IT Security Policies and Employee Compliance: The Effects of Organizational Environment

Kendal Stephens LaFleur, Narasimha Shashidhar
Department of Computer Science
Sam Houston State University
Huntsville, TX
{kks016, karpoor}@shsu.edu

*Abstract***— A major threat to IT security in today’s business world is the simple problem of careless employees choosing not to comply with security policies and guidelines. Many studies have been done to track the reasoning behind this problem and try to find a solution. To address this issue, our study proposes to look at the effects of company culture and environment, including relationships among co-workers as well as their feelings toward upper management, in order to determine if a correlation exists between this relationship and an employee’s compliance with IT security policies. In order to do so, we designed a survey comprised of various questions dealing with workplace environment and thoughts on IT security policies in order to gain insight on the topic and gather useful data. We administered the survey to an anonymous group of people we assembled, ranging in age and employed by a variety of companies. The survey results were then analyzed and data trends were uncovered in order to see if a correlation does in fact exist. We found that there is a positive correlation between employees’ organizational environment and their compliance with IT security policies. We also discovered that there appears to be a lack of employee education on security policies in the workplace, which needs to be studied further in the future. To the best of our knowledge, our method is unique and stands apart from prior work in that the data gathered was not limited to employees from a specific company or of equal job status. We believe that the wide variety of our chosen participants will provide a more comprehensive look at this issue. Additionally, our study does not focus on any specific behavioral theories or try to implement any new methods in the workplace as was done earlier. We merely look at the employees’ daily, ordinary feelings and actions, giving a special “real” and “true” quality to our results.**

Keywords—policy; compliance; security; education

I. Introduction

Now more than ever, IT security issues pose a major threat to companies everywhere. Security breaches, computer infections, system failures, and data loss are all serious dangers. One way to help combat these risks is by implementing IT security policies, which provide employees with a set of rules and guidelines to follow to help lessen the likelihood of security issues. A major problem, however, involves employees choosing not to comply with all of these policies, which puts the organization at risk. Our study explores a possible connection between the level of employee compliance with IT security policy and the state of their organizational environment. We gather data from employees at various jobs in several companies in order to gain insight on this correlation, studying how they function in their ordinary workplace. Our method enables one to take a look at the daily life of employees, without altering anything about the way the workplace normally operates. Using this approach rather than studying behavioral methods and then implementing those in the workplace makes our study unique and provides us with useful results distinctive from the findings of prior studies.

II. Literature review

A great number of studies have been done in the area of employee compliance with security policy. It has been shown that many IT issues and security breaches are merely the result of an employee failing to adhere to the company’s rules and procedures, which indicate that these should be easily preventable. This leads researchers to question what exactly influences this type of employee behavior and what could be done to increase compliance with IT security policies and suggested guidelines.

Many of the prior research studies focus on trying to implement different behavioral methods to control the behavior of employees. Tyler’s [5] study uses a command-and-control model where managers implement sanctions and punish undesired behavior. While this can provide useful insights, it does not uncover how employees’ behavior is impacted on a normal daily basis. We believe that it would be more beneficial to study the current company culture, relationships among employees, and other factors of this type that affect their behavior, rather than having managers make sudden changes and test different theories that are not part of the usual workplace. Forgas et al. [13] conducted a study focusing on the Affect Infusion Model to delve into experimental social psychology and organizational behavior to determine the influence that affective states have on decision making and behavior in organizations. Dillon et al. [2] analyzed how different behavioral models affect the ways that employees accept new technologies and the consequences of those innovations. Our study will differ from these earlier studies in the way that it gathers data by having participants answer questions about their daily routine workplace, not about the effects of some foreign new behavioral method.

