Abstract

IS security research has historically concentrated on evaluating phenomena’s effects on behavioral intention rather than actual behavior. We believe that an air-gap exists between behavioral intention and actual behavior - particularly as it relates to information security policy compliance. In this paper, we show through input from a panel of 12 information security experts that intention to comply with security policy may be interrupted for many different reasons. Using a ranking-Delphi method, we quantify information security expert opinion regarding what sort of scenarios are most likely to disrupt one’s desire (attitude) and intention to comply with information security policy. While our panel did not reach consensus on which scenarios may be most likely to interrupt security compliance, their experience and insight has reinforced the notion that behavioral intention is not an absolute predictor of actual behavior. As such IS security research should not culminate in evaluating impact to behavioral intention, but should instead attempt to understand a phenomena’s correlation to actual behavior whenever possible.

Keywords

compliance, IS security, behavioral intention

Introduction

There are technological and managerial mechanisms to control and persuade employees, but in the end, organizations are subjugated by the decisions of its employees – especially as it relates to information security. Herath and Rao (2009) note, employees within an organization have the autonomy to decide whether they will or will not abide by established security policies designed to reinforce security principles (p. 155). The IS (IS) security literature has recognized this problem and has suggested a range of motivation strategies to ensure compliance. In most of the studies we found, the focus of each respective motivator of compliance (with security policy) was rooted in questions regarding its impact on behavioral intention. For example, can structuring security controls in consideration of cultural norms directly impact one’s intention to comply? Or, can training and awareness programs that focus on deterrence and neutralization techniques have a positive effect on one’s intention to comply?

If we are to accept that behavioral intention is the only predictor of actual behavior, and our research ends with understanding a phenomena’s effect on behavioral intention alone, in our view, we are diminishing our capacity to contribute to IS security knowledge and understanding, and we are doing the research field a disservice. We do not doubt that behavioral intention contributes to actual behavior. However, we must relent that it is not the only determinant or predictor of actual behavior; research by Limayem et al. (2007), Webb & Sheehan (2006), and Paternoster and Simpson (1996), bears this out.

Why should IS security researchers be content to examine only one’s behavioral intention to adhere to security policy or control rather than measuring actual behavior? We advocate as Crossler et al. (2013) does – IS security research methodologies should endeavor to evaluate a phenomena’s correlation to actual behavior rather than settle for its correlation to behavioral intention. This endeavor leads to the
question driving the purpose of this paper – what may interrupt one’s intention to comply with security policies? Assuming, as we do, that there is an air gap between behavioral intention and actual behavior, with respect to IS security compliance, we seek to understand what may cause one’s intention to decouple with his or her actual actions.

**Literature review**

In this section, we review the IS security literature and examine how the behavioral intention to comply and actual compliance with security policies has been understood. Over the past several decades the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB) (Fishbein, 1980; Fishbein & Ajzen, 1975) have provided a rich foundation for IS and information security scholars. According to Webb and Sheeran (2006), “the TRA proposes that behavioral intention is the proximal determinant of behavior and mediates the influence of both the theory’s predictors (attitude and subjective norm) and external variables (e.g., personality and demographic characteristics). Thus, according to TRA, intention is the most immediate and important predictor of behavior” (p. 249).

Since its inception in 1975 by Ajzen and Fishbein, the theory of reasoned action (TRA) — attitude/subjective norms determine behavioral intention, which leads to actual behavior — has evolved. Ajzen, in 1991, revised TRA to include perceived behavioral control as an informant to behavioral intention (along with attitude and subjective norms) and called the resultant theory, the theory of planned behavior (TPB). The reasoned-action approach (RAA) was published by Fishbein and Ajzen in 2010 to further refine their original theory. The most significant modification was the addition of actual control as an intermediary input to actual behavior after behavioral intention. Ajzen and Fishbein’s theory as it stands today suggests that behavioral intention and actual control are the only immediate predictors of actual behavior.

