The Social Psychology of IT Security Auditing From the Auditee's Vantage Point: Avoiding Cognitive Dissonance

Thomas J. Bell III, Ph.D., CISA, is a professor of business administration in the School of Business at Texas Wesleyan University in Forth Worth, Texas, USA, and an IT security auditor for ComputerMinds.com in Euless, Texas, USA. His IT auditing specialty is IT audits for small community banks (IT security audits and external penetration testing) and SAS 70 Type I and II audits. Bell has published quarterly material for the Business/Technology Chapters of *Continuing Professional Education (CPE) Direct*, which is released in conjunction with the American Institute of Certified Public Accountants (AICPA)'s *Journal of Accountancy*.

Independence, objectivity and impartiality are all auditing hallmarks and are essential if an auditor is to render sound professional opinions that are constructive components of corporate governance and capital resource allocation judgments. Yet, they are all seemingly innocuous descriptive terms that are also chock-full of innuendos and dissonance. Perhaps an understanding of social psychologist Leon Festinger's seminal research on his theory of cognitive dissonance would help. The theory examined the psychological phenomenon that presents discomfort when an individual is faced with a discrepancy between their existing beliefs and their actions. According to the cognitive dissonance theory, there is a tendency for individuals to seek consistency among their cognitions (i.e., beliefs, opinions) and actions. When there is an inconsistency between attitudes and behaviors (dissonance), something must change to eliminate the dissonance. In the IT context, dissonance occurs when an auditor perceives a logical contradiction among their cognitions and their professional code of ethics. ISACA's Code of Professional Ethics for auditors states the following:

> *Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.*[1]

This article discusses the auditor's objectivity and due diligence, as a corollary to requisite soft skills or the social psychology of conducting a security audit and the need to understand the individual's (auditee) thoughts, feelings, behaviors and influences. Recognized principles of human social behavior hold the potential of teaching auditors some useful techniques to improve their auditing services.

Many information security specialists will agree that security depends on people more than policies, controls or technology.[2] Extending this maxim, people (employees) pose a far greater threat to information security than outsiders.

It follows from these observations that improving security depends on changing beliefs, attitudes and behavior of both employees being audited and auditors. Social psychology can assist an auditor's comprehension of how best to work with human predilections and predispositions to achieve their goals of improving security.

The social psychology issue of dissonance is brought to bear when an auditor's independence and objectivity are impaired by preconceived notions or generalizations, which present as an issue of dissonance a possible conflict with the previously quoted statement of ISACA's Code of Professional Ethics, which mandates objectivity, due diligence and professional care. Preconceived notions or generalizations arguably impair an auditor's objectivity.

The aim of a security audit is to express an opinion based on an unbiased evaluation of the system in question after performing some test. Since time and resources are in short supply, the entire IT infrastructure cannot be tested; therefore, only a subset of the system is examined by an auditor, which may appear arbitrary to the auditee and objective to the auditor if their findings note issues of noncompliance with standards or IT security lapses.

Yet, the human psychology of the audit client (when collecting and evaluating evidence of an organization's information systems, practices and operations) is often overlooked, with emphasis usually placed on the process and not the client. In a number of ways, auditing is a human relationship business. As such, auditors should understand the social psychology or the people side of auditing beyond the standards, procedures

and best practices. Clearly, it is important to understand the process of obtaining and evaluating evidence to determine if an information system adequately safeguards assets and maintains data integrity while operating effectively and efficiently to achieve the organization's goals and objectives. However, understanding the social psychology of IT security auditing is equally important as the auditing processes and procedures. Doug Schweitzer, an Internet security specialist and freelance writer, stated:

> *Security isn't only about protecting your network from external threats; it's also about protecting against threats from within. The first step to security is awareness; therefore, it's important that all your employees know not only the potential threats but also how to recognize and prevent such threats. Education and awareness empowers each employee with the knowledge of his role in protecting the organization's network. This, in turn, will go a long way toward mitigating risk.*[3]

Persuading audit clients to become more security-conscious may involve finding ways to overcome auditing anxiety by effectively communicating with auditees, and letting them know what they are expected to do and what the auditor is doing to support their efforts to reasonably safeguard the organization's information assets. However, no security controls or technology will successfully protect an organization if employees are naive, poorly trained or not made aware of the impact of security violations. Again, security depends on people more so than technology. Therefore, improving security depends on changing the beliefs, attitudes and the behavior of audit clients. Social psychology can help us better understand how to work with human predilections and predispositions to achieve the auditor's goals of improving security.

