# The Assumptions and Profiles Behind IT Security Behavior

Puzant Balozian
Lebanese American University
Puzant.Balozian@lau.edu.lb

Dorothy Leidner
Baylor University and Lund University
Dorothy_Leidner@baylor.edu

## Abstract

*Among the major IT security challenges facing organizations is non-malicious employee behavior that nevertheless poses significant threats to an organization's IT security. Using a grounded theory methodology, this paper finds that organizational security behaviors are inherently related to employee assumptions regarding the importance of IT security policy compliance and regarding the reason why IT security measures are implemented. Analyzing these assumptions uncovers four profiles of perspectives concerning IT security: the IT Security Indulgence, the IT Security Overindulgence, the IT Knows Best and the IT Security Disconnect profiles. These profiles are useful in understanding employee IT security behaviors and may help IT departments in developing more effective strategies designed to ensure policy compliance.*

## 1. Introduction and Literature Background

Employees pose a significant threat to information technology security (ITsec) in organizations [4, 28]. Studies indicate that employees are responsible for over 50% of reported security breaches [21] and that carelessness or lack of awareness accounts for nearly 40% of insider security incidents [29]. 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 [20] and various industries have advanced standards regulating organizational IT security measures [4]. Nevertheless, some employees continue to show non-malicious opportunistic behaviors, circumventing IT security policies and thereby decreasing IT security effectiveness. Not all insiders are non-compliant, and not all non-compliant insiders have the same profiles.

In this paper, we investigate the working assumptions and the backgrounds of compliant and non-compliant employees, making this study one of the few that touches on the subject of profiling internal non-malicious volitional security violators. We uncover four profiles of IT security, each with different assumptions about ITsec measures. In the following paragraphs, we give a brief overview of the literature on IT security before describing the methodology and the analysis sections. The IT security literature is extensive, covering such manifold topics as information sharing among peers [11], disclosure of vulnerabilities in software [16], disclosure of security breaches [23], technical capabilities against outside attacks [2] and technical capabilities against opportunistic employees [12]. Several published reviews of the ITsec literature provide comprehensive meta-analyses of technical and behavioral ITsec research [25], of the deterrence approach in compliance [8], and of the different approaches to increase employee compliance to ITsec policies [1]. Evident in these reviews of the literature is the assumption implicit in most empirical IT security research that IT security is de facto "good", that the more IT security, the better, and that motivating employees to comply with IT security is a highly desirable objective for IT departments. Users face a plethora of ever-increasing security requirements that are sometimes viewed as constraining, demanding, and challenging to understand or follow [18, 19, 28]. The burden of security compliance may induce some employees to circumvent the policies with negative consequences for organizations [18, 24]. In a survey of thousands of employees, such explanations as "not-thinking about policies because of work overload" and "the inconvenience to follow policies" are reported as the main reasons for ISP violations [5].

This study seeks to advance our understanding of the assumptions behind compliant and non-malicious non-compliant users and the implications of these assumptions for IT security. In particular, the study employs a case study to uncover assumptions of compliant and non-compliant users to ITsec measures

URI: http://hdl.handle.net/10125/41767
ISBN: 978-0-9981331-0-2

and, in so doing, create profiles of internal employees' perspectives of IT security. Using a grounded theory methodology, we analyzed data obtained via interviews of faculty, staff, and administrators at a large private university in the southwest United States. Our analysis uncovers two basic assumptions underlying varying perspectives of IT security in organizations. Using these two assumptions, we develop a matrix of IT security policy perspectives (MSPP). The matrix depicts four perspectives of IT security policies. These perspectives are helpful in understanding internal employee reactions to increased security as well as their potential to circumvent IT security policies.

Consistent with grounded theory methodology, we did not enter the field with specific theories in mind. However, we did undertake a thorough review of the IT security literature to apprise ourselves of the theories and constructs widely used in studies of IT security and policy compliance. It was through our reading of the IT security literature that we noticed the dearth of research and theory into understanding the mindset of compliant vs. non-compliant professionals in organizations. In the interest of space, we refer the readers to several review papers for in-depth coverage of the IT security literature [1, 8, 25]. The remainder of our paper will present our method, data analysis, and emergent matrix of the profiles of compliant and non-compliant insiders as well as the implications of these profiles.

