The SANS Technology Institute

A Bit of Psychology to Improve your Security Awareness Program

Information Security Awareness

Psychology Perspective

September, 2010
Ahmed Abdel-Aziz
CISSP, SANS GIAC

Table of Contents

ABSTRACT 3

PSYCHOLOGY & INFORMATION SECURITY AWARENESS 3

STEP-1: WHY PEOPLE BEHAVE THE WAY THEY DO 4

- ASSUMPTIONS, BELIEFS, AND VALUES (ABVS) 5
- PERCEPTIONS 5
- CONCLUSIONS 5
- FEELINGS 6
- BEHAVIOR 7

STEP-2: HOW TO INFLUENCE HUMAN BEHAVIOR TO IMPROVE SECURITY 7

- APPLYING THE APCFB MODEL TO SELF – I CHANGE MY OWN BEHAVIOR 7
- ABVS - OUR KEY TARGETS TO INFLUENCE BEHAVIOR 9
  - *Target 1: Assumptions 9*
  - *Target 2: Beliefs 11*
  - *Target3: Values 13*

CONCLUSION 14

REFERENCES 15

Abstract

The ultimate goal of a security awareness program is not to be security aware, but to change human behavior as needed (SANS, 2009). Psychology models have been developed to explain the cognitive process of linking external events to employee behavior (Silbiger, 2005).

The purpose of this paper is to use Psychology as a science to help us improve our security awareness programs. First, we will understand why people behave the way they do using one psychology model. Second, we will use that knowledge to help influence human behavior and achieve the ultimate goal of a security awareness program.

Psychology & Information Security Awareness

Psychology is commonly defined as the scientific study of human mental functions and behaviors. It can easily be argued that the science of Psychology has been around much longer than information security has. If we are dealing with people and targeting to change their behavior through security awareness programs, wouldn't it be useful to turn to the experts in human behavior for help?

Psychology being such a large field with vast amounts of research, this paper will focus on only two subfields of psychology to improve security awareness programs:

1- **Cognitive Psychology:** Studies the thinking underlying behavior. This includes perception, reasoning, and memory.
2- **Social Psychology:** Studies social behavior and mental processes. This includes the influence of others on an individual's behavior.

Understanding a bit of Psychology will definitely help in motivating people to do the right thing when it comes to **making security decisions**. That is because a change in one's awareness does not necessarily mean a change in one's behavior (Stewart, 2009).

Step-1: Why People Behave the Way they Do

To understand why people behave the way they do, we will use a Psychology model called the **APCFB** model *(Assumptions, Perceptions, Conclusions, Feelings, Behavior)* pictured below.