COGNITIVE DISSONANCE THEORY

More than half a century ago, social psychologist Leon Festinger developed the cognitive dissonance theory.[4] Cognitive dissonance is an uncomfortable feeling caused by holding two contradictory thoughts simultaneously. The thoughts or cognitions in question may include attitudes, beliefs and awareness of one's behavior. The theory of cognitive dissonance proposes that people have a desire to reduce dissonance by changing their attitudes, beliefs and behaviors, or by justifying or rationalizing their attitudes, beliefs and behaviors.

Dissonance normally occurs when people perceive a logical inconsistency among their cognitions. This happens when one idea implies the opposite of another. For example, an auditor having a predisposition prior to the audit is inconsistent with ISACA's Code of Professional Ethics. Becoming aware of the contradiction would lead to dissonance, which is characterized by a host of emotional states such as stress, anxiety, shame, guilt, anger and embarrassment. Audit clients may also experience dissonance when they smile and heartily agree to assist the auditor in any way possible; when in fact the auditee may feel that the auditor is:

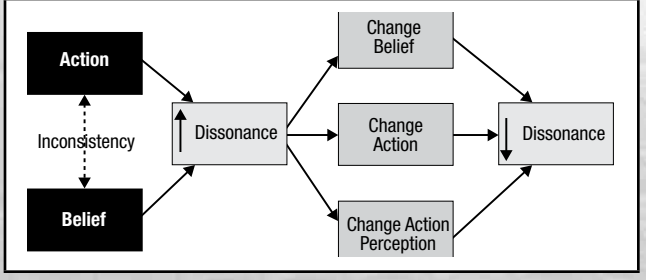
- Simply overlooking what is being done right in order to find problems
- Blindly operating from an archaic set of laws and regulations that he/she knows are no longer relevant
- There to do management's dirty work (i.e., get people fired)
- Not weighing the severity of the risk against the cost of containing or eliminating the risk
- Asking dim-witted questions
- Unaware of how the systems work, resulting in asking the same questions over and over again
- Asking for documents no one reads or has
- Wasting time getting documents and running meaningless test(s)
- Visiting only to find mistakes and report them to the boss
- Writing up harmless findings as if it will put the company at dire risk

Given the audit client's feelings, information may be withheld, omitted or even hidden from the auditor. Such conflicting emotional distress may cause anxiety for the auditee and lead to rationalization (the tendency to create additional reasons or justifications to support one's behavior).

Festinger's cognitive dissonance theory is based on three fundamental assumptions (see **figure 1**):

1. **Humans are sensitive to inconsistencies between actions and beliefs.** Auditees may recognize at some level when their behavior is inconsistent with their beliefs, attitudes and opinions. In fact, one could argue that everyone has a built-in filter that alerts them when inconsistency between their actions and thoughts occurs.

Figure 1—Cognitive Dissonance Theory



2. **Recognition of this inconsistency will cause dissonance and will motivate an individual to resolve the dissonance.** When an auditee realizes he/she has violated one of his/her principles, some type of emotional anguish will occur. The degree of dissonance will vary based on the individual's level of conviction and the extent of inconsistency between behavior and actions. Motivation to resolve the perceived dissonance increases proportionately to the degree of dissonance.
3. **Dissonance will be resolved in one of three basic ways:**
   - Change beliefs—Perhaps the simplest way to resolve dissonance between actions and beliefs is simply to change beliefs. Fortunately or unfortunately, individuals' basic beliefs and attitudes are fairly stable and are not likely to change easily unless they understand or perceive a reason for doing so. Although this option seems easy, it is infrequently embraced.
   - Change actions—A second option is cessation—never performing that action again. However, aversive conditioning (i.e., guilt/anxiety) often goes amiss. A problem with this option occurs when individuals rationalize away the negative feelings, thereby alleviating the need to change their actions.
   - Change perception of action—A third and more complex method of resolution is to change the way one views, remembers or perceives an action. That is to say, rationalization occurs. For example, auditees may justify stonewalling since an auditor is wasting their time anyway. Or they could say to themselves that everyone stonewalls the auditor, so why not us? By engaging in some mental gymnastics, auditees can reframe their actions in a different manner or context, so as to alter their views to align their beliefs with their actions. Such behavior is usually discernible on the part of others, yet difficult to detect in oneself.