Vroom et al. [6] studied the human factor in IT security from many different angles. *Organizational culture* is defined and explained so that its meaning is clearly understood, and conclusions are drawn that the culture of an organization could have a huge impact on the security of information, either in a negative or a positive way. The subject of organizational behavior is then discussed, showing how it affects the actions of employees. Final conclusions state that it will be beneficial to study a combination of both organizational culture and behavior in order to determine a way to successfully change an organization's culture one portion at a time. This perspective is interesting, as the researchers look at how various characteristics of the organization come into play with employee behavior and compliance with policy, and then conclude that they should be changed a small bit at a time to eventually get the organization where it needs to be. This approach seems more practical and beneficial than using a specific behavioral theory to completely change the way the workplace operates and then recording the results of that experiment. Our study approach will build on this paradigm, observing how the workplace functions on a daily basis rather than examining how it changes with the different methods being implemented.

Chan et al. [1] showed that information security is a very complex matter and its study should incorporate not only technical factors, but also social factors as well. They introduce a concept called *organizational climate*, which they distinguish from organizational culture since it refers to the way employees view both formal and informal policies, procedures, and practices of an organization. The study uses organizational climate to provide researchers with some insight on the more subtle, less apparent aspects of an organization's culture. They show that emerging evidence exists to show that specific climates are predictive of specific outcomes. For example, employees in a workplace with a strong safety climate seemed to comply with more safety guidelines. They claim that this is important because safety programs and information security programs share many characteristics and are both critical components of an organization. The authors then discuss how organizational climate can be influenced by socialization with coworkers and peers, and by practices of supervisors and upper management. This is definitely an important observation; however, this article fails to explore it further and see how these relationships actually affect the climate and the behavior of employees. One primary goal of our research study is to look into this further and see what connections might be uncovered in order to fill this gap. We like to stress that our study is the first of its kind, to the best of our knowledge, to undertake this approach on examining this correlation.

A study done by Herath et al. [3] brings up organizational commitment and how it has influenced organizational behavior literature. They define *organizational commitment* as an individual's feelings of dedication and contribution to their work organization. The study discusses how an employee's commitment to an organization is likely to play a role in his or her engagement in security behaviors. The conclusion that is drawn is that the strength of employees' organizational commitment will positively affect their intentions to follow policies in the workplace. But does an employee's *intention* to follow a policy mean that they actually do it? We believe that this is a fundamental weakness in this work. Although they present several interesting ideas revolving around organizational commitment, it still remains uncertain as to how this directly affects an employee's real actions. There are several questions that remain unanswered - Just because an employee thinks that something is the right choice, or feels more obligated to do a certain thing, does that mean that they actually follow through and do that? We examine this question further. In contrast to this study and many others, our study will focus on actual employee actions, and not just what they are "likely" to do because of feelings of obligation.

Pahnila et al. [4] conducted a study of employee behavior towards IS security policy compliance in which they suggest that the behavior of employees is generated by the way that they interact with each other and prove that this is true through data collection. This is an important deduction and raises the following questions in this area. Does positive interaction between employees increase their compliance with security policies? Does interaction between an employee and their supervisor or top management members have a greater or lesser effect on compliance than their interaction with same-level co-workers? We aim to address these questions in this study.

While prior work is extensive in this area, we have chosen to survey only the most directly relevant work and it is not to be treated as an exhaustive survey. We found many informative and significant pieces of research regarding employees' compliance with IT-related security policies. However, we believe that there are still many avenues and ideas that need to be explored. Our study aims to provide a closer insight on what exactly affects an employee's compliance with security policies in their typical workplace by examining organizational culture and climate as well as the interactions among different co-workers. The ultimate goal is to determine if and how these factors positively impact an employee's adherence to security policies. Our study departs from earlier work by not looking only at the "intentions" to comply with policies and also by not implementing different behavioral models to try and alter employees' behavior.

III. Main Research

A. *Methodology*

The reasoning behind our theory about employees' compliance with security policies being related to their work environment is well justified. A great deal of scientific research has been done in the area of employee compliance with rules and different behavioral influences. For instance, Tyler [5] discusses some of these behavioral theories including the "command-and-control model" and the "self-regulatory model." The first of these models looks at how employee behavior is controlled by managers or bosses and the way they punish undesired behavior. The latter looks at how the ethical values of employees motivate them to follow rules. A study done by Cardona et al. [12] discusses how the social exchange relationship between employees and their organization affects their attitude and feelings. The more positive they view the relationship, the more connected they feel to the organization, leading to increased feelings of obligation and commitment. This leads us to question if this increased commitment holds true in the area of IT security policies, and if these positive feelings affect employees' compliance with them. Although studies such as this one give the impression that such a connection exists, there is no definite evidence. We wanted to look deeper into assessments of employee behavior and relationships and see how compliance with IT security policies is connected.