Over the course of TRA’s evolution into RAA, it has been used immensely in empirical research across many research fields. One need only do a cursory search to confirm the impact Fishbein and Ajzen have had in academia. Davis’ Technology Acceptance Model (TAM) in the IS research community is a widely-recognized case-in-point. However, the TRA (and its later derivatives) have also seen dissent and counter-proposition regarding their stated behavioral predictors.

For example, Limayem et al. (2007) suggest that habit (automaticity and mental efficiency of behavior occurring in stable contexts (p. 714)) can have a direct effect on actual behavior, or, habit can be a moderator of actual behavior. They refute the notion proliferated by supporters of theory of reasoned action that habit is instead merely a predictor of intention and that actual behavior is driven by intention alone (p. 717). Limayem et al. (p. 728) represent findings whereby habit is considered as a direct effect as well as a moderator for actual behavior. Ultimately they came to the conclusion that, “circumstances might exist under which this effect [intention's capacity to exert a direct effect on actual behavior] is partly or even entirely suppressed. In these cases, intention could no longer be regarded as a reliable predictor of actual behavior” (p. 730).

Webb & Sheehan (2006) did a meta-analysis of 47 studies to rigorously understand the relationship between intention and actual behavior. They were motivated by their observation that, “most tests of the intention–behavior relation involve correlational studies that preclude causal inferences” (p. 249), and they found that, “a medium-to-large sized change in intention engenders only a small-to-medium change in behavior. Findings also showed that intentions have less impact on behavior when participants lack control over the behavior, when there is potential for social reaction, and when circumstances of the performance are conducive to habit formation. Thus, this review suggests that intentional control of behavior is a great deal more limited than previous meta-analyses of correlational studies have indicated” (p. 262).

Paternoster and Simpson (1996) stated that intention should not be viewed, “as a direct proxy for actual behavior but as an indicator of a motivational state that exists just prior to the commission of an act. We think of it as a measured reflection of a predisposition to [act]” (p. 561). Their perspective once again denigrates the absolution of behavioral intention’s capacity to predict actual behavior.

The case has been made by Fishbein and Ajzen (2010) that behavioral intention and actual control are viable predictors of actual behavior; but other studies are not inherently consistent with their theory.
What Interrupts Intention to Comply with IS-Security Policy?

This, at the very least, elucidates responsibility on the part of researchers to explore actual behavior vice behavioral intention whenever possible. The point here is not to suggest that we should throw out decades of research and literature because it is predicated upon TRA, TRB, or RAA, but rather that we should not blindly accept RAA’s predictive capacity or avoid empirically testing actual behavior in future research endeavors if we are to truly understand a phenomena’s impact on the real world.

In the IS security domain, recent contributions by Crossler, et al. (2013) recognize the need and capacity of researchers to evaluate actual behavior rather than intentioned behavior in future IS security research endeavors. Crossler, et al. point out that previous studies have suggested that it is preferable to measure actual behavior rather than behavioral intention within the IS security research field. As is so poignantly pointed out, intentions do not always lead to behaviors and, with respect to information security, “it is the actual behavior that matters – not the intention to perform the behavior” (Crossler, et al., 2013, p. 95). Moreover, “individuals are either performing the risk-mitigating behavior or they are not – intention without action may lead to a security breach” (p. 95).

We have shown (see Appendix 1) that a vast majority of current IS security research is heavily reliant on TRA and TPB and thus on behavioral intention. We have also shown research exists which potentially diminishes the IS security researcher’s capacity to rely on assessing a phenomena’s impact on behavioral intention if results are to be considered reliable. For these reasons, it is our aim for the remainder of this paper to demonstrate scenarios exist where behavioral intention is decoupled from actual action in a way that is inconsistent with what TRA/TRB/RAA and the notion of behavioral intention would otherwise predict. Our research goals include further demonstrating the necessity to assess a phenomena’s impact on actual behavior rather than intention whenever possible, understanding what may cause someone to abandon their intention in lieu of another course of action with respect to IS security compliance, and finally to advance theory with respect to user behavior and actual IS security compliance.

