareness that employees have been fired, fined or jailed for not complying with information security policies is a strong deterrent.

> *"I heard of incidents at the university where they terminated people because things they found on their machine…"*

3.2.4 Accomplishable

Accomplishable refers to a policy that is realizable, achievable, doable or manageable. The employees have the ability to actually comply with the information security policy. The information security policy makes sense to the employees and they can actually implement it. The information security policy is well defined so that the employees can act on it.

Sub-Category	**Open codes**
Consequences	▪ Ramifications ▪ Liability ▪ Consequences
Enforcement	▪ Enforcement ▪ Terminated people ▪ Arrested ▪ Sent to jail

"I think the policy has to make sense. It needs to be understandable. You need to be able to act on that policy and actually implement it."

"Yes, to a varying level. I think the rules need to be easy to follow. I think they need to make business sense…"

Sub-Category	**Open codes**
Implementable	▪ Business sense ▪ Credibility ▪ Implementable ▪ Able to act on them ▪ Complexity ▪ Disconnect
Convenient	▪ Convenience ▪ Extra work ▪ Increasing complexity

3.3 Information technology

Information technology is the application of hardware (computers, network devices, printers, etc.) and software (operating systems, communication software, application software etc.) to store, retrieve, transmit and manipulate data, often in the context of a business or an enterprise. Information technology consists of access controls and usability of the compliance process.

Access controls refer to the use of information technology (both hardware and software) to enforce the content in the security policies. For example, all interviewees mentioned that their organizations had password policies in place specifying the frequency of changing one's password, the length of each password, the mix of characters to use, etc. This policy was enforced by reminding users when a new password was due, and only accepting new passwords in compliance with the password policy. Another example is accessing information through very specific systems. Role based access control refers to restrictions in place to control who, when, and where data can be accessed and a record of the transactions being kept. They have data drives that can only be accessed by certain authorized individuals with the right log-in credentials.

"happen but most is driven through technology in the sense of our computers are all set up in the network so that we have to log-in to the computers, we have encryption on all of our machines, like full-desk encryption. So we have to log in to our machines and apply the pass code to open the encryption process so then our exchange account is

available through this building and outside of this building in VPNs for our department network that we have to sign into…"

3.4 Compliance with IS Policies

Compliance with the information security policies suggests that policies should be efficient, easy to learn and satisfying to use by the employees. Information technology that is usable is consistent across time and applications, instant access to needed information, meaningful error messages, not overwhelming, minimizing memorizing requirements, controllable, and empowering the employee.

Sub-Category	Open codes
Access controls	▪ SIS Access ▪ Technology driven ▪ Encryption ▪ Segmented ▪ Password system ▪ Double login ▪ Pass code ▪ Central control ▪ Data drives ▪ Software design
Usability	▪ Sensible ▪ Well defined ▪ Clarity

4. Discussion

The primary goal of this study was to understand how organizations can intrinsically motivate their employees to comply with information security policies. Although our data analysis shows that employees need both intrinsic and extrinsic motivation to improve their compliance, the discussion here is limited to intrinsic motivation. Deterrence and ramification categories are excluded from this discussion because they are extrinsic motivators.

Our study found three intrinsic motivation categories. These are employee engagement, knowledge, and employee perception that a task can be accomplished. These three sources of intrinsic motivation are influenced by three organizational practices, organizational culture, training, and job design, respectively. We explain further using three propositions below.

4.1 Proposition # 1

Organizational culture will have a positive impact on the individual employees' engagement in the organization.

There are many definitions, conceptualizations and dimensions of culture (Leidner & Kayworth, 2006), but our interest here is in organizational culture. Some of the value dimensions of organizational culture include solidarity, mission, involvement, sociability, people-orientation, constructive, supportiveness, employee orientation, task-orientation, concern for production, innovation, results orientation, job orientation, passivity, aggression, consistency, adaptability, bureaucracy, process, normative values, markets, clans, parochial values, and pragmatism (Leidner & Kayworth, 2006).

Of the above value dimensions, involvement, supportiveness, people-orientation, concern for people, and solidarity are similar to the findings from the analysis of the interview data in this study. Involvement is the sense of control among a firm's members (Denison & Mishra, 1995). Supportiveness, people-orientation and concern for people refer fairness, collaboration, trust and concern for people issues. Solidarity is the degree to which organizations members

work together to realize common objectives efficiently regardless of personal ties (Hoffman & Klepper, 2000; Leidner & Kayworth, 2006)

Research shows that organizations that are high in solidarity culture experienced more favorable outcomes when adopting technology (Leidner & Kayworth, 2006). Another study showed that people-oriented cultures tended to experience greater implementation success in information technology use and outcomes (Harper & Utley, 2001).

