Chapter 74
The Role of Human Operators' Suspicion in the Detection of Cyber Attacks

Leanne Hirshfield
Syracuse University, USA

Gregory J. Funke
Air Force Research Laboratory, USA

Philip Bobko
Gettysburg College, USA

Vincent F. Mancuso
MIT Lincoln Laboratory, USA

Alex J. Barelka
Illinois State University, USA

Victor Finomore
Wright-Patterson Air Force Base, USA

Mark R. Costa
Syracuse University, USA

Benjamin A. Knott
Air Force Office of Scientific Research, USA

ABSTRACT

Despite the importance that human error in the cyber domain has had in recent reports, cyber warfare research to date has largely focused on the effects of cyber attacks on the target computer system. In contrast, there is little empirical work on the role of human operators during cyber breaches. More specifically, there is a need to understand the human-level factors at play when attacks occur. This paper views cyber attacks through the lens of suspicion, a construct that has been used in other contexts, but inadequately defined, in prior research. After defining the construct of suspicion, the authors demonstrate the role that suspicion plays as the conduit between computer operators' normal working behaviors and their ability to alter that behavior to detect and react to cyber attacks. With a focus on the user, rather than the target computer, the authors empirically develop a latent structure for a variety of types of cyber attacks, link that structure to levels of operator suspicion, link suspicion to users' cognitive and emotional states, and develop initial implications for cyber training.

DOI: 10.4018/978-1-5225-8897-9.ch074

INTRODUCTION

Cyber security is currently a high-ranking national security issue – a statement supported by recent congressional testimony noting that the United States saw a 782% increase in the number of reported cyber attacks against federal agencies from 2006 to 2012 (GAO-13-462T). Regarding potential *causes* of security breaches, the Ponemon Institute (Ponemon Institute 2013) suggested that 64 percent of data breaches in 2012 were the result of human error and problems in the ways that systems were constructed by humans (improperly configuring software that resulted in inadvertent data dumps, logic errors in data transfer, etc.). In a recent report by IBM that looked at common cyber attacks across 3,700 IBM clients in 130 countries, it was found that in most cases humans were the primary reason the breach occurred and humans were labeled as the 'weak links' in cyber networks (IBM 2013). The report also noted that cyber threats are becoming more opportunistic as human fallibility is exploited (IBM 2013), and the analysis suggested that human errors account for approximately 80 percent of company breaches.

With the exception of research studies devoted to cyber security training in specific settings (Abawajy 2012, Camp 2009, Jansson and von Solms 2013, Sheng et al. 2007