## 2. Methodology

Grounded theory is a methodology that does not force-fit data to a priori theory; rather, its aim is to derive theory from data [6]. The building blocks of the theoretical framework (the matrix) to be developed in this approach are intimately tied to the data [9]. Grounded theory has three basic components: 1) theoretical sampling and site selection, 2) data collection, and 3) data analysis and validation [6, 10].

### 2.1 The Site and Data Collection

The data collection site is a southwestern private higher education institution (PHEI) in the United States comprising ten colleges and employing approximately 1,000 staff and faculty. As of the date of this research, the university had roughly $300 million in operating cash, with total assets around $3 billion. Information security is highly valued by the university. The position of chief information security officer (CISO) was created in 2008.

To date, PHEI has never been hacked and, according to the CISO, is at the forefront of security implementations. In 2014, double authentication VPN was implemented so that those users who were off-campus but who wanted to access specific systems would not be able to access the network without a second authentication level (a code sent to an app on their smartphones). The trend for the coming years is that PHEI is moving toward making the majority of the systems inaccessible without a double-authentication method. Furthermore, PHEI has begun a project to encrypt voice mails and web and videoconferences. In recent years, PHEI has also added additional security including encryption to all institutionally provided computer devices. Although private devices are permitted on the premises, the devices can only access the Internet and no device can connect to the networks and printers. All institutionally owned mobile devices are tracked and remotely accessible by PHEI's IT department so that PHEI can wipe any device if stolen or lost. PHEI's website contains 43 pages of ITsec policies and guidelines. This strong emphasis on security policies makes PHEI a good site to analyze the plethora of users' responses to increased IT security.

Data collection consisted of conducting 32 semi-structured interviews (30 respondents) across the research setting. Sixteen IT related staff (4 females and 12 males) and 14 users (8 females and 6 males) were interviewed. Sample questions included "How do security policies enable and constrain your work practice?", "In what ways do IT security policies make you more effective in your role?" and "Are there ways that you feel the security policies constrain your work? If so, can you give me an example?". Four types of data were collected: 1) the interview data 2) internal documents on ITsec policies, 3) Q&A emails exchanged with IT security specialists, and 4) notes taken during attendance at a security awareness meeting designed for end users. We conducted the interviews over a 4-month period in 2015 and ranged from 17 to 48 minutes with an average of around 30.

### 2.2 Validation

Data validation occurred in two phases. First, we engaged in source triangulation. We sought input from directors who are faculty members, directors who are staff, faculty who are also administrators (e.g., department heads) and faculty not holding any administrative role. Some staff members interviewed were administrators, others were not, some staff in the Information Technology Services (ITS) were senior staff members, others were junior in their position. Some ITS staff worked as a bridge between the IT department and faculty/staff/admins, other ITS staff worked purely for the IT department. We triangulated at the strategic, managerial and operational levels in the organization in order to establish credibility, enhance the validity of the results, and avoid skewing the results [7].

In the second phase of the validation, six of the study's participants (almost 20% of the total interviewed) reviewed the findings. It is important to note that this technique, called member checking, is the "most critical technique for establishing credibility" in a grounded theory approach [14, 7].

### 2.3 Data Analysis

The unit of analysis is the individual, with a focus on understanding individuals' perspective of ITsec policies their behavioral response to the policies. We used Nvivo 10 software to code the data in the 3 phases of open, axial, and selective coding [17] during which we employed constant comparative analysis to guide the effort. This form of analysis allows for an evolution of themes, concepts, and categories from the data collected [22]. Following Charmaz [3], we interacted with the data to develop codes. Codes were then compared with data and other codes to develop categories. Concepts emerged through the process of comparing categories with other categories and codes. For example, the "user frustration" category described the following codes: "painful", "not fun", "frustration", and "adversarial dance [with IT]". The inadequate justification" category included codes like "not seeing the value yet", "surprised", "not understanding", "not knowing why" and "having no idea". The point of saturation for data collection and analysis was achieved whenever no new codes emerged from the data and when identified categories repeated themselves in the data [10]. At this point, we grouped the identified categories through axial coding. The goal of axial coding is to create themes to represent various related concepts identified in the transcribed manuscripts. For example, the profile "IT Security Overindulgence" emerged by several categories related to each other: "loss of productive time", "IT going overboard", "Not seeing value in ITsec measure(s)", and "lack of justification". Via selective coding, we related the concepts to each other to develop the profile matrix. These coding techniques ultimately resulted in four profiles (Figure 1) and 6 action/reaction outcomes toward ITsec measures: enforcers, cheerleaders, indifferent, circumventors, outspoken frustrated, and cautiously frustrated.