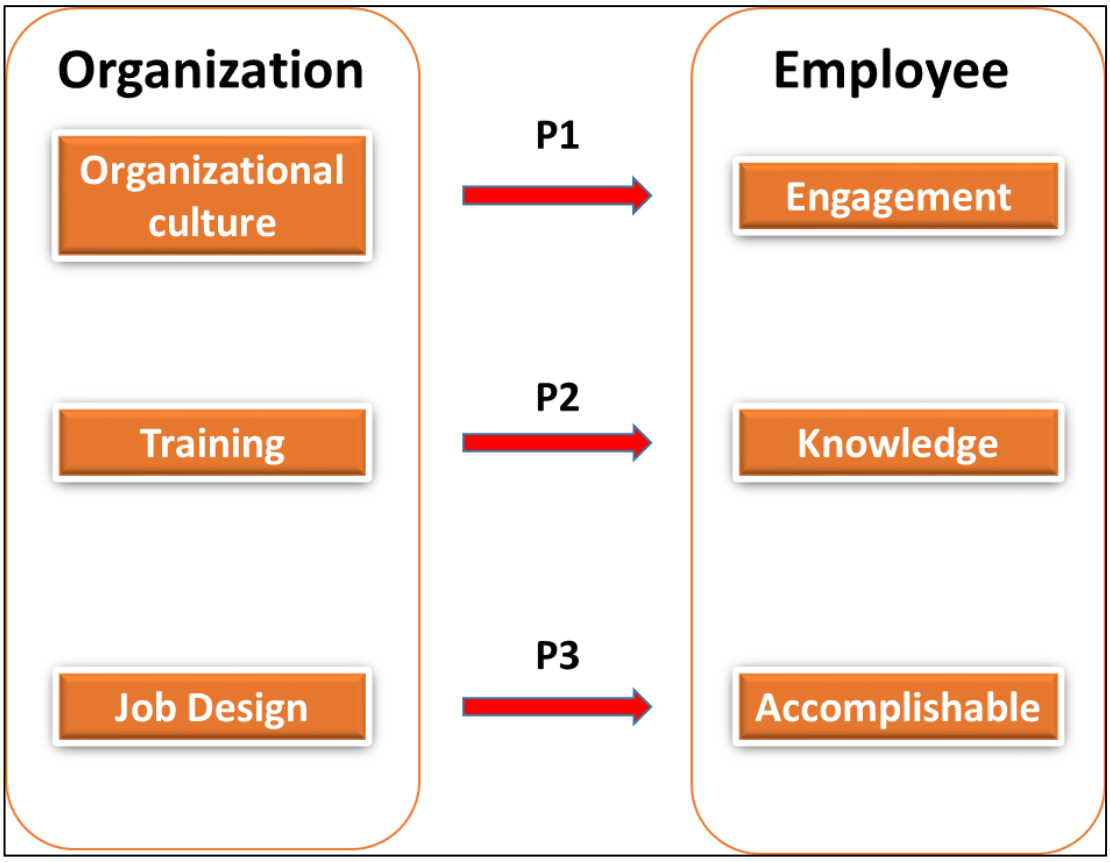

Figure 3. Model for intrinsically motivating employees to comply with IS Policies

4.2 Proposition #2

Employees' awareness of information security policies and their purpose is an outcome of appropriate training.

Training is one of the most commonly suggested methods for employee compliance with information security policies (Sagers & Hosack, 2015). Previous information security compliance approaches include psychological training approaches; training approaches based on learning theories; security awareness program approaches; process approaches; situational approaches; social engineering preventive approach and computer based training approaches (Karjalainen & Siponen, 2011).

In one of the seminal studies on information systems security policy training (Puhakainen & Siponen, 2010), two theories were applied. From psychology, elaboration likelihood model (ELM) was used, and from the learning theories, Universal Constructive Instructional Theory (UCIT) was used. In their study, Puhakainen and Siponen (2010) identified nine key ways information security policy compliance training can be effective. Five of these key findings, listed below match with the findings in this study.

i. Use of methods enabling learner's systematic cognitive processing of information.
ii. Use of learning tasks that are of personal relevance to the learners.

iii. Take into account the learners previous knowledge of information systems security policies compliance.
iv. Integrate training with normal business communication in the organization.
v. Make information security communication a continuous activity rather than limiting it to a single occasion.