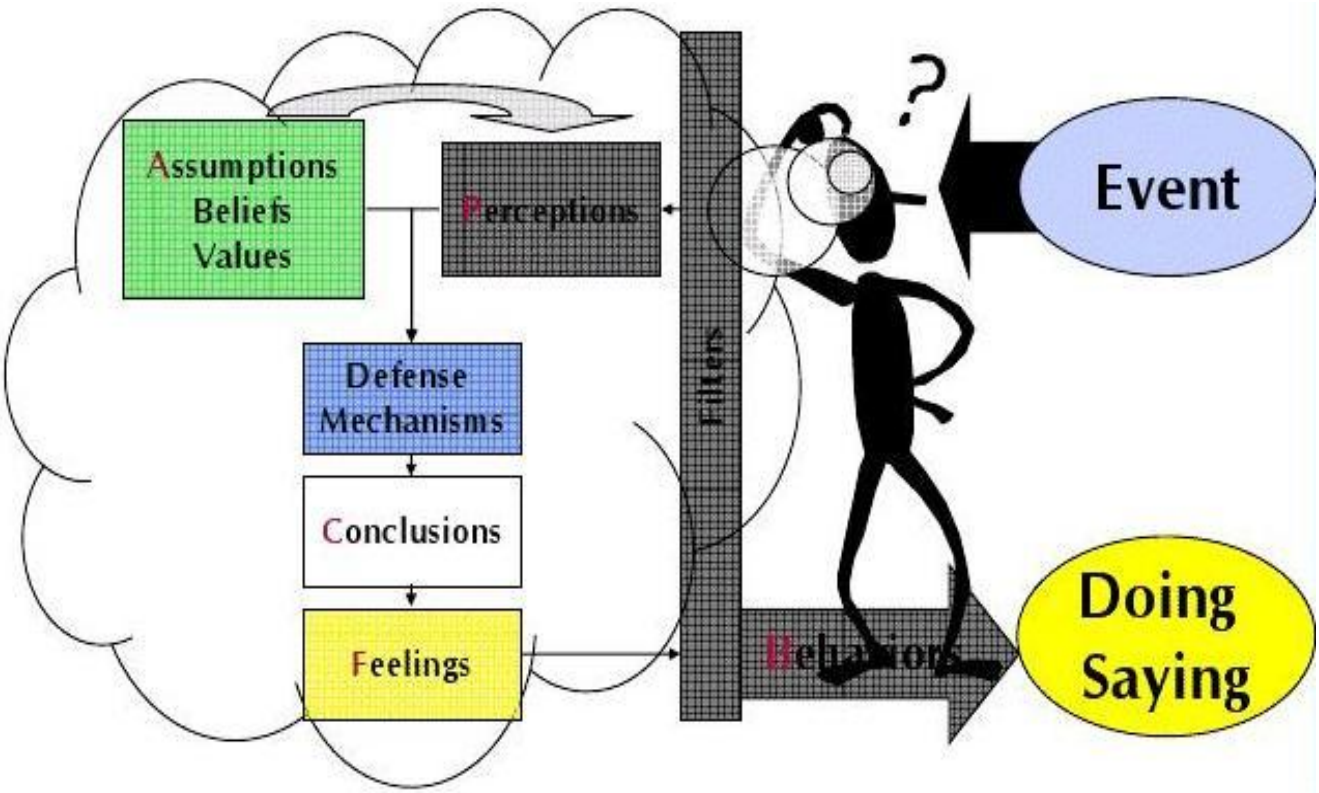

Figure 1: The APCFB Model (FocusBlog, 2010)

The work of psychologist Albert Ellis and other "rational emotive" researchers provides a foundation for a model that recognizes thoughts and feelings along with behavior (Clawson, 1991). The APCFB model is a form of Rational-Emotive-Behavior **(REB)** model and attempts to explain the cognitive process of linking external events to one's behavior (Silbiger, 2005).

Assumptions, beliefs, and values affect the ***perceptions*** people have. Those perceptions affect the ***conclusions***. And those conclusions prompt ***feelings***. Ultimately those feelings drive ***behaviors*** that others observe. Due to confounding forces within people, we all see through ***filters*** that often prevent us from perceiving

events accurately. Filters also prevent us from acting out our true desires. In addition, we all have ***internal defense mechanisms*** that act as additional filters to protect us from psychological damage.

Assumptions, Beliefs, and Values (ABVs)

ABVs are our personal set of assumptions, beliefs, and values about the way the world should be, or the way other people should behave. Our ABVs develop early and over many years. We learn them from our parents, our friends, our teachers, and our experiences. ABVs vary considerably from person to person. People have ABVs both about the way other people should behave *(the external view)*, and about the way they themselves should behave *(the internal view)*.

Some ABVs we hold strongly; some we exchange for others rather easily depending on the evidence and where we got them. Assumptions can be changed easier than Beliefs, which are easier to change than Values. Values are deeply held inside us and may be altered, if at all, only in time (Silbiger, 2005). Finally, our ABVs affect how we see events and so they influence our perceptions (Kabay, 1999).

