Institute for Homeland Security Solutions

Applied research • Focused results

# One Size Doesn't Fit All: Cybersecurity Training Should Be Customized

September 2012


Authors

Maranda McBride, PhD, North Carolina A&T State University

Lemuria Carter, PhD, North Carolina A&T State University

Merrill Warkentin, PhD, Mississippi State University

## Introduction

Insider abuse, which occurs when employees violate cybersecurity policies, is frequently identified as the greatest single source of threat to organizational information systems (IS) security. Technical controls are ineffective at preventing motivated insiders from performing various forms of insider abuse, thus organizations utilize a range of behavioral controls, including security education, training, and awareness (SETA) programs; IS security procedure reminders; and punishments (i.e., sanctions) for IS security violations. In our study, we identify individual personality traits that influence employees' intention to violate cybersecurity policy. We develop and test a comprehensive model of cybersecurity violation intention that includes personality, deterrence, and protection motivation factors on non-compliance among employees.

## Individual Differences and Cybersecurity Compliance

Personality differences can be used to establish cybersecurity training modules by first identifying significant relationships between individual personality dimensions and policy violation intention motivations. These relationships can then be used to establish guidelines for developing various cybersecurity protocols customized to meet the unique needs of diverse employees.

A common personality assessment is the "Big Five" personality test, also referred to as OCEAN (Buchanan et al., 2005; Karim et al., 2009; Landers & Lounsbury, 2006). This test includes five personality traits: **O**penness, **C**onscientiousness, **E**xtraversion, **A**greeableness, and **N**euroticism. Openness refers to characteristics such as open-mindedness and independence of judgment. Conscientiousness relates to trustworthiness and a sense of responsibility. Extraversion refers to the sociable and assertive nature of a person. Agreeableness is a trait common among people who tend to be tolerant, trusting, and accepting. Finally, neuroticism describes people who are emotionally unstable and have low self-esteem.

In addition to personality traits, we also explore the role of sanctions on non-compliance. Deterrence theory suggests that individuals will be discouraged from performing undesirable behavior (e.g., computer abuse, policy violation) if they believe they will be punished (i.e., sanctioned) and these punishments are certain, severe, and swift. However, such deterrence affects individuals differently due to their relative morality and rationality. The effective application of deterrence controls presumes that individuals consider the benefits of a policy violation (e.g., convenience of temporarily leaving a workstation without logging off or selecting a weak password that is easy to remember) and the costs of such violations (e.g., perceived

sanction certainty, severity, and swiftness), and make a rational choice to engage in noncompliant or criminal behavior. Therefore, SETA programs can inform employees about sanctions, but individuals will cognitively process that information in unique ways.

Finally, we assess employees' inherent nature to protect themselves from threats. Protection motivation theory (PMT) suggests that when individuals perceive that they are more vulnerable to security threats (e.g., malware or hard drive crashes) and when threats are more severe, they are more likely to adopt a recommended response to the threat (e.g., scanning for malware or backing up data), as long as the individual employee possesses sufficient self-efficacy (i.e., confidence in their ability to perform the recommended response) and perceived efficacy (i.e., effectiveness of the response itself), both of which can be influenced.

## Results of an Empirical Research Project

To test the impact of these individual factors on non-compliance, we conducted a scientific study in which we administered an online survey to 150 individuals who have held a job that requires the use of a computer and adherence to security procedures. A few of the key findings are summarized in **Error! Reference source not found.**.

To illustrate the application of these findings, we provide a discussion of one bulleted point from each side of the table. For example, one of the findings from Table 1 indicates that extroverted individuals with a low sense of sanction severity are less likely to violate cyber security policies. Now that we have empirically established this relationship, future scholars can develop a training protocol that is framed in such a way that it will have more impact on individuals with a low sense of sanction severity. For instance, extroverted individuals with a low sense of sanction severity are not motivated by punishments (such as a receiving a negative evaluation or losing their job). Hence, training for these individuals could de-emphasize sanctions as a part of the training program.

With regards to those individuals who are more likely to violate policy, one of our findings indicates that agreeable individuals with a low sense of sanction certainty are more likely to violate cybersecurity policies. Simply being an agreeable individual doesn't necessarily mean that you more or less likely to violate a cybersecurity policy. However, our research indicates that agreeable individuals who feel that sanctions may not be likely are more likely to violate cybersecurity policies even when they are equipped with the knowledge that punishments will be enforced. Hence, training protocols for these individuals might focus on the impact of other situational factors instead of sanctions. Perhaps, training protocols which leverage appeals to threat severity will be more effective.

**Table 1: Effects of Big Five Traits on Deterrence Theory, PMT, and Efficacy Factors**

| Individuals who are less likely to violate cybersecurity protocol | Individuals who are more likely to violate cybersecurity protocol |
|---|---|
| • Open individuals with a low sense of Self-Efficacy<br>• Open individuals with a low sense of Threat Severity<br>• Open individuals with a low sense of Response Cost<br>• Conscientious individuals with a low sense of Threat Severity<br>• *Extroverted individuals with a low sense of Sanction Severity*<br>• Agreeable individuals with a low sense of Self-Efficacy<br>• Agreeable individuals with a low sense of Sanction Severity<br>• Neurotic individuals with a low sense of Self-Efficacy<br>• Neurotic individuals with a low sense of Sanction Severity | • Open individuals with a low sense of Sanction Severity<br>• Conscientious individuals with a low sense of Response Efficacy<br>• Extroverted individuals with a low sense of Threat Severity<br>• Extroverted individuals with a low sense of Threat Vulnerability<br>• Extroverted individuals with a low sense of Response Cost<br>• *Agreeable individuals with a low sense of Sanction Certainty*<br>• Neurotic individuals with a low sense of Sanction Certainty |

## Conclusions

The results of this study confirm that individuals react differently to the same conditions and imply that the approach we adopt to cybersecurity training must also differentiate between individual employee personality types. This study represents an initial step to integrate the impact of the Big Five factors with perceptions of threats and sanctions to see how they work together to promote cybersecurity compliance. However, additional research is needed to develop the appropriate set of training protocols and the appropriate framing for each employee profile. The purpose of this study is to establish a foundation for which these protocols can be developed. This study highlights the need for future research to develop customized training protocols that incorporate the interrelations between the Big Five personality factors and individual perceptions of security threats and organizational sanctions.

## References

Buchanan T, Johnson JA, Goldberg LR. (2005). Implementing a five-factor personality inventory for use on the internet. European Journal of Psychological Assessment. 21(2):115-27.

Karim NSA, Zamzuri NHA, Nor YM. (2009). Exploring the relationship between Internet ethics in university students and the Big Five model of personality. Computers & Education. 53(1):86-93.

Landers RN, Lounsbury JW. (2006). An investigation of Big Five and narrow personality traits in relation to Internet usage. Computers in Human Behavior. 22(2):283-93.