Training content should be relevant and concise, and the training process should include promotion activities and repetition. This will have a direct impact on employee knowledge. Similar to culture above, the definition of knowledge has been debated since the Greek era (Alavi & Leidner, 2001). However, Alavi and Leidner identified three major points on knowledge.

i. There is a difference between data, information and knowledge.
ii. Knowledge is personalized, and in order for it to be useful to others, it must be expressed in such a manner as to be interpretable by receivers.
iii. Hoards of information are of little value; only that information which is actively processed in the mind of an individual through a process of reflection, enlightenment, or learning can be useful.

These three points are aligned with the findings of this study, which is that appropriate training by the organization will have an effect on the employee knowledge. Knowledge consists of awareness and purpose of the information security policies. In this case, awareness refers to information that has been processed in the mind of the employee. This will lead to improved employee compliance with information security policies.

The findings in this study are also in line with the findings of a quantitative-positivist study (Bulgurcu et al., 2010) that incorporated an information security awareness concept in their model. They argue that knowledge influences persuasion which in turn influences decision. Therefore, they hypothesized that information security awareness positively affects attitude which in turn positively affects intention to comply. In their study, this hypothesis was supported.

4.3 Proposition #3

Employee perception of implementation and convenience of information system security policies is an outcome of job design.

Task Technology fit theory posits that information technology is more likely to have a positive impact on individual performance and be utilized if there is a fit between task characteristics and technology characteristics (Goodhue & Thompson, 1995). Therefore the perception by employees on their ability to conveniently comply with the information security policies is greatly influenced by their job design.

4.4 Contributions to research

Senior scholars in management information systems have called for a 'good theory' (Watson, 2001) in information systems and the development of our 'own' theory (Weber, 2003). Over the years, the information systems discipline has borrowed a variety of theoretical lenses to explain phenomena in information systems research (Watson, 2001). Heeding this call, this study developed the basis for a theory of intrinsically motivating employees to comply with information security policies.

4.5 Implications for practice

This research suggests that organizations can improve employee compliance with information security policies through creation of an enabling organizational culture, effective training, and design of job processes that match the security policy requirements. Organizations should involve employees in the policy creation process and provide support in a number of ways. One of these could be senior leadership leading by example. Training should be relevant and concise. Management should send out regular reminders and have refresher training repeated annually. Lastly, the work expectations should be aligned with security policies. Policies should **not** be seen as inconvenient, intrusive, and harming performance.

4.6 Limitations, future research, and conclusions

We note two limitation to this study. Although a number of steps were taken to improve the trustworthiness of the study, the credibility could have been improved through triangulation of data. Instead of relying on data collected through semi-structured interviews only, use of data from organizational documents would have raised the trustworthiness of the findings. The lack of document data was not for lack of trying but rather reluctance of management in many organizations to open up internal communications to people from outside. Second, while the sample size is somewhat small, the amount of data collected and its richness is significant. As such, we believe future studies will validate our findings.

There are four major directions we see future follow-up research taking. The improvement of the theory presented in this study by including document data in further analysis; development of a measurement model; stratification of compliance along management levels; and determining the role of national culture in employee compliance with information security policies. Further, the incongruity of job and policy require more study. Like previous studies, we start with the notion that the policy with which to comply is correct and perfect. That is likely not the case.

To conclude, the purpose of this study was to have a better understanding of the cognitive factors that influence employee compliance with information security policies. Towards this goal, we have presented a theoretical framework that hopefully makes a contribution towards our collective understanding of this phenomenon.

References

Acuna, D. (2016). Enterprise Computer Security: A Literature Review. *Journal of the Midwest Association for Information Systems, 2016*(1), 37 - 53.

Alavi, M., & Leidner, D. E. (2001). Review: knowledge management and knowledge management systems: conceptual foundations and research issues. *MIS Quarterly, 25*(1), 107-136.

Aurigemma, S., & Panko, R. (2012). *A composite framework for behavioral compliance with information security policies.* Paper presented at the 45th Hawaii International Conference on Systems Sciences, Hawaii.

Birks, M., & Mills, J. (2011). *Grounded Theory: A practical guide*. Thousand Oaks, California: Sage.

Boxall, P., & Macky, K. (2009). Research and Theory on High-Performance Work Systems: Progressing the High Involvement Stream. *Human Resource Management Journal, 19*(1), 3 - 23.

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems, 11*(4), 283-295.

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-A527.