Perceptions

Perceptions are a subset of what we observe; it is what is left to our awareness after we've filtered whatever it is that we filter out. What we perceive is a result of interplays between past experiences (our ABVs), and the interpretation of the perceived. For example, we observe a glass of water; we may perceive it as half full or half empty.

Conclusions

The key to understanding why people behave the way they do is in the comparison of what they see and what they believe ought to be, the comparison between one's perception and one's ABVs. It is this comparison we make that motivates our activity (Clawson, 1991).

Let′s consider a simple example. Suppose two security administrators learn a server has been compromised. One believes that, given his experience, he should not have a compromised server. He compares his perception of the event - server compromised - with what he believes, and realizes there is a gap. This gap is disturbing. He becomes angry and tries to keep the anger in, but has a hard time and the anger shows through body language and facial expressions. The second security administrator, on the other hand, compares his assumption *"Any server can get compromised, regardless of my experience in securing it"* with his perception of having a compromised server, and calmly follows the incident handling procedure and tries to understand why this happened. The event was the same but the behavior was not. The comparison of same event with different ABVs generated different experiencing and behavior.

When we see something, we immediately, in a nanosecond, compare it with our ABVs. If what we perceive matches our ABVs, then all is right with the world, and we move on; if there is a mismatch, then we have a problem. In any case, the comparison is done and a conclusion is reached. The conclusion represents the judgments we make about the situation, the people, or ourselves (Clawson, 1991). In our example, the conclusion reached by the first security administrator was **"I failed!!",** while the conclusion reached by the second security administrator was *"a security control must be missing"*.

Feelings

Our reached conclusions generate emotions. When our conclusions reflect a match between what we perceive and what we expect *(our ABVs)*, we usually experience the positive feelings – happiness, contentment, satisfaction, pride. When our perception violates our ABVs about others, or ourselves, we conclude that "things" or "we" are not "right", or we tend to experience the negative feelings – sadness, discontent, anger, jealousy, disappointment (Clawson, 1991). The first security administrator felt angry because his ABVs were contrary to the event.

Behavior

Our conclusions and our feelings shape our behavior, but our conclusions and feelings are based on our **ABVs**. Therefore, behavior is also based on our **ABVs**. If we ignore what lies behind people's behavior *(the Event←→ABVs comparison)*, we are ignoring a powerful tool for understanding and influencing people. This is a tool we can surely use to improve security awareness programs.

Trying to change human behavior to be security conscious by looking only at the behavior will not take us very far. What we need to do is to look at the target audience's ABVs, and focus our efforts there.

Step-2: How to Influence Human Behavior to Improve Security

In this section, we will leverage the knowledge gained from the previous section about the APCFB *(Assumptions, Perceptions, Conclusions, Feelings, Behavior)* model and move closer to our goal – Influencing human behavior to improve security.

Applying the APCFB Model to Self – I Change My Own Behavior

People have assumptions, beliefs, and values (ABVs) both about the way other people should behave *(the external view)* and about the way they themselves should behave *(the internal view)*. Humans have a unique ability to judge themselves. Not only can we observe the behavior of others, we can also observe our own behavior. We have developed assumptions, beliefs, and values that describe a "good" self. We may call this internal perspective of our ABVs the ***Ideal Self***. Our Ideal Self is our vision of how we "should" be. Like other ABVs, some parts of the Ideal Self are more important than other parts. The important parts we defend vigorously (Clawson, 1991).

We can call the perception we have about ourselves our ***Self Image***. We make self-judgments or conclusions, by comparing what we believe we should be with what we see ourselves doing. According to the APCFB model, these conclusions can affect our feelings and behavior. We may become so convinced that we are or are not

something that we stop trying to do anything differently. For example, we may assume that, "People who have good jobs must be well connected." If we are not well connected, then we may never exert an effort to find a good job and future – and this could be a significant loss for ourselves and for the community if we are talented. The illustration below describes the application of the APCFB model to the self. We can note that our own behavior is the ***Event*** and is the input to our ABVs comparison.