We were motivated to study this topic because of the increasing importance of IT security policies in the workplace, and issues with non-compliance. Employees failing to follow IT policies can lead to major consequences for a company, such as data breaches, viruses and infections, unauthorized access to information, and many other issues. Because of the serious impact of these threats, we felt the need to study what might affect compliance with policies. Our goal was to establish conclusions that could be studied further and could be used as valuable information by employers to help increase employee compliance with IT security policies in the workplace. In the recent years, organizational culture and environment have become increasingly popular topics, with many companies striving to promote a friendly and caring atmosphere while providing great amenities for employees, and with national awards being given for "Great Place to Work" and "Best Corporate Culture." This led us to ask questions about the possible correlation between organizational environment and employee compliance with security policies. Could these two things be connected? We began to think about the different types of relationships and interactions among people in the workplace and explored possible links between employee behavior and following rules and policies.

Psychological studies have been criticized for focusing only on the negatives of situations and not the positives. In a study on organizational behavior, it has been shown that studies in psychology, as well as in business and management, need to use a more positive approach [8]. Thus, our motivation in this study is to place emphasis on a positive correlation, rather than a negative one. We chose to differ from the norm by not looking at how negative work relationships impact non-compliance with policies, but rather focus on how positive relationships increase compliance with policies.

A study conducted by Bishop et al. [7] looks at how commitment to an organization and commitment within work teams leads to desired employee outcomes. We used this idea of positive commitment leading to positive job performance in developing our theory. If an employee is committed to their organization and holds themselves and their workplace to high standards, then will this positively influence whether or not they follow policies? This is one of the many questions we aim to answer in this study. We show that our theory is rational and in the next section outline how we collect the requisite data to substantiate our claim.

B. *Beginning Processes*

First, we designed a survey consisting of eleven multiple-choice questions relating to employees' feelings towards co-workers and management, as well as their thoughts on IT security policies in the workplace. This online survey was then sent out to 40 individuals for completion. Participants were told to be as candid and honest as possible and all results were to remain anonymous. The participants ranged in age from 22-55 and included both men and women, providing us with a good amount of variation. A study by Morris et al. [11] found that age can play a part in perceptions of technology and its use in the workplace, so we chose to use participants with a fairly large age deviation in order to get accurate results from the general working population, and not narrow it down to the outlooks of one specific group. Also, participants were all employed by a variety of different companies. For example, one participant was an elementary school teacher, one worked for a large accounting firm, and one was a field supervisor for an oil and gas company. A great amount of diversity was present in this group of people surveyed. We wanted to test our hypothesis in a wide variety of work settings and not limit it to one specific company or type of employee.

C. *Study Details*

A critical component of our research method was determining the specific questions to be included in the survey. One important goal was to keep the number of questions below 15 so that participants would not get bored, which might drive them to answer quickly and carelessly in an attempt to finish. We also required the questions to provide us with insight on how employees get along with others in the workplace, how they feel about IT security policies, and what possible associations might exist between these two areas. We created multiple questions revolving around these subjects. The survey was led by the following question:

> *How informed are you of your workplace's IT security policies (computer passwords, data protection, web monitoring, rules and legal issues, etc.)?*
>
> a. *Very well informed*
> b. *Well informed, familiar with most policies*
> c. *Partly informed, not familiar with numerous policies*
> d. *Not informed at all*

Since the survey participants had no idea beforehand what the survey would be concerning, this question was asked first in order to get them thinking about IT security policies and enable us to gauge how well-educated they were on the subject. Questions were also asked concerning their relationships with others in the workplace. Here are examples of two such questions: *How would you describe the company culture/environment in your workplace? How would you describe your relationship with top management and bosses at your workplace?* The goal was to get an idea of participants' feelings on both topics of workplace relationships and IT security policies, design questions combining the two ideas.