Chuang, C.-H., & Liao, H. (2010). Strategic Human Resource Management in Service Context: Taking Care of Business by Taking Care of Employees and Customers. *Personnel Psychology, 63*(1), 153 - 196.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658. doi:10.1057/ejis.2011.23

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.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and Intrinsic Motivation to Use Computers in the Workplace. *Journal of Applied Social Psychology, 22*(14), 1111 - 1132.

Denison, D. R., & Mishra, A. K. (1995). Toward a Theory of Organizational Culture and Effectiveness. *Organization Science, 6*(2), 204 - 223.

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

Goodhue, D. L., & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly, 19*(2), 213 - 236.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

Harper, G. R., & Utley, D. R. (2001). Organizational Culture and Successful Information Technology Implementation. *Engineering Management Journal, 13*(2), 11 - 15.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Hoffman, N., & Klepper, R. (2000). Assimilating New Technologies: The Role of Organizational Culture. *Information Systems Management, 17*(3), 36 - 42.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top management and Organizational Culture. *Decision Sciences Journal, 43*(4), 615 - 659.

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.

Ifinedo, P. (2012). Understanding information security systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory. *Computers & Security, 31*, 83 - 85.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-A544.

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.

Leidner, D. E., & 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.

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. doi:10.1016/j.dss.2009.12.005

Liao, H., Toya, K., Lepak, D. P., & Hong, Y. (2009). Do They See Eye to Eye? Management and Employee Perspectives of High-Perfomance Work Systems and Influence Processes on Service Quality. *Journal of Applied Psychology, 94*(2), 371 - 391.

Messersmith, J. G., Patel, P. C., & Lepak, D. P. (2011). Unlocking the Black Box: Exploring the Link Between HighPerformance Work Systems and Performance. *Journal of Applied Psychology, 96*(6), 1105 - 1118.

Minor, W. W. (1981). Techniques of Neutralization: a Reconceptualization and Empirical Examination. *Journal of Research in Crime and Delinquency, 18*(2), 295-318. doi:10.1177/002242788101800206

Pahnilaa, S., Siponena, M., & Mahmood, A. (2007). *Employees' Behavior towards IS Secur ity Policy Compliance.* Paper presented at the Proceedings of the 40th Hawaii International Conference on System Sciences, Hawaii.

Patel, P. C., Messersmith, J. G., & Lepak, D. P. (2013). Walking the Tightrope: An Assessment of the Relationship Between High-Performance Work Systems and Organizational Ambidexterity. *Academy of Management Journal, 56*(5), 1420 - 1442.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 767-A764.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology, 91*(1), 93.

Sagers, G., & Hosack, B. (2015). Personal Computing Security Fundamentals. *Journal of the Midwest Association for Information Systems, 2015*(2), 15 - 30.

SANS. (2014). Information Security Policy Templates. Retrieved from http://www.sans.org/security-resources/policies/ Siponen, M., & Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Siponen, M., Pahnila, S., & Mahmood, A. (Eds.). (2007). *Employee's Adherence to Information Security Policies: An Empirical Study* (Vol. 232). Boston: Springer.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *IEEE Computer*, 64 - 71.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Informaton Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-A412.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255 - 276.

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22*(6), 664-670.

Takeuchi, R., Chen, G., & Lepak, D. P. (2009). Through the Looking Glass of a Social System: Cross-Level Effects of High-Performance Work Systems on Employees' Attitudes. *Personnel Psychology, 62*(1), 1 - 29.

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'Theory' Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems. *Information Systems Journal, 20*, 357 - 381.

Urquhart, K. (2012). *Grounded Theory for Qualitative Research: A Practical Guide.*

Venkatesh, V. (1999). Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation. *MIS Quarterly, 23*(2), 239 - 260.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105. doi:10.1057/ejis.2009.12

Watson, R. (2001). Research in Information Systems: What We Haven't Learned. *MIS Quarterly, 25*, vii - viii.

Weber, R. (2003). Still Desperately Seeking the IT Artifact. *MIS Quarterly,* 27(2), iii-xi.

Author Biographies

David Sikolia is an assistant professor at Illinois State University, teaching programming and security courses. His research interests include information assurance and security and the use of Grounded Theory Methodology. He received his Ph.D. from Oklahoma State University.

David Biros is an associate professor at Oklahoma State University. He received his PhD from Florida State University. He is a Retired Air Force Lt Col with a background in information technology and security. He has published in MIS Quarterly, Decision Support Systems and many other journals and conference proceedings. He is actively involved in student recruitment efforts.

Page intentionally left blank