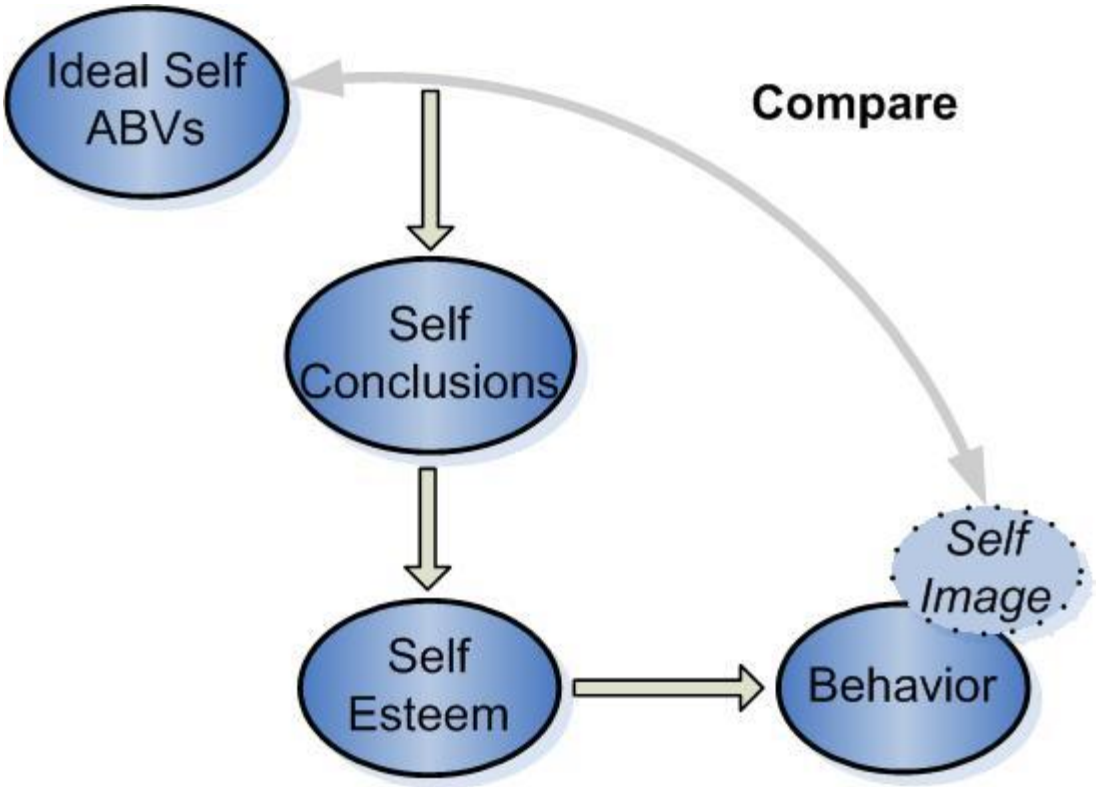

Figure 2: The APCFB Model Applied to One's Self (Clawson, 1991)

When there is a gap between our Ideal Self (self-oriented ABVs) and our Self Image, when we behave in ways that we don't think we should, we reach a negative conclusion about ourselves, and our feelings about ourselves, our Self Esteem, go down. The more our Self Image overlaps our Ideal Self, the better we feel about ourselves. The more distant our Self Image is from our Ideal Self, the worse we are likely to feel about ourselves. In the end, we all want to conclude positive things about ourselves and feel good about ourselves; this is a fundamental human

motivation (Clawson, 1991). Therefore, we can assume that ***we*** tend to change ***our own*** behavior so that our Self Image moves closer to our Ideal Self.

ABVs - Our Key Targets to Influence Behavior

The premise of this paper for influencing behavior is to influence the Ideal Self to become security friendly. This will eventually lead to people changing their own behavior to move their Self Image closer to their Ideal Self. By changing their behavior, they are following the fundamental human motivation – concluding positive things about themselves and feeling better.