> *Would you be more likely to violate an IT security policy if the reasoning was to help out a co-worker you're friends with?*
>
> *a. Definitely*
> *b. Maybe*
> *c. Not sure*
> *d. No*

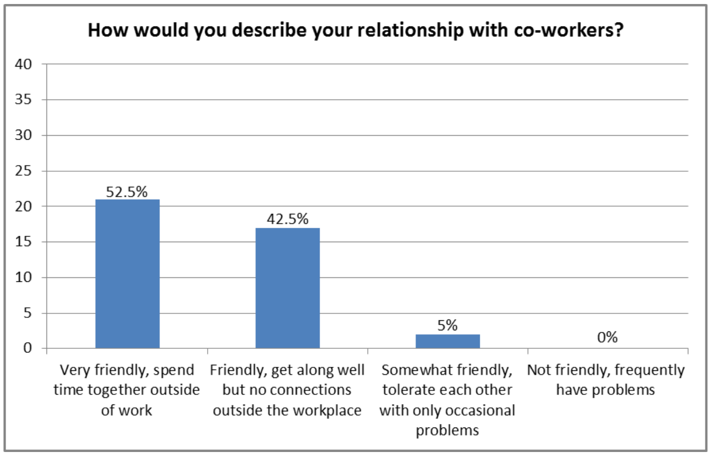
Responses to a question like this provide us with concrete answers as to how positive work relationships impact compliance with security policies. While our theory is that this correlation is positive, it also seems plausible that it might be just the opposite. Employees might be more willing to violate a policy if doing so would help out a fellow employee they're friends with, and they feel a higher obligation to that friendship than to the company. Prior studies done by Truckenboldt [9] and by Wayne et al. [10] examine this concept, looking more closely at different levels of employee commitment and social exchanges. We asked questions like the one above in order to test out multiple possibilities and look at the theory from all perspectives.

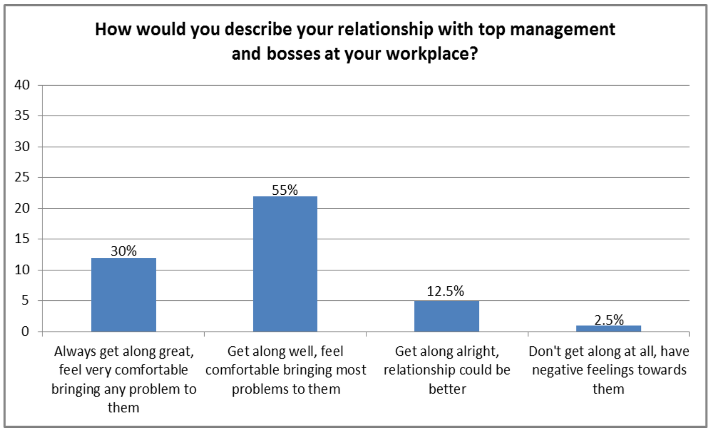
Recall that we had a total of eleven questions on the survey. Some questions were only concerned with IT security policies, some were only concerned with workplace relationships, and some comprised a combination of the two topics in order to see what effects they had on each other. We chose to perform the research and data gathering in this manner for several reasons. First, we wanted to get the most honest and accurate answers from participants as possible. By hosting the survey online and having responses remain anonymous, employees would not be inhibited to share their true views and not worry about feeling embarrassed to admit something, if for example they don't know very much about security policies or they have violated them in the past. Secondly, a multiple-choice survey makes it easier to compare and analyze results than other survey options. Had we elected to include open-ended questions, this might have forced us to analyze many different responses for each question and possibly not have been conducive to data mining and analysis. Our survey method was also less time-consuming and provided quicker results than doing workplace observations of employees. It also allowed us to gather responses from individuals in many different professions. We also wanted to collect information that reflected how employees operate in their daily routine workplace. Many prior studies have tried implementing different behavioral methods and then studying employees' reactions. For example, having a boss punish certain behaviors and reward others to see how it affects employees' compliance with policies. We wanted our study to differ from those by not introducing any type of changes in the workplace before we gathered our data. Our primary goal was to ensure that the results reflected real world circumstance.