Methodology

The Delphi method is a mechanism by which a group of experts may reach a consensus – though this is not necessarily the goal (Von der Gracht, 2012, p. 1527); its genesis was in the 1950s by the RAND Corporation (Okoli & Pawlowski, 2004, p. 16). As noted by Okoli & Palowski, the Delphi method has been used to (among other things):

- Forecast the role of the systems analyst in the 21st century
- Compile a ranked list of 12 future scenarios related to the potential success of the Wireless Application Protocol (WAP)
- Develop a conceptual taxonomy of organizational design actions — mechanisms to enhance technology users’ propensity to innovate in information technology.
- Develop a ranked list of common risk factors for software projects as a foundation for theory building about IS project risk management.

The Delphi method has several derivations that can be applied to various situations and research scenarios according to the topic being researched or the problem being solved. In our case, we elected to use a ranking-type Delphi method to look for group consensus among IS security experts regarding what may interrupt one’s intention to comply.

The ranking-type Delphi method implements an iterative, algorithmic approach to refine issues and ultimately rank them. At a very high level, the algorithm is implemented as follows (Schmidt, 1997, pp. 764-765):

1. Identify a set of issues;
2. Elect a set of experts to participate in the ranking;
3. Until a consensus is reached regarding the ranking of the issues or rankings stabilize:
4. Each expert independently ranks the issues;
5. Researchers consolidate the list and calculate rank-mean for each issue;
6. Issues outside of an established threshold are removed from the list;

In our case, we were not ranking a set of issues, but rather a list of possible scenarios and their likelihood of facilitating the interruption of one’s intention to comply with security policy.
Survey Group

Regarding the establishment of a set of scenarios that may interrupt one’s intention to comply with security policy, we leveraged input from a group of IS security professionals (Step [1] in the ranking-type Delphi method described above). A preliminary list of nine (9) scenarios that may interrupt one's intention to comply was shown to 278 professionals. Of these, almost 80% were in the information technology and services or computer and network security industries. Job titles of these professionals included Information Security Specialist, Business/Corporate Strategist, Consultant, Founder/Partner, Information Technology Generalist, and Information Technology Systems Administrator/Engineer among others. As a result of this review, the list of nine original scenarios grew to 18. These 18 scenarios were finalized and then used in the first round of the ranking-type Delphi survey we conducted.

As suggested by Okoli & Pawlowski (2004), we wanted to use a group of 10-18 experts to rank the 18 scenarios we identified. We solicited interest from our group of IS security experts and were able to gain participation from 12. Ultimately, the panel of 12 we selected was comprised of information security experts that we expected (based on its members’ own professional experience) would be capable of providing an aggregate level of understanding regarding what it has seen interrupt one’s intention to comply with a given security policy.

We conceded that the group’s responses would be conjecture to some extent, but we expected this to be compensated for by the nature of its professional experience, education, and understanding of implementing technology or assessing security control performance and risk metrics. On average, our participants had over 10 years of IS security experience (see Table 1).

<table>
<thead>
<tr>
<th>#</th>
<th>Current Job Title</th>
<th>Years Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Senior IT Auditor</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Senior Technical Writer</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Sr. Cyber Security Analyst</td>
<td>20+</td>
</tr>
<tr>
<td>4</td>
<td>Cybersecurity Analyst</td>
<td>14</td>
</tr>
<tr>
<td>5</td>
<td>Senior Security Analyst</td>
<td>13+</td>
</tr>
<tr>
<td>6</td>
<td>IT Risk Manager</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>Director</td>
<td>20+</td>
</tr>
<tr>
<td>8</td>
<td>System Administrator</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>Information Technology Specialist</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>Enterprise Security Architect</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>CISO</td>
<td>10</td>
</tr>
<tr>
<td>12</td>
<td>Penetration Tester</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 1 Survey Group Job Titles and Years Experience

Scenarios That May Interrupt One’s Intention to Comply

The following list of 18 scenarios was contrived by myriad information security professionals and represents a consolidation of professional opinion regarding what may disrupt and interrupt one’s intention to comply with security policy. The origin of this list was predicated upon the following scenario (Figure 1).