Therefore, our key targets to influence the audience behavior are:

1- Their Assumptions
2- Their Beliefs
3- Their Values

Target 1: Assumptions

Assumptions in this paper constitute the set of opinions and knowledge that one has acquired over time. These assumptions may include erroneous knowledge that a person considers as facts. According to Silbiger (Silbiger, 2005), assumptions are the easiest to change in one's set of ABVs. Typical security awareness programs will be targeting the audience's assumptions, and making people security "aware". An example of targeting assumptions would be teaching the audience to exercise safer social networking. After learning, the audience changes their assumptions to:

- *Personal information and photos displayed are available to everyone and anyone, not just my friends*
- *I should not list my full birth date because I will become an easy target for identity thieves.*
- *I should not mention being away from home, because it's like putting a "Nobody's Home" sign on my front door.*
- *I should have an up-to-date web browser and comprehensive security software on my computer.*
- *Etc.*

The NIST Special Publication 800-50 (Wilson, & Hash, 2003) can be used to help build an IT security awareness program to address assumptions.

To more effectively target the assumptions component of ABVs, we will need to consider the following psychology factors:

- The perceived risk level by someone is not necessarily the same as the actual risk level
- Certain attributes impact human perception of risk (Stewart, 2009):
    - **Observable or not** (we fear invisible threats more than the visible)
    - **Defined or not** (we tend to exaggerate risk when there is uncertainty)
    - **Old or not** (we have a greater fear of new risks, think Swine Flu)
    - **Familiar or not** (we perceive familiar items as less risky)
    - **Chronic or acute** (we fear acute conditions, but chronic is more lethal)
    - **Controlled by us or not** (we tend to trust ourselves more than others)
- We build mental shortcuts called heuristics to come to solutions quickly. Heuristics are simply rules-of-thumb and lead to cognitive biases. Although useful, inaccurate heuristics and biases lead to dangerous risk assessments. Some security-related biases follow (Sternberg, 2010):
    - **Loss aversion** (we prefer a sure small gain over risky larger gain; and prefer a risky larger loss over a sure small loss)
    - **Optimism bias** (we tend to overestimate the likelihood of positive events and underestimate likelihood of negative events. *"It won't happen to me"* philosophy)

  Some security-related heuristics follow (Stewart, 2009):
    - **Availability heuristic** (we tend to assess likelihood of event by how recent it is or how easy we can imagine it)
    - **Affect heuristic** (we tend to have a lower risk perception of a situation if it is tied to a positive effect – good feeling: thrill, pleasure, etc.)

When considering these psychology factors, we recognize why our audience's risk perception may be different than what we expected, and we can better predict future risk perceptions. This enables us to adjust our effort when communicating risk to

have the perceived risk aligned with the actual risk. For example, to compensate for the availability & affect heuristics, a threat that is hard for people to imagine and tied to a situation with a positive affect, will require that we provide the audience with real-life examples of the threat in action, and emphasizing the negative feelings associated with the experience. When the perceived and actual risk levels are aligned, people will make better security decisions (Schneier, 2008), which will have a positive influence on people behavior. However, people behavior is not that simple. Just because someone has been educated about the dangers of smoking, and had their assumptions rightfully tuned, doesn't mean they will actually stop smoking *(change behavior)*. That's why we move into targeting a deeper part of the ABVs – Beliefs.

Target 2: Beliefs

Beliefs are deeper and more complex than our first target – assumptions. A belief is more difficult to change than an assumption in one's set of ABVs. In this paper, a belief is the sum of assumptions about something; a belief forms an **attitude**. For example, one might have the following assumptions: *exercise is good for my health; exercise makes me look good; exercise takes too much time; exercise is tiring.* The sum of these assumptions lead to the belief: *I should exercise, or I should not exercise.*

According to Samuel W. Chun (Chun, 2007), the field of **social psychology** offers us subtle, unconscious ways to influence people's beliefs. We will cover some influence methods based on well-known phenomena in the science of influence.