## 3. Analysis and Discussion

### 3.1 The Security Assumptions

Via grounded theory, we found two main security assumptions: a) Assumptions about the reasons for security (the y-axis of Figure 1) and b) assumptions about the importance of fully abiding by security policies (the x-axis of Figure 1).First, we uncovered a continuum of assumptions on security breach effects on organizations. Some employees assumed that security breaches are regular routine phenomena in this day and age and that any security breach is unlikely to seriously harm an organization. These employees think that the IT department feels so strongly about security not necessarily because the organization may suffer in the event of a breach, but because the IT department would be embarrassed. Employees on the other end of this assumption spectrum think that security breaches could seriously harm PHEI. In the security profiles section, we will give examples that describe these assumptions. The second assumption, related to the importance of fully abiding by security policies, ranges from "always important" to "not always important". Some organizational employees perceive that ITsec policies are important and therefore try to abide by them even if their productivity is hindered. Other employees do not perceive the policies as always important and are inclined to find a way to circumvent them to reduce hindrances to their productivity.

### 3.2 The Security Profiles

Figure 1 shows four quadrants resulting from the two assumptions described above. The IT security overindulgence quadrant, comprised of both IT staff and professional users, is skeptical about the enforced security measures. Individuals in this group assume that a security breach is unlikely to seriously harm PHEI and that abiding by the security policies is not always important. The IT security indulgence quadrant is comprised of employees who assume that ITsec measures may only embarrass the IT department rather than harming the overall organization but nevertheless feel that it is best to abide by ITsec measures. The "IT Knows Best" quadrant assume that the ITsec policies are always important and that a security breach in the organization may seriously harm the organization. Finally, the IT Security Disconnect quadrant is comprised of individuals who assume that a security breach could damage the university, but nevertheless do not consider it important to abide by ITsec policies. Instead, they believe that a breach of their own personal computer or their own ID/password would not constitute a security breach for PHEI.

We categorized each respondent into a quadrant based on our analysis of each interview transcript. We looked for statements that shed light on their assumptions. We counted ten respondents in the IT Security Overindulgence quadrant (6 IT staff and 4 professional users); 6 respondents in the IT Security Indulgence quadrant (all of them users); 10 respondents in the IT Knows Best quadrant (8 IT and 2 users) and 4 respondents in the IT Security Disconnect quadrant (1 IT and 3 users). These profiles are explained next.

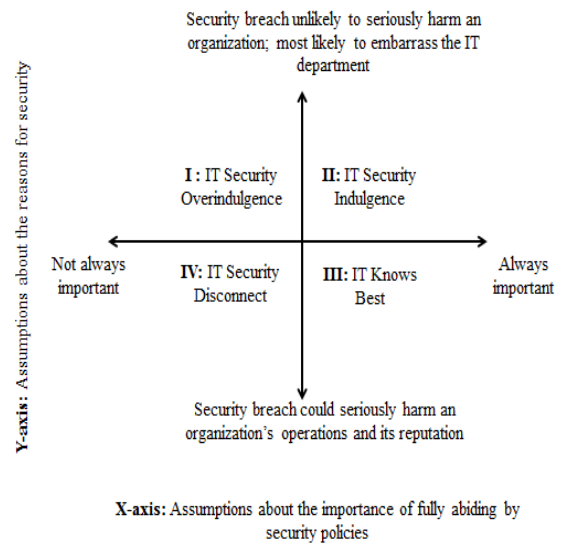
Security breach unlikely to seriously harm an organization; most likely to embarrass the IT department
I : IT Security Overindulgence
II: IT Security Indulgence
Not always important
IV: IT Security Disconnect
III: IT Knows Best
Always important
Security breach could seriously harm an organization's operations and its reputation
Y-axis: Assumptions about the reasons for security
X-axis: Assumptions about the importance of fully abiding by security policies