(1) Bob works for Company X
(2) Company X has robust security policies and infrastructure in place
(3) Bob is aware of and knowledgeable about the security policies of Company X
(4) Bob wants (attitude) and intends (intention) to comply with Company X security policy
(5) Bob does not comply with Company X security policy

Figure 1 Scenario of Interruption

Given this scenario, we attempted to identify what may happen during or after (4) above with respect to Bob to produce the outcome (5) that Bob does not comply with Company X security policy. We took care to focus only on scenarios where Bob’s attitude and intention to comply remained unchanged until such
time that he actually did not comply with security policy. This list is not necessarily exhaustive; however, it is a well-vetted list that has been evaluated, commented on, and contributed to as previously described.

1. Productivity 10. Social Norm
2. Habit 11. VIPs
3. Management Direction 12. I’m IT; it’s OK
4. Convenience 13. Lack of Tech
5. Rely on IT 14. Urgency
6. Avoid Confrontation 15. Management Expectations
8. Misunderstanding 17. Peer Pressure

**Study Administration**

Using the 18 scenarios outlined above, we asked our panel of 12 IS security experts to rank each of the 18 scenarios (from 1 – 18) based on the likelihood (in their experience) that the scenario would interrupt one’s intention to comply with security policy in consideration of Figure 1.

For example, to represent the notion of *convenience*, we presented the scenario, “Bob knows that he should not store his credentials in his SSH or FTP client; however, there is one system that he rarely accesses for which he can never remember his password, so he makes an exception here and stores his credentials.” For the scenario of *coercion*, we presented the scenario, “Bob has a gambling problem and owes a lot of money to his bookie. Bob knows he shouldn’t share Company X intellectual property with his bookie, but his bookie is threatening his life unless he shares trade secrets. Bob shares trade secrets.” As a final example, to represent *urgency*, we presented the scenario, “Fred is not a developer, but his job requires him to publish changes made by developers to production. Fred is on vacation and production is suffering, so Bob, who is a developer and should not make changes to production, makes the changes anyway.”

Upon completion of the first ranking round by the panel, the rank-mean for each scenario was calculated, and any scenario receiving a rank-mean greater than 10 was terminated from the next iteration of ranking. This effectively reduced the number of items to rank from 18 to 13. The first round of ranking was also the round that generated the most consensus (though it was nominal) amongst the panel. Consensus was measured using Kendall’s Coefficient of Concordance, $W$ ($0 \rightarrow 1$, where 0 is no consensus and 1 is total consensus) (Schmidt et al., 2001). The first round yielded a $W$-value of .282 with the majority of consensus being exerted to identify those scenarios that are least likely to interrupt one’s intention to comply (e.g., coercion and moral obligation).

This process was repeated for four rounds; at the conclusion of each ranking round, scenarios with the least likelihood to interrupt one’s intention to comply (higher rank-means) were terminated and not presented in subsequent rounds. This was done consistent with the Ranking Delphi method in order to facilitate movement towards consensus.

Figure 2 shows the rank-mean by round for each of the 18 scenarios. For each round, rank-mean highlighted in red indicates the scenario did not proceed into subsequent rounds; black indicates the scenario graduated to the next round. The termination-threshold used for each round is also included in Figure 2 and was selected at each round in order to drop the bottom half of the ranked scenarios. We made an exception to this approach in round 1 to ensure our initial termination of scenarios was not too aggressive.
It is important to note that our criterion for stopping the rounds of ranking was not predicated upon consensus (as many Delphi studies incorrectly are), but rather on stabilization of the rank-orders. As pointed out by Linstone and Turoff (2011), “Our 1975 book clearly states that Delphi is a method for structuring a group communication process, not a method aimed to produce consensus. The number of rounds should be based on when stability in the responses is attained, not when consensus is achieved” (p. 174). In this vein, we could have stopped ranking after three rounds; however, we conducted the fourth round in an effort to achieve both consensus and rank-order stabilization.

Greatorex & Dexter (2000) suggest that mean and standard deviation may be used to calculate stability in rank-order between rounds (p. 1019). We used the Coefficient of Variation (CV) to determine when rank-stabilization had occurred (at the third round). According to Dajani at al. (1979), stabilization increases as the difference (Δ) between CV between rounds approaches zero (Figure 3).