Reciprocity:

The obligation to reciprocate on debt has been observed by scientists in every culture on Earth. Social psychologists have discovered that people's ingrained sense of indebtedness can be exploited so that uneasy feelings of debt can be induced. What is interesting is that a small favor can produce a sense of obligation to return a much bigger favor. By offering inexpensive "favors" or "gifts" as part of the security awareness program, we can elicit indebtedness in audience. This may

play a role in the audience deciding to take the security awareness program seriously (Chun, 2007).

Self-Persuasion:

Social psychology research has found that one of the most effective methods to achieve a change in an individual′s belief or attitude is to have the individual play a role contrary to their belief. For example, having a security reluctant individual adopt the role of an information security specialist, and then be asked to justify security policy and the security awareness initiative. The individual will be holding conflicting ideas simultaneously *(role-play & belief)* causing an uncomfortable feeling. In Psychology this state is called cognitive dissonance and acts as a stimulus to change their belief (Corona, 2009).

Individualization:

People behave differently based on the perception of being part of a group as opposed to being an individual. We tend to feel less responsibility in a group than as a single individual. Psychologists call this diffusion of responsibility and it is observed across all cultures. The idea of individualization is to remind people of themselves via visual stimuli or self-observation. When individualization is perceived, people tend to be more honest, take more responsibility, and take the security program more seriously. Individuality can be encouraged through small investments such as name plates, name tags, customized workspaces, and maybe mirrors (Chun, 2007).

Social Proof:

Group interaction tends to polarize attitudes on a given subject rather than moderate it. We use actions of others as important guidelines in our own behavior. We do this because early in life we learn that doing as "others do" is more likely than not the right behavior. When others can observe positive attitudes toward aspects of a security awareness program, social proof can serve as a multiplier in encouraging positive behavior & beliefs. On the other hand, negative beliefs toward security awareness can quickly spread, especially in confined environments. Senior management and security managers need to quickly deal with those who set bad examples, and to encourage and promote those who take security policy seriously

(Chun, 2007). In addition, the security beliefs and behavior of management, in specific, will definitely influence others' beliefs.

Familiarity & Repeated Exposure:

Scientists have found overwhelming evidence that repeated exposure to stimuli almost always results in positive belief or attitude change. Even in the face of audience dissatisfaction, repeated exposure to the policies and rationales for the security awareness program is essential for changing audience beliefs. The most common mistake observed with a security awareness program is its inconsistency. A security awareness program designed with consistency and longevity in mind *(regular E-reminders, management announcements, etc.)* will have a better chance of changing the beliefs of audience to adopt the security awareness program (Chun, 2007).

Target3: Values

Values are the deepest of our set of ABVs. The approach for targeting values is different than that of assumptions or beliefs because values may be altered, if at all, only in time (Silbiger, 2005). While we attempted to influence assumptions and beliefs, we will not even attempt to do so for values. The logical approach to target values is to ***highlight*** in the security awareness program how following the security policy is in congruence with the audience values.

Silbiger (Silbiger, 2005) suggests that when a manager is able to tap into the values of subordinates, then real productivity results, and the desired behavior is produced. The same concept can be applied for security awareness programs. For us to tap into the audience's values, we need to identify them first. The audience will likely have some common values, which are the organization's values; organization values can be found in the organization's Code of Conduct. Another method to identify common audience values is to use simple exercises created by human development specialists (Mocke, 2010). As an example, if "**creative expression**" & "**exercising competence**" are two identified values for our audience, we can highlight in our awareness program that security policy allows ***responsible use*** of

social networking sites. That way the audience recognizes that their values are congruent to the security policy. By helping the audience link their values to the behavior expected from them, they become more motivated to follow security policy.