IV. Results

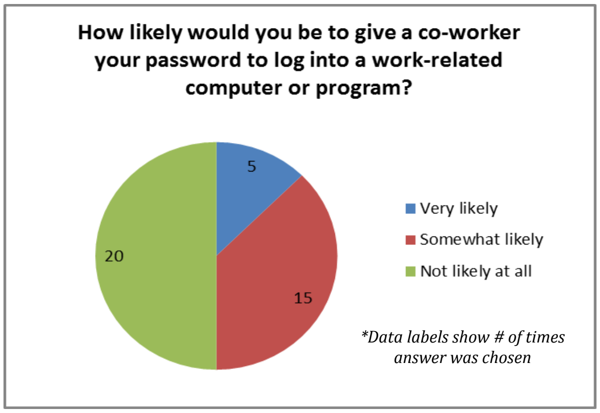
A. Data Observations

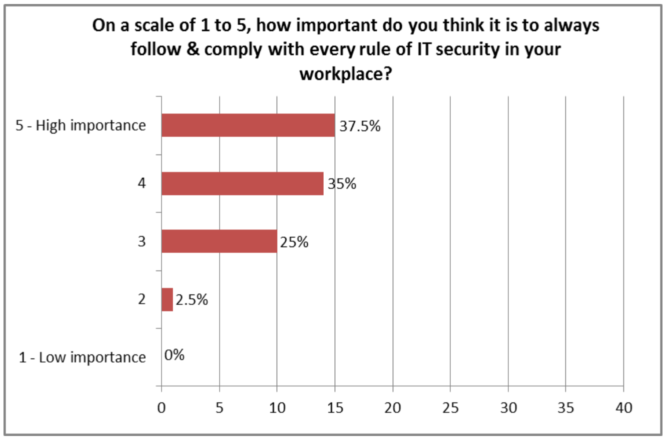
We observed from our data analysis that 45% of participants feel that they are only partly informed of their workplace's security policies and feel unfamiliar with numerous policies. This leads us to believe that one major cause of employees not complying with policies might be simply because they are unaware of them. Regardless of the social environment in the workplace, it appears that increasing user education would likely have a positive impact on policy compliance. The following two graphs display the results of questions dealing with relationships in the workplace.





From this data, we conclude that the majority of participants have a very positive relationship with both co-workers and upper management. A survey question asking participants to describe the company culture/environment in their workplace also produced positive answers, with 38% choosing "very comfortable and friendly environment where everyone feels relaxed" and the remaining 62% choosing "somewhat comfortable environment where everyone usually gets along fine." No participants chose slightly tense or very tense environment. Keeping this in mind, we now take a look at their usual inclinations towards IT security policies.





From these responses, we can gather that the majority of employees surveyed take security policy seriously and understand that compliance is extremely important. Results showed that 50% of employees answered “not likely at all” when asked how likely they would be to give a co-worker their password. We also asked if participants would be more likely to violate a policy if the reasoning was to help out a co-worker who is their friend, and 41% answered “no” and only 10% answered “definitely”. From these responses we can draw the conclusion that a positive relationship with co-workers seems to positively impact compliance with IT security policies. For most participants, they would not put their friendship above all else and violate a policy because of obligation to the co-worker.

It also seems that participants very rarely violate a policy, or if they do they are unaware of it, since 82% of participants chose “hardly ever” or “never” when asked how many times they have violated or not complied with a security policy or guideline. We also found that 59% of participants are very highly concerned with pleasing their boss and making others in their workplace happy by always doing an outstanding job at work. This makes it no surprise that 62% feel they have an extremely high sense of responsibility and accountability in the workplace.

When looking overall at the questions asked and the data collected, a majority shows positive results when dealing with both environment of the workplace and feelings towards IT security policies. The figure below displays a summary of all eleven survey questions and their most commonly chosen answer, along with the percentage of participants that selected that response.