**Discussion**

Let us set aside any (potentially misguided) dissatisfaction with the panel’s inability to reach consensus, and instead focus on the three final, remaining scenarios from a list that began with 18. These three scenarios, since the second round of ranking, remained the three most likely scenarios (according to our panel of experts) to interrupt one’s intention to comply with security policy. The reason these three were ranked as highly as they were by the panel is not known and may well be the subject of future inquiry. However, one may easily reason with confidence why these three consistently remained at the top of the rank-order.

If lack of convenience is the most likely scenario to interrupt one’s intention to comply, then the sensible response is to design security policy and controls in consideration of convenience as well as security. There is plenty of IS security research out there that focuses on the economics of security — balancing risk reduction with cost (Huang & Behara, 2013; Anderson & Moore, 2009; Gordon & Loeb, 2002; Beutement & Sasse, 2009; Salim et al., 2013); however, there is surprisingly little research focusing on balancing security with utility and business functionality (Shultz et al., 2001, p. 620). Perhaps future directions in the IS security field should include some volume of research focusing on balancing (or even emphasizing) convenience with security.

Shultz et al. (2001) address some aspects of convenience by looking at usability design. They observed, “When users must interact with systems to implement, use, and/or maintain security, the usability of the interaction tasks is a critical factor in determining user willingness to engage in these tasks” (p. 622). Restated in the context of our research here, if control systems (security systems) are not user-friendly or convenient to use, they will be resisted or rejected altogether. Certainly the usability design of technical controls (e.g., authentication, encryption, digital signature, physical access) is only one portion of a larger compliance and control model (which may include both technical and non-technical, operational controls) that may be implemented by organizations; however, the point that users will resist or reject security measures that are not, in their view, easy to use is consistent with our findings.

Outside of the security research arena, there has also been some academic work done with respect to how convenience drives users to interact with information technology in general. Bhatnagar et al. (2000) explored the attraction of online versus traditional shopping. They cite a seminal study by Becker (1965) that shows consumers always maximize their utility subject to time constraints and cost constraints. Given that most online retailers are able to offer competitive, if not better, pricing for goods, it becomes
apparent over the course of their study that time constraints and convenience factors play a more significant role in the decision-process to shop online or at brick and mortar.

The study also points out that the price constraint may have been replaced by a risk constraint whereby a consumer’s perspective of riskiness combined with their view of convenience influences their decision to shop online. Bhatnagar, et al.’s data analysis shows trends that delineate perception of risk across market segments, age, gender, and experience on the Internet.

It is important to note, however, that the perception of risk within the context of this study is unequivocally personal. That is, consumers are not concerned with risk implications for anyone other than themselves. According to the study, risk is perceived according to two different classifications: product risk (will a shirt fit or will the sunglasses look good on the consumer?) and financial risk (the likelihood that fraud will occur affecting the consumer).

Both of these perceived risks are associated with possibility of personal loss. In our view, an important observation is that in the workplace, workers do not necessarily assume the risk profile of the company in the same way. Herein lies another reason why convenience seems to trump risk-aversion in the workplace. This line of research may also provide valuable insight on how best to protect information.

Without also delving into urgency or increased productivity here, one would likely concede that it is fairly trivial to identify cases where these top three scenarios could significantly undermine security implementations and controls executed by companies. Moreover, it is easy to conceive that scenarios emphasizing urgency or increased productivity over security could be very commonplace across different industries, organizations, or even individual business units.

**Implications for Research and Practice**

It is evident that these security experts agree it is possible to decouple one’s intention to comply from his or her actual behavior. It is also evident from the contributions of our panel of 12 IS security experts that many of the 18 scenarios we proposed as having the capacity to interrupt one’s intention to comply have merit. We have also shown that while behavioral intention is a very capable predictor of actual behavior, it is not absolute. As such, it would be prudent for future IS security research endeavors to begin focusing more on a phenomena’s impact on actual behavior rather than stopping with an assessment of its impact on attitude and intention. If there is a gap between intention and compliance as our research suggests, IS security research streams (particularly those focusing on compliance) should no longer endeavor to merely assess implications on attitude and intention. Instead, they should assess actual compliance and actual behavior whenever possible.