Conclusion

The objective of this paper was to tap into the enormous field of Psychology to improve our security awareness programs. This was achieved through two steps. First, using the APCFB Psychology model to understand why people behave the way they do. Second, apply the model to one's self and using a bit of Psychology to induce the needed behavior. In this paper, we saw why information security awareness can really benefit from the Psychology discipline, especially the Cognitive and Social Psychology sub-fields. Our assumptions, beliefs, and values *(ABVs)* dictate the judgments we will make in response to events; ABVs will also dictate how we feel, and consequently how we will behave in response to those events. We experience positive feelings when our Self Image is aligned with our Ideal Self and negative feelings when they are far apart. By targeting the Ideal Self to be security friendly, we are influencing people to make better security decisions and behave as needed. We target the Ideal Self by targeting people's **assumptions, beliefs, and values**. Risk perception, heuristics, and cognitive biases help us in better influencing assumptions; while Social Psychology helps us in better influencing beliefs. As for values, we are better off leveraging them, rather than influencing them in our security awareness program.

When we consider that Psychology overlaps with many other fields *(Medicine, Biology, Computer Science, etc.)*, it is no surprise that **a bit of Psychology can improve our security awareness programs**.

References

[1] Silbiger, S.(2005). *The 10-Day MBA, A Step-by-Step Guide to Mastering the Skills Taught in Top Business Schools*. London, UK: Piatkus Books

[2] Stewart, G.(2009). *Maximizing the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles*. Egham, England: Department of Mathematics, Royal Holloway, University of London

[3] Clawson, J.(1991). *Why People Behave the Way they Do*. Virginia, US: Darden Business Publishing, University of Virginia

[4] SANS (2009). *How to Establish a Security Awareness Program.* SANS.

[5] Psychology. (2010). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved August 10, 2010, from http://en.wikipedia.org/wiki/Psychology

[6] FocusBlog. (2010, May 30). In cautarea adevarului. documentarea in jurnalism (ii) [Web log message]. Retrieved from http://www.focusblog.ro/2010/05/in-cautarea-adevarului-documentarea-in-jurnalism-ii/

[7] Ellis, A., Harper, R.(1997). *A Guide to Rational Living*. Hollywood, CA: Melvin Powers Wilshire Book Company

[8] Kabay, M.E. (1999). Using Social Psychology to Implement Security Policies. In H. Tipton, M. Krause (Ed.), *Computer Security Handbook, 4th Edition* (pp. 35-1-35-22). USA: Auerbach Publications.

[9] Sternberg, G. (2010). The Psychology Behind Security. *ISSA Journal*, Retrieved from http://www.issa.org/images/upload/files/SternbergPsychology%20Behind%20Security.pdf

[10] Schneier, B. (2008, January 18). *The Psychology of Security*. Retrieved from http://www.schneier.com/essay-155.html

[11] Perception. (2010). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved August 14, 2010, from http://en.wikipedia.org/wiki/Psychology

[12] Chun, S.W. (2007). Change That Attitude: The ABCs of a Persuasive Security Awareness Program, In H. Tipton, M. Krause (Ed.), *Information Security Management Handbook, Sixth Edition* (pp. 521-530). CRC Press

[13] Wilson, M., Hash, J. U.S. Department of Commerce, National Institute of Standards &

Technology. (2003). *Building an Information Technology Security Awareness and Training Program* (Special Publication 800- 50). Gaithersburg, MD

[14] Heuristic. (2010). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved August 17, 2010, from http://en.wikipedia.org/wiki/Heuristic

[15] Theory of Reasoned Action. (2010). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved August 19, 2010, from http://en.wikipedia.org/wiki/Theory_of_reasoned_action

[16] Corona, C.(2009). *Information Security Awareness: An Innovation Approach*. Egham, England: Department of Mathematics, Royal Holloway, University of London

[17] Mocke, D. (2010). Determine Your Personal Values. Sustainable Employee Motivation. Retrieved from http://www.sustainable-employee-motivation.com/personal-values.html