How informed are you of your workplace’s IT security policies?	*Partly informed, not familiar with numerous policies – 45%*
How likely would you be to give a co-worker your password to log into a work-related computer or program?	*Not likely at all – 50%*
How likely would you be to violate or not comply with an IT security policy if it required you to do extra work or you felt it wasn’t all that important?	*Not likely at all – 56%*
How would you describe your relationship with co-workers?	*Very friendly, spend time together outside of work – 52.5%*
How would you describe your relationship with top management and bosses at your workplace?	*Get along well, feel comfortable bringing most problems to them – 55%*
How would you describe the company culture/environment at your workplace?	*Somewhat comfortable, everyone usually gets along fine – 62%*
On a scale of 1 to 5 (with 5 being highly important), how important do you think it is to always follow and comply with every rule of IT security in your workplace?	*5 – 37.5%*
Would you be more likely to violate an IT security policy if the reasoning was to help out a co-worker you’re friends with?	*No – 41%*
On a scale of 1 to 5, how concerned are you with pleasing your boss and making others in your workplace happy by always doing an outstanding job at work?	*5 – 59%*
On a scale of 1 to 5, how high is your sense of responsibility and accountability in your workplace?	*5 – 62%*
To your knowledge, how many times have you violated or not complied with a security policy or guideline at your workplace?	*Hardly ever – 46%*

B. How our Results Compare to Prior Research

When comparing our results to those found in prior related studies, we proved Pahnila et. al’s conjecture that “individuals create their behavior based on the interaction with each other” [4], and discovered how this is true in the area of IT security policies. We found that a good relationship between employees and co-workers, as well as that between employees and upper management causes them to have a more positive attitude towards following security policies. From our research it is not apparent if either of these relationships has a stronger effect on compliance than the other, but it is an interesting question to explore and we hope that our present work will motivate future studies on this topic.

Our results also relate to Herath et al.’s [3] study on organizational commitment. They claimed that an individual’s feelings of organizational commitment have a positive influence on their intentions to follow policies. We questioned whether an employee’s *intentions* are actually carried out and shown in their actions. Looking at our survey results, we can see that a great majority of employees have high levels of organizational commitment, and they also very rarely violate security policies and clearly understand their importance. We can conclude from this that organizational commitment not only influences the *intentions* to follow policy, but it also influences the actual actions of employees and leads them to follow policies more often.

Our findings are valuable to the research community because we have shown an important link between organizational environment and employee compliance with IT security policies. This correlation exists in the ordinary workplace in a variety of different job settings. We did not implement behavioral methods and try to alter the behavior of employees as many researchers have done in the past, but rather chose to focus on daily, typical relationships and actions. This has led us to significant research findings that will be meaningful and helpful in future studies because they exhibit the behavior of actual employees in their natural workplace interactions.

V. CONCLUSIONS

From our data analysis, we conclude that a positive relationship does in fact exist between workplace environment/relationships and employee compliance with IT security policies. However, since a majority of study participants already have a positive work environment as well as high inclinations to follow security policies, this makes us question why so many security breaches and IT problems still occur due to employee negligence? The only hint at this answer that can be gathered from our study is lack of employee education when it comes to policies. A total of 53% believed they were only partly informed or not at all informed in regards to their company's IT security policies. Since a majority also believed that following the policies is important and that they hardly ever violate them, it seems that a possible explanation is that they simply aren't familiar with the specifics of all policies. Perhaps future research done in this area could focus on employee education and knowledge of rules and policies, and possibly find that to be a reason behind the lack of compliance. Future research is also needed in the area of company culture and relationships affecting policy compliance, testing larger groups of participants and possibly separating companies into different categories to get a better idea of specific variations among different types of employees.

VI. REFERENCES

[1] M. Chan et al., "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," Journal of Information Privacy & Security, 2005, pp 18-41.

[2] A. Dillon and M. Morris, "User acceptance of new information technology: theories and models," Annual Review of Information Science and Technology, Vol. 31, 1996, pp 3-32.

[3] T. Herath and H. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organizations," European Journal of Information Systems, 2009, pp 106-125.