**Figure 1: Matrix of Security Policy Perspectives (MSPP)**

### 3.3 IT Security Overindulgence

The IT Security Overindulgence profile is comprised of both professional users and IT professionals. One might have expected IT professionals to all be in the IT Knows Best profile, but that was not the case. The IT professionals fitting this profile are the IT client services staff who are serving the professional users including faculty, staff and administrators in their business and functional needs. They find software, solutions or applications in the market to serve the functional needs of business units. Applications may range from proctoring software to online teaching solutions like blackboard or Canvas and a plethora of applications that enhance teaching, research and administrative roles in higher educational institutions.

These IT professionals who do not think that IT knows best and who may feel frustrated with current ITsec measures are the IT staff who are evaluated based on their productivity: how many and how fast they find solutions and how successfully they meet business needs. We notice that the IT staff of this group naturally might have a conflict of interest with the IT security goals: On the one hand, IT security staff want to minimize security vulnerabilities and therefore tend to reject the majority of the solutions suggested by the IT client services but on the other hand, the IT client services takes pride in the number of solutions found, suggested and implemented by them that solve functional problems and expand opportunities in PHEI (Res 5, 8, 10, 11, 13).

Driving the assumptions of these IT professionals is their belief that industry standards in the marketplace are enough. They view security breaches as routine and mundane ("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" Res. 8) and feel that the IT department need not go beyond industry levels, unnecessarily decreasing the productivity levels of business units.

One IT project manager whose role is to find software solutions on the market and make recommendations for their adoption at PHEI experienced frustration at a solution being rejected on security grounds in spite of the fact that "it's a widely used system" among universities and "none of them (the other universities) have any problems with it." He felt as if the university was trying to impose future standards on today's world: "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 software) standard in the industry and everybody's okay with that, why are we not? I don't understand it."

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, 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 [ability to change a grade].’ *That seems a little silly and unlikely, because the it’s a well-known widely trusted publisher,* but that was one of those scenarios where we didn’t get a chance to really do that (Senior Academic Consultant).

High activity organizational users and professionals also are part of this group. These professionals are evaluated based on productivity, specifically based on maintaining a high number of program enrollees (Resp. 25, 29 and 30) and/or a strong focus on research (Resp. 19 and 28). These are fast-paced professionals and they may be less tolerant of security constraints or measures that may impede or slow their productivity pace than other users who do not have a high activity level of work environment.

One administrator who is part of the university’s internal marketing department wanted to purchase an analytics system to help in the identification and analysis of prospective students. Her request was denied. She listened to the explanations for why the analytics system should not be used, but still does not find it justified:

> “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” (Director of a department).

Many others had similar feelings toward ITsec measures, aptly summed by one senior faculty member:

> I think at least in my case that the approach they take to this is 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, and not being there to really serve you. You’ve got to release a little bit of control. 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” (Senior professor).

In summary, the highly active and non-administrative professionals and users are skeptical of some of the IT security measures, particularly when the measures seem to be beyond those commonly found in other institutions and industries. For these users, excessive security is viewed as a hindrance to their productivity (Res. 17, 19, 25, 28, 29 and 30). They are the lifeline of the business units. Furthermore, their productivity levels are behind the organizational raison d’etre. They may be inclined to have a negative attitude to security measures from the IT department. This group perceives that IT security staff are enamored with the latest in security technology and that some security is only undertaken as much to legitimize the security professionals’ roles as to benefit the organization.

### 3.4 IT Security Indulgence

The IT Security Indulgence professionals are the respondents who are indulging the IT department and the ITsec measures without feeling strongly for or against either. They are either ambivalent concerning ITsec and/or they are problem avoiders who want to comply in order to stay away with from troubles with IT or leadership. One of them expressed his opinions toward ITsec measures by saying:

> The way PHEI has set that up [single log-in] is actually quite efficient so it’s not like we’re having to keep track of a bunch of different log ins with a bunch of different passwords. *I think we just assume* that they have the appropriate amount of security to protect the systems that we have, and *if they ask us to change passwords every three months or every six months or something, people just do it.* (Faculty and chair).

