Resiliency as an Outcome of SETA Programs

Emergent Research Forum (ERF) Paper

Angela Denise Landress
Nova Southeastern University
landress@nova.edu

James Parrish
Nova Southeastern University
jlparrish@nova.edu

Steven Terrell
Nova Southeastern University
terrell@nova.edu

Abstract

The authors seek to understand the relationship between the outcomes of traditional Security Education Training & Awareness (SETA) programs, which have been popular in Information Systems (IS) as a mechanism to protect users from cybercrime. The issue is that most SETA programs in IS change at the pace much slower than the pace of cybercriminal tactics. Therefore, the authors propose viewing SETA outcomes through the lens of the psychological concept of resiliency. This paper proposes a model that extends reputable resiliency theories and models to the field of IS Security.

Keywords

Security training, Security Awareness, Resiliency, SETA

Introduction

While much research has been performed in the area of Security Education Training & Awareness (SETA) programs and their impact on information systems (IS) security, the number and severity of security breaches continues to rise. This could be, in part, due to the relatively low educational objectives that most SETA programs achieve in their efforts to protect individuals in a complex and ever-changing threat landscape.

The focus of this paper is to that examines the goals of SETA programs in terms of the resiliency of an individual to reintegrate post attack by developing a theoretical model that examines the various outcomes an individual can achieve. These outcomes obtained through extending Richardson's (2002) resiliency model in the Journal of Clinical Psychology to the field of IS, will relate to an individual's outcome when an attack on a user of IS occurs. The authors postulate that if their model is applied, future researchers will be able to view the design of future SETA programs which have historically been focused primarily on the awareness of users without considering the ability for their employees to be resilient enough to avoid attacks, and/or reintegrate post attack.

Literature Review

Richardson (2002) proposed three waves of resiliency inquiry that explains the components of the resilience theory postulated by Richardson et al (1990). The first wave describes resilient qualities one must possess to rebound from adversity. The second wave describes the resiliency process of coping with challenges and coming out of it with improved protective factors. It also accounts for reintegration, which is a person's ability to back into either the same situational mindset, or an improved one, after a loss. The

third wave is innate resilience, which serves to identify an individual's motives and experiences that cause the utilization of resilient forces. Richardson (2002) cites resilient qualities from a phenomenological perspective. The foundational premise of resiliency is that people possess, either by nature or experience, selective qualities that help them survive adverse situations. The qualities are defined as protective factors. Foundational studies of resiliency were originally conducted to study youth survival behaviors (Werner & Smith 1992; Rutter 1979, 1985; Garmezy et al 1984; Benson 1997). All of these studies found that children of various ages displayed resiliency when being faced with extreme harsh circumstances more than 25% of the time. Resiliency has also been cited in psychological studies as well. Over the last decade, psychological resilient characteristics include happiness, subjective well-being, optimism, faith, self-determination, wisdom, excellence, creativity, morality, self-control, gratitude, forgiveness, hopes, dreams, and humility (Seligman & Csikszentmihalyi 2000; Buss 2000; Diener 2000; Peterson 2000; Ryan & Deci 2000; Schwartz 2000; Baltes & Staudinger 2000; Lubinski & Benbow 2000; McCullough & Snider 2000; Baumeister & Exline 2000; Emmons & Crumpler 2000; Tangney 2000).

Richardson's (2002) second wave describes how people lose something then reintegrate, causing them to learn resiliency. He describes the process of the second wave as homeostasis, life experiences, disruption of those experiences, being ready to reintegrate after disruption, then implementing reintegration behavior. To simplify, in order to cope with life, people learn resilient behaviors over time to try to create a life that is balanced and as routine as possible. It's the disruption that leads one to reflect on how to prevent that disruption, or react better to a similar future disruption. He proposes a resiliency model to this effect. This second wave describes learned behaviors that humans adapt over time with various experiences.

The third wave relates most to natural characteristics that are derived from within a person. Many psychologists have argued that resilience is a force within people that urges them to right their paths after they face adversity (Werner & Smith 1992). The focus of this paper is on the second wave, as opposed to the resilience metatheory, which is the basis of the third wave (Wilber 1996).

Theoretical Model

The conceptual model below shows the linkage between Richardson's (2002) resiliency theory and the typical outcomes related to an attack from a cybercriminal.