The presumption that attitude and intention are primary predictors of behavior is not necessarily incorrect in all cases; however, we have shown that with respect to IS security compliance, it is certainly not absolute. This is not a new observation, but merely reinforces prior research which has served as detractors of TPB and its derivatives. It is conceivable that in many research environments, assessing actual behavior can be quite challenging. This is why TPB is so attractive as a methodological driver. If TPB is correct in that attitude and intention (and actual control) is absolute when predicting actual behavior, assessing attitude and intention may be considered equivalent to assessing actual behavior. However, we believe that it is not. As a result, we believe it is incumbent upon researchers to either (i) confirm that TPB is absolute in the context with which they are using it, (ii) make the concession that the use of TPB is a limitation of their research, or (iii) endeavor to assess actual behavior instead of relying on TPB.

With respect to practice, imagine a computing environment where encrypting and decrypting e-mail was inherently convenient inside or outside the workplace. What if there were a simple, convenient way for various healthcare providers to securely share patient health information electronically? What if information security training was short but exceptionally impactful? What if security policy and protocol didn’t inhibit productivity, but rather enhanced it? And, what if companies were more concerned with security than the speed with which they produced their service offerings? These are all scenarios that could bolster the security posture of organizations while also catering to convenience, productivity needs, and reduced emphasis on urgency. And, they are all scenarios that may minimize deviation from or circumvention of IS security control according to the findings of our research.
Conclusion

This essay has endeavored to show that IS security compliance is not governed by intention alone and that scenarios exist that interrupt behavioral intention and amicable attitude ultimately resulting in actual behavior predicated on other factors. While convenience, productivity, and urgency are the drivers most likely to interrupt intention to comply with IS security policy, future research streams should explore each of the 18 scenarios in greater detail to ascertain their capacity to influence actual behavior with respect to IS security compliance. The findings of such research may be paramount to the design and development of more effective IS security control.

It would also be interesting to apply systems design theory to IS security control design. It would not be surprising to learn that tenets of good systems design, e.g., usability, efficiency, simplicity, may serve designers and developers of security controls well. This is especially true for IS security controls that have direct implications for users or that require some level of compliance or participation from users directly affected by them. If researchers can identify controls that cater to functions of convenience, productivity, and urgency (or any of the remaining 15 potential scenarios discussed above), the level of compliance may well see a positive impact.

REFERENCES

What Interrupts Intention to Comply with IS-Security Policy?


## Appendix 1

<table>
<thead>
<tr>
<th>Title</th>
<th>Framework</th>
<th>Journal</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Awareness of Security Countermeasures and Its Impact on IS Misuse</td>
<td>TRA</td>
<td>ISR (2009)</td>
</tr>
<tr>
<td>Beyond Deterrence: An Expanded View of Employee Computer Abuse</td>
<td>TPB, TRA</td>
<td>MISQ (2013)</td>
</tr>
<tr>
<td>A Canonical Analysis of Intentional Information Security Breaches by Insiders</td>
<td>TRA</td>
<td>IMCS (2009)</td>
</tr>
<tr>
<td>Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness</td>
<td>TPB, TRA</td>
<td>DSS (2009)</td>
</tr>
<tr>
<td>Employees' adherence to information security policies: An exploratory field study</td>
<td>TRA, Actual Behavior</td>
<td>I&amp;M (2014)</td>
</tr>
<tr>
<td>Does deterrence work in reducing information security policy abuse by employees?</td>
<td>TPB, TRA</td>
<td>Comm ACM (2011)</td>
</tr>
<tr>
<td>Motivating IS security compliance: insights from habit and protection motivation theory</td>
<td>TRA, TPB</td>
<td>I&amp;M (2012)</td>
</tr>
</tbody>
</table>

Table 3 Recent IS Security Research