We asked another faculty about her knowledge and experiences with the Virtual Private Network (VPN) security guidelines. She responded:

> I know that *you do have to agree* to certain policies as you begin to use things like a VPN, but for the most part, that’s fairly standard, *so I don’t have any problems with agreeing to any of the policies* (Faculty)

This group is comprised of non-IT professionals who either have solely administrative duties (Res 18 and 32) or have fairly routine or low activity levels of work (Res 2, 24 and 27). They usually do not question increased ITsec measures and are either compliant or indifferent to security matters.

### 3.5 IT Knows Best

IT Knows Best profile includes IT professionals who are either in senior IT positions (Resp. 12, 16 and 21) and/or whose job role entails (fully or partly) the enforcement of security measures (Resp. 21) or the configuration and/or support of software implementations (Resp. 9, 14, and 15). These individuals are evaluated in their jobs partly based on security implementations. This group has also a number of users who are generally favorable toward both the overall ITsec measures and toward new security implementations.

The IT Knows Best professionals exhibit highly positive attitudes regarding security measures. One respondent explained with pride how the IT department uses a method created by the Department of Defense to erase all computers prior to recycling them:

> "We'll bring the computer back, wait for two weeks to make sure they (the users) have all their files, and then we use the magnetic storage data sanitization, the Department of Defense has kind of a method that uses seven passes to wipe a hard drive. We wipe it with that. From there the computers go to pallets to be sold to recyclers. They have to be certified basically" (Desktop configuration specialist).

The IT Knows Best professionals were not only quick to dismiss any inconvenience incurred by users resulting from PHEI's security procedures but also assumed (wrongly, as above-mentioned sections revealed) that most users understood the necessity of tight security measures. When asked about the possible downsides of the mandated encryption on the institutionally provided laptops, the director of the repair shop replied:

> "It's an inconvenience, but I think most people *probably* understand the need for the security. There is a little bit of delay [in the repair of the institutionally provided laptops], as I mentioned, if we're trying to recover data or trying to run some utilities on the drive, the drive needs to be unencrypted. But again, *I think* most people understand why the security is there. Once we explain what we have to do, they're pretty understanding about that." (Director of hardware support)

The IT Knows Best professionals are driven by their belief in the necessity of constant security improvement and seem to have little awareness of how the security improvements are received by users. Their attitude is well summarized by the CISO:

> 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 (CISO).

Unlike the skeptical users, these accepting users do not question the decisions of the IT department and acquiesce to any policies. An administrative user who also has a background in federal security contracting said "ITsec measures at PHEI are not constraining". She further expressed her positive attitude toward the ITsec policies by adding:

> There's an understanding of why they do what they do, and a thankfulness. I don't fault them for the layers they put in place, and I don't find they're without reason. I think that the way they operate it is quite reasonable, especially for the amount of knowledge, and security, and information they store and maintain. When you think about having to pull transcripts from 15 or 20 years ago, and with the incoming class of freshman of over 3,000, and multiply that. That in and of itself is just massive. Then you have the financials that have to be maintained, tuition records, and everything else. It's an immense amount of information that's required. *I will never fault them in protecting that knowledge.* I'm not saying don't ever question, but when it comes to things like this, *if you have a problem with this, why are you working here?* We keep our information more secure than the government does, and *I'm happy with that*. (Office manager)

In summary, we found that the attitude of IT Knows Best professionals toward ITsec measures is very positive. They systematically uphold the implemented security measures and perceive them with high regard. On the surface, this might seem obvious but as the previous sections demonstrated, neither all IT professionals nor all users are equally enthusiastic about IT security.