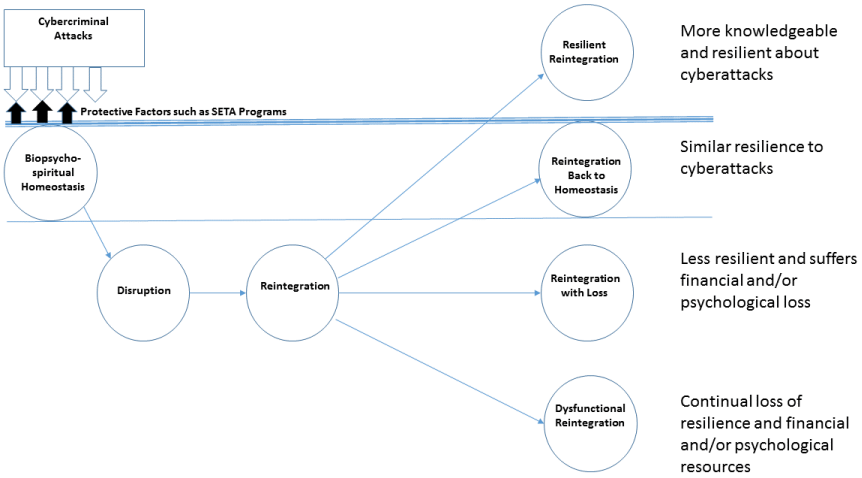

Figure 1: Conceptual Model

The conceptual model above starts with a user in a status of homeostasis. In the context of this paper, this assumes that the user has undergone a standard SETA process. This process, in part, provides the protective mechanisms depicted in the model. Once a user is exposed to the threat of an attack by a cybercriminal, they are disrupted and faced with four options in which to reintegrate:

1. Resilient Reintegration – The user does not fall prey to the attack and gains increased knowledge about future attacks.
2. Return to Homeostasis – The user does not fall prey to the attack.
3. Reintegration with Some Loss – The user may fall prey to the attack and experience some psychological or financial loss.
4. Dysfunctional Reintegration – The user falls prey to the attack and the cybercriminal has them engage in dysfunctional behaviors.

Perhaps an example would better describe the types of reintegration behaviors depicted in the model. Let's imagine that there is a user that has their homeostasis disrupted through receipt of a new type of phishing email that has made it past their organization's spam filter. The user then will engage in one of the four integration outcomes stated above. If they reintegrate resiliently, then they will not fall prey to the email and possibly engage in some activity to increase their knowledge of this type of attack. Thus, making them more resilient to it in the future. A second outcome is that they could just delete the email without learning more about the changes in cybercriminal tactic that this new type of email employs. The third type of reintegration would have them fall prey to the attack and suffer some sort of loss in the form of some sum of financial currency or a loss of self-esteem or computer self-efficacy. The final, and most detrimental option would involve the user engaging in continuous loss of financial resources or psychological well-being to avoid having the fact that they have fallen prey to the cybercriminal known, to avoid embarrassment, feeling like they have already invested too much to go back, or even having the belief that they will eventually come out on the positive end of the exchange. This is seen many times when users are tricked into believing that if they keep paying for bogus charges created by the cybercriminal they will receive some large sum of currency in return or that the malware on their computer is more difficult to remove than the "support technician" first perceived.

Regardless, the authors feel that this lens provides a more accurate view of the outcomes of an attack by a cybercriminal and therefore could be used to improve SETA programs. IS industry leaders in security training require the following objectives to be in place for their standard user-based security training programs. It must address the security threat environment, while reinforcing the business culture of the organization it supports. They state that the biggest risk is not the implementation of the technology, rather the lack of awareness of those who use it. They believe if the employees understand the risks to the business and the potential consequences of their action or inaction, they will change their security behavior (PCI Security Standards Council 2014). However, Proctor (2016) states that traditional SETA training is ineffective in today's fast-paced IT environment. While these programs have been implemented, institutionalized, and standardized, the rate of attack has increased. By proposing to change the way users are trained, the authors believe the rate of security incidents will decrease, while the resilient and mindful characteristics of the employee will increase. The following graphic displays what aspects of the model apply to the basic tenets of SETA.

Basic Tenants of Security Awareness Training	**Resiliency Characteristics**
Facilitates the concepts of confidentiality, integrity, and availability	Second Wave
Apply Defense in Depth Concept	Second Wave
Assess the Audience's Needs	First, Second, Third Wave
Classify the Training Audience by Role	First, Second, Third Wave
Enforcing Awareness Behaviors	First Wave

Table 1: Training, Resiliency, Mindfulness Mapping

Conclusions and Future Work

The authors postulate that if security trainers seek to increase resiliency as an augmentation to traditional security awareness training, the rates of attacks by cybercriminals will decrease in both number and severity. Future work in this area will look to create a new model for security training which incorporates Langer's (1989) notion of mindfulness as an enhancement to the protective mechanisms provided by the SETA program.