SECURITY AWARENESS

A security awareness process that engages and educates the audit client can help better secure the organization's IT resources. A broad base of informed workers is a cost-effective way to mitigate security risks and better assist auditors. To change the audit client's negative perceptions, it is essential to have an understanding of behavioral patterns that are often at the core of misconceptions. An auditor should understand how audit clients:

- Internally develop a system for assigning meaning to the ostensibly unrestrained control wielded by the auditor
- Inadvertently distort their ability to understand and cooperatively facilitate the audit process due to their belief system
- Due to misunderstandings, may act or react with the auditor in detrimental and unproductive ways that further exacerbate miscommunication and often lead to rationalization and generalization, which, in turn, yield more resistance

The often ignored objective of an audit is to build a sense of security awareness one user at a time. In fact, studies show that when people understand why they are being asked to do something, they are more inclined to cooperate. A case in point: When zoo signage was replaced from, "Please stand three feet from the cage" to, "Animals spit," drastically different behavior was exemplified by the zoo patrons. Simply explaining why a safe standing distance was necessary had positive results. Prior to changing the signage, patrons would often be seen sitting or leaning over the safety rails, yet after understanding the reasoning behind the request, patrons stood well beyond three feet when viewing the animals.[5] Changing the thoughts or beliefs of the zoo patrons ultimately changed their actions—which supports the cognitive dissonance theory.

Auditing was originally designed as a didactic profession that tended toward documenting findings focused on the mistakes and the negative behavior or practices of others. Historically, auditors would show up unannounced, conveying an implied message of surprise or distrust to the audit client, with the perception being that an auditor's objective was to simply catch the auditee in the act of doing something wrong. Or, even worse, auditors would ask clients to make modifications or corrections because of some rule(s) without an adequate explanation.

To bring about security awareness, auditors must be willing to relinquish a measure of control, as they learn to facilitate risk reduction through effective communication. Once auditees are empowered to realize that they have the resources and authority to better safeguard the organization's information assets, their actions will respond accordingly. An essential part of developing security awareness is to engage the auditee and allow the auditor to experience a paradigm shift—where auditors begin to comprehend the problems they unintentionally create by their mere presence.

CONCLUSION

The social psychology of security auditing from the auditee's vantage point is paradoxical in that people are alike yet different. People are physiologically alike (eyes, ears, nose, mouth, mind, etc.) and share the same biological needs (air, water, food, clothing and shelter). Conversely, people are also uniquely different—emotionally, physically, mentally—with varying levels of motivation. Suffice it to say, maintaining a balance between treating everyone the same and being sensitive to individual differences is a challenge at best.

People bring their own perspective to the auditing process, which is colored by their predilections and predispositions. Auditors ought to realize on a human behavioral level that neither behaviors nor security conditions are static, with each constantly changing to meet the demands posed by new and changing security threats. Security perceptions are the predecessor to attitude formation and beliefs that subsequently shape security impression.[6] Understanding the cognitive dissonance principle and applying some of the fundamental social cognition constructs or audit awareness will help auditors avoid auditing dissonance, which could impair the objectivity, due diligence and professional care that are required by ISACA's professional ethics standards and best practices. The following summary is a listing based on well-established principles of social psychology. These tenets, in no particular order, identify ways an auditor can mitigate or avoid auditing dissonance by:[7]

- Participating in a security awareness effort, which includes many realistic examples of security requirements and breaches
- Endeavoring to inspire a commitment to security rather than merely describing it
- Emphasizing improvements rather than reduction of failure
- Listening with understanding for current security beliefs among employees and managers
- Never glorifying computer criminals with accolades or positive images and words
- Challenging employees who dismiss security concerns or flout security requirements; never ignoring such attitudes or beliefs
- Identifying senior executives most likely to succeed in setting a positive tone for subsequent security training
- Encouraging specific employees to take on public responsibility for information security within their work group
- Collaborating with management to build a culture that rewards responsible behavior such as reporting security violations
- Contributing to a working environment in which employees are respected. Explaining why IT security is important and the role each client plays in shoring up system security is more conducive to good security than operating in an environment that devalues and debases employees.
- Discussing security matters one on one with the participants, where possible, before calling a general meeting
- Remaining impartial and encouraging open debate during security meetings
- Bringing in outside experts as appropriate to counter groupthink and routinely playing devil's advocate (taking the opposing viewpoint) during security meetings

ENDNOTES

[1] ISACA, Code of Professional Ethics, *www.isaca.org*

[2] Lippa, Richard A.; *Introduction to Social Psychology*, Wadsworth, USA, 1990

[3] Schweitzer, Doug; "Security Lessons Learned—Employee Training and Education Can Mitigate Threats," *Processor Magazine*, vol. 27, issue 20, 20 May 2005, p. 1

[4] Festinger, Leon; *A Theory of Cognitive Dissonance*, Stanford University Press, USA, 1957

[5] Randolph, Alan; *Getting the Job Done! Managing Project Teams and Task Forces for Success*, Prentice Hall, USA, 1992

[6] *Op cit*, Lippa

[7] *Ibid*.