### 3.6 IT Security Disconnect

The IT Security Disconnect profile is comprised of users who feel that even though a real security breach could damage the university, they do not believe that a breach of their own account or the loss of their own laptop constitutes a security breach. They therefore do not consider it important to abide by ITsec policies and may find the security measures unnecessarily constraining. Their view of security allows for a disconnect between their own IT security habits and those prescribed by the university. One program director and senior professor expressed his views by saying:

> I do not understand AT ALL why my laptop needs to be encrypted. Even if someone stole my laptop and even if that someone managed to guess my password (both events are unlikely and their simultaneous occurrence even more unlikely), I do not believe that this breaches the university's IT security. I do believe that a "real" breach of security could hurt the university. I just do not believe that a "real" breach can be effectuated through my computer. (Senior professor and director of a program)

Some professionals do not find that their use of some systems is a security breach. One example of this is from the university's marketing department. A marketing manager purchased and began using an inexpensive analytics application in 2008. At the time of its initial purchase, the application had been approved by the IT department. Yet, subsequent to the establishment of the CISO position and the strict focus on security, the particular application was disapproved for use in other departments. The marketing department wanted to remain under the radar in order to continue to use a now disallowed system:

> "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" (Director of a program).

Even the non-use of a security feature is regarded as valid. After encryption was enforced on institutionally provided mobile devices including laptops (which dramatically increased the repair time of the devices), some professionals abstained from using PHEI's laptops. One software analyst and programmer told us: "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 an [institutionally provided] laptop" (Senior IT analyst).

In summary, we found four main profiles corresponding to two assumptions toward ITsec measures. These profiles have different outcomes for IT security behaviors. To this end, we dedicate the remainder of our paper in the following section.

## 4. Outcomes of the Four Profiles

The four groups in our matrix respond differently to security measures, even if they agree within their group on the security perspective. We found that the IT staff in the IT Security Overindulgence group although often frustrated, are more cautious in their assessments of IT intentions and are less prone to circumvent IT policies than the Security Overindulgence users. The latter group assumes that the IT department wants control, an assumption that we did not find in the interview texts of the IT client services (or at least not openly expressed in words). Furthermore, the security overindulgence users are more prone to be circumventors of ITsec measures. In the following table we briefly analyze the probable outcomes of each profile vis a vis security measures and we advance relevant propositions. Due to space limitations, this section is briefed in Table 1 and the quotations are limited to one quote per outcome. More quotes and proofs may be made available upon request by contacting the corresponding author.

Some existing ITsec theories seem to resonate with and complement our theory (MSPP) in Figure 1 although our theory differs from the existing ones in important areas. One of the most widely used theories in studies of IT security and IT security policy compliance is neutralization theory. Neutralization theory [26] describes the psychological techniques individuals use to justify socially undesirable behavior. These include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, appeal to higher loyalties, and the metaphor of the ledger. Some of these techniques might be employed by individuals fitting our IT Overindulgence and IT Disconnect profiles. However, the neutralization techniques are not based on assumptions, but rather rationalizations. In the case of neutralization, perpetrators are aware that they are behaving poorly but rationalize their behavior. Our analysis focuses on the underpinning assumptions of individuals that then drive their behavior. In the case of profiles, the individuals who are not complying with IT security policies do not believe that they are doing anything wrong. Hence, it is not that they are rationalizing, or neutralizing, their behavior; rather, based on their assumptions, they are acting rationally. Another theory called Control Reactance Compliance Model (CRCM) [15] has some similarities with MSPP as well as major differences. CRCM introduces the notion of "threat to freedom", "reactance to ITsec policy" and "proneness to reactance". Reactance is the negative emotional response (i.e. anger, frustration…) that is caused by the loss or threat of loss of behavioral/decisional freedom. CRCM finds that the threat to freedom and the proneness to reactance both positively influence the reactance, which ultimately negatively impacts the intention to compliance with the new ITsec measure. Although our profiles IT Security Overindulgence and IT Security Disconnect profiles share outcomes with the Reactance construct in CRCM, MSPP focuses on individuals' perceptions of IT security itself rather than on how IT security impedes, or promotes, their behavioral freedom. We maintain that in order to influence individuals' long-term IT security behaviors, IT departments must shape individuals' assumptions about security and not focus exclusively on the outcomes of their IT security behaviors. Finally, security literature profiling compliant and non-compliant employees focuses only on their motivations (malicious vs. non-malicious) [28], their intentional vs. unintentional noncompliance [4] and their level of technology expertise [1]. Our paper moves away from these dimesions to analyze the working assumptions and backgrounds of compliant and non-compliant employees.