When facilitating concepts of confidentiality, integrity, and availability (CIA), the training program should be augmented by employing the resiliency characteristics of Richardson's (2002) second wave, which describes people who learn resilient behaviors to cope with life. It's the disruption that leads one to reflect on how to prevent that disruption, or react better to a similar future disruption. In the case of CIA, it's important to teach employees how to maintain a system's or an organization's confidentiality, integrity, and availability both before and after an attack. It's even more important to teach employees how to employ mindfulness and recover and reintegrate from an attack and maintain CIA (National Security Agency, 2001). Employees should also be trained how to learn new things and generate new information about their environment, which aligns with Langer's (1989) four dimensions of mindful thinking.

Applying the outer core of the defense in depth concept, which targets the human aspects of defense (Proctor 2016), is another valued component of typical security awareness training programs. Defense in Depth was developed by the National Security Agency as a method to employ security layering. The first part of the layer involves many aspects of human behavior. Augmenting training programs by educating employees on resilient behaviors from Richardson's (2002) methodology, and exposing them to simulated attacks, while also teaching novelty-seeking, novelty-producing, and engagement behaviors from Langer's (1989) study has the potential to significantly increase one's ability to avoid attacks and recover quickly from real ones.

REFERENCES

Baltes, P., and Staudinger, U. 2000. "Wisdom: A metaheuristic (pragmatic) to orchestrate mind and virtue toward excellence," in *American Psychologist,* (14:4), pp. 122-136.

Baumeister, G., and Exline, J. 2000. "Self-control, morality, and human strength," in *Journal of Social and Clinical Psychology,* (19:1), pp. 29-42.

Benson, P. L. 1997. *All kids are our kids*. Minneapolis; Search Institute.

Buss, M. 2000. "The evolution of happiness," in *American Psychologist*, (55:1), pp. 15-23.

Diener, E., Suh, E. M., Lucas, R. E., and Smith, H. L. 2000. "Subjective well-being: three decades of progress," in *Psychological Bulletin,* (125), pp. 276-302.

Emmons, R., and Crumpler, C. (2000). "Gratitude as a human strength: Appraising the Evidence," in *Journal of Social and Clinical Psychology,* (19:1), pp. 56-69.

Garmezy, N., Masten, A. S., and Tellegen, A. 1984. "The study of stress and competence in children: A building block for developmental psychopathology," *Child Development*. (55), pp. 97-111.

Kell, H., Lubinski, D., and Benbow, C. 2000. "Who rises to the top? Early indicators," in *Association for Psychological Science.* (24:5), pp. 618-659.

Langer, Ellen J. 1989. *Mindfulness.* Reading, MA: Addison Wesley.

McCullough, M. E., and Snyder, C. R. 2000. "Classical sources of human strength: Revisiting an old home and rebuilding a new one," in *Journal of Social and Clinical Psychology,* (19:1), pp. 1-10.

National Security Agency. 2001, June 8. *Defense in Depth*. Retrieved from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Proctor, W. R. 2016. "Investigating the efficacy of cybersecurity awareness training programs," in *ProQuest Dissertations & Theses Global*. (1789299787). Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1789299787?accountid=6579

Richardson, G. E., Neiger, B. L., Jensen, S., and Kumper, K. L. 1990. The Resiliency Model. *Health Education*. (21:6), pp. 33-39.

Richardson, G. E. 2002. "The metatheory of resilience and resiliency," in *Journal of Clinical Psychology,* (58:3), pp. 307-321.

Rutter, M. 1979. "Protective factors in children's responses to stress and disadvantages," In Kent, M. W., Rolf, J. E., eds. *Primary Prevention of Psychopathology*, *Vol III Social Competence in Children*. Hanover, N.H.; University Press of New England, 49-74.

Rutter, M. 1985. "Resilience in the face of adversity: Protective factors and resistance to psychiatric disorder," *British Journal of Psychiatry*, (147), pp. 598-611.

Ryan, R. M., Deci. 2000. "Self determination theory and the facilitation of instrinsic motivation, social development, and well-being," in American Psychologist, (55:1), pp. 68-78.

Schwartz, M. 2000. "RSA SecurID Breach Cost $66 Million. Information Week." Retrieved from http://www.darkreading.com/attacks-and-breaches/rsa-securid-breach-cost-$66-million/d/d-id/1099232?

The Security Awareness Program Special Interest Group PCI Security Standards Council. 2014. *Best Practices for Implementing a Security Awareness Program*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Werner, E., Smith, R. 1992. *Overcoming the odds: High risk children from birth to adulthood*. Ithaca: Cornell University Press.