[4] S. Pahnila M. Siponen, and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," Proceedings of the 40th Hawaii International Conference on System Sciences, 2007, pp 1-10.

[5] T. Tyler, "Promoting Employee Policy Adherence and Rule Following in Work Settings: The Value of Self-Regulatory Approaches," Brooklyn Law Review, Vol. 70:4, 2005, pp 1287-1312.

[6] C. Vroom and R. Solms, "Towards information security behavioral compliance," Computers & Security, 2004, pp 191-198.

[7] J. Bishop, K Scott and S. Burroughs, "Support, commitment, and employee outcomes in a team environment," Journal of Management, Vol. 26, 2000, pp 1113 – 1132.

[8] A. Baker and W. Schaufeli, "Positive organizational behavior: Engaged employees in flourishing organizations." Journal of Organizational Behavior, 2008, pp 147 – 154.

[9] Y. Truckenbrodt, "The relationship between leader-member exchange and commitment and organizational citizenship behavior." Acquisition Review Quarterly, 2000, pp 233 – 244.

[10] S. Wayne, L. Shore and R. Liden, "Perceived organizational support and leader-member exchange: a social exchange perspective." Academy of Management Journal, Vol. 40, 1997, pp 82 – 111.

[11] M. Morris, V. Venkatesh and P. Ackerman, "Gender and age differences in employee decisions about new technology: an extension to the theory of planned behavior." IEEE Transactions on Engineering Management, Vol. 52, 2005, pp 69 – 84.

[12] P. Cardona, B. Lawrence and P. Bentler, "The influence of social and work exchange relationships on organizational citezenshp behavior." IESE Business School, 2003, pp 1 – 27.

[13] J. Forgas and J. George, "Affective influences on judgements and behavior in organizations: an information processing perspective." Organizational Behavior and Human Decision Processes, Vol. 86, 2001, pp 3-34.

VII. APPENDIX A

Below is the survey we designed for our study.

Survey

Please answer all questions and be as honest as possible. All results are anonymous.

1. How informed are you of your workplace's IT security policies (computer passwords, data protection, web monitoring, rules and legal issues, etc.)?

○ Very well informed
○ Well informed, familiar with most policies
○ Partly informed, not familiar with numerous policies
○ Not informed at all

2. How likely would you be to give a co-worker your password to log into a work-related computer or program?

○ Very likely
○ Somewhat likely
○ Not likely at all

3. How likely would you be to violate or not comply with an IT security policy if it required you to do extra work or you felt it wasn't all that important?

○ Very likely
○ Somewhat likely
○ Not likely at all

4. How would you describe your relationship with co-workers?

○ Very friendly, spend time together outside of work
○ Friendly, get along well but no connections outside the workplace
○ Somewhat friendly, tolerate each other with only occasional problems
○ Not friendly, frequently have problems

5. How would you describe your relationship with top management and bosses at your workplace?

○ Always get along great, feel very comfortable bringing any problem to them
○ Get along well, feel comfortable bringing most problems to them
○ Get along alright, relationship could be better
○ Don't get along at all, have negative feelings towards them

6. How would you describe the company culture/environment in your workplace?

○ Comfortable & friendly environment, everyone feels relaxed
○ Somewhat comfortable, everyone usually gets along fine
○ Somewhat tense, not usually very friendly
○ Very tense, not a healthy environment

7. On a scale of 1 to 5 (with 5 being highly important), how important do you think it is to always follow and comply with every rule of IT security in your workplace?

○ 1
○ 2
○ 3
○ 4
○ 5

8. Would you be more likely to violate an IT security policy if the reasoning was to help out a co-worker you're friends with?

- ○ Definitely
- ○ Maybe
- ○ Not sure
- ○ No

9. On a scale from 1 to 5 (with 5 being highly concerned), how concerned are you with pleasing your boss and making others in your workplace happy by always doing an outstanding job at work?

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

10. On a scale of 1 to 5, how high is your sense of responsibility and accountability in your workplace?

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

11. To your knowledge, how many times have you violated or not complied with a security policy or guideline at your workplace?

- ○ Many times
- ○ A few times
- ○ Hardly ever
- ○ Never