## 5. Limitations, Contributions and Conclusion

As with any research, ours is not without limitations. First, we conducted this research at one site. Some may argue that the validity of one site is questionable. Nevertheless, Sarker et al., [22] 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 [13]. 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 paper 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 [27]. In 2015 alone, three major high profile security breaches hit Penn State University, the University of Connecticut, and the University of Virginia [27]. We believe the current reality of security breaches in the world, makes PHEI a relevant and credible proxy to other industries.

We conducted a grounded theory approach interviewing employees in a higher education organization and exploring their views on security measures applied in their institution. This study makes several important contributions. Our research extends the IT security literature investigating non-malicious security violators by looking at IT employees themselves as potential non-malicious violators. Most of the extant work treats IT employees as potential malicious violators because their expertise would seem to make it unlikely that they would inadvertently violate security policies. However, we uncover the possibility that IT employees can also be non-malicious violators. Future research should examine IT employees who are not necessarily disgruntled with their jobs or their organizations, but are ironically disgruntled with IT security itself. Second, this study revealed the underlying assumptions of employees in organizations regarding ITsec measures. The extant literature seldom touches on the assumptions of different groups concerning ITsec measures. Previous studies generally describe the antecedents of employee security behavior intentions. Our research examines the assumptions behind the antecedents of employee security behavior. Furthermore, future research is needed to incorporate IT expertise/knowledge into the MSPP matrix and to control for it among the profiles. The preliminary findings in MSPP shows that there are no differences among the IT Security Disconnect and IT Security Overindulgence vis a vis IT expertise, since in both groups we found both users and IT staff who expressed the above mentioned assumptions in the analysis section.

On the managerial level, this study challenges the dominant assumption of IT security and IT security policy compliance research that security and security compliance are de facto positive and good for organizations. We do not question the need for IT security, but our results do suggest that more security is not necessarily better security and that sometimes, in seeking to make oneself more secure, organizations inadvertently alienate high performing employees. The data suggests that there can be adverse effects to increased security measures on user satisfaction with the IT department and on security itself, especially in cases where users feel that the security measures are unaccompanied by adequate explanation and justification from the IT department toward the users (and other IT staff), thereby reinforcing their assumption of IT security overindulgence. The research on the downsides of ITsec measures is still young and evolving. We hope future researchers will extend and test the MSPP matrix with a view towards developing a stream of research that explicates the mixed and often contradictory feelings toward ITsec measures.

**Table 1: Profiles, Outcomes and Propositions**

| **Profile → Outcome** | **Quote → Proposition** |
|---|---|
| **IT Knows Best (IT staff) → Security Enforcing** | "Most of our updates [on systems] are pushed out via a couple of different methods. So, most of them are pushed out. Despite the fact that they're pushed out, we try to educate the users and make sure they know to check for updates, make sure their machine is updated and that sort of thing. But that's easier said than done, getting them to actually do that, which is why we try to be pretty proactive about pushing out updates (Software support specialist)."<br>**Proposition 1:** IT Knows Best IT staff will be more prone to enforce ITsec measures than to explain and justify a priori why they are enforced. |
| **IT Security Overindulgence (IT staff) → Frustrated but Staying Cautious** | "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 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 (Director of a computer center).<br>**Proposition 2:** IT Security Overindulgence IT members will be less prone than users to fault the ITsec measures and are less prone than non-IT users to circumvent ITsec policies. |
| **IT Security Overindulgence (users) and IT Security Disconnect → Circumventing and/or →Openly Frustrated** | "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. (Res. 30)"<br>In the words of a program director, "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, even without reflecting on who it's helping and what problem it's solving.*" (Senior professor)<br>**Proposition 3:** Security measures without sufficient justification in the eyes of the users increase non-malicious volitional security violations.<br>**Proposition 4:** In the absence of circumvention opportunities, security measures without sufficient justification in the eyes of the users increase user frustration with the IT department. |
| **IT Knows Best (users) →Cheerleading** | "You hear about all of these security breaches [in government], and hacks, and everything else. The one thing I would say is that you very rarely hear of a university ever having to disclose that there has been a breach of their information. If you consider all the financial records that are held by the universities, if they can protect it, why can't you [government]? Do you know what I mean? I would say universities have a model in place that would probably benefit some government areas (Office manager)"<br>**Proposition 5:** Users who have worked in a security-related firm in the past will encourage increases of IT security measures. |
| **IT Security Indulgence → Indifferently complying** | "I would assume that somewhere in the email is something about why and how important the VPN double authentication is, but I also assume that most of us don't read our email that in detail, and we also skim websites where we're picking up instructions on how to do the process we have to do, so we probably don't explicitly process that message, but I think it's there, but I'm assuming that." (Faculty)<br>**Proposition 6:** Users related to routine and administrative jobs will be more prone to comply with IT security measures than high activity non-administrative users. |

# References

[1] P. Balozian and D. E. Leidner, “Review of IS security policy compliance: Toward the building blocks of an IS security theory,” The DATABASE for Advances in Information Systems, (2016), forthcoming.

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

[3] K. Charmaz, “Grounded theory methods in social justice research”, The Sage Handbook of Qualitative Research, (4), 2011, pp. 359-380.

[4] Y. R. Chen, K. Ramamurthy, and K-W. Wen, “Organizations' information security policy compliance: Stick or carrot approach?” Journal of Management Information Systems, 29(3), 2012, pp. 157-188.

[5] Cisco Systems, Cisco Connected World Technology Report. San Jose, CA, 2011.

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

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

[8] J. D’Arcy and T. Herath, “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), 2011, pp. 643-658.

[9] K. Eisenhardt, “Building theories from case study research”, Academy of Management Review, 14(4), 1989, pp. 532-550.

[10] B. Glaser and A. Strauss, The discovery of grounded theory: Strategies for qualitative research. Aldine Publishing Company, New York, 1967.

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

[12] M. Keith, B. Shao, and P. Steinbart, “A behavioral analysis of passphrase design and effectiveness”, Journal of the Association for Information Systems, 10(2), 2009, pp. 63-89.

[13] A. S. Lee and R. L. Baskerville, “Generalizing generalizability in information systems research”, Information Systems Research, 14(3), 2003, pp. 221-243.

[14] Y. S. Lincoln and E. G. Guba, Naturalistic Inquiry, Beverly Hills, CA: Sage, 1985.

[15] P. B. Lowry and G. D. Moody. “Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies”, Information Systems Journal, 25 (5), 2015, pp. 433-463.

[16] S. Mitra and S. Ransbotham, “Information disclosure and the diffusion of information security attacks”, Information Systems Research, 26(3), 2015, pp. 565-584.

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

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

[19] G. V. Post and A. Kagan, “Evaluating information security tradeoffs: Restricting access can interfere with user tasks”, Computers & Security, 26(3), 2007, pp. 229–237.

[20] PWC, PricewaterhouseCoopers, Global state of information security survey 2013, New York, 2013.

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

[22] S. Sarker, and S. Sarker, “Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context”, Information Systems Research, 20(3), 2009, pp. 440-461.

[23] R. Sen and S. Borle, “Estimating the contextual risk of data breach: An empirical approach”, Journal of Management Information Systems, 32(2), 2015, pp. 314-341.

[24] M. Siponen, “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), 2000, pp. 197–209.

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

[26] M. Siponen and A. Vance. “Neutralization: New insights into the problem of employee information systems security policy violations”, MIS Quarterly, 34(3), 2010, pp. 487-502.

[27] K. Wagstaff and C. Sottile, “Cyberattack 101: Why hackers are going after universities”, NBCNews, 2015. Retrieved November 4, 2015, from http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821

[28] D. S. Wall, “Organizational security and the insider threat: Malicious, negligent, and well-meaning insiders”, Symantec Research Report, Mountain View: CA, 2011.

[29] E. Young, Get ahead of cybercrime, Ernst & Young’s 2014 Global Information Security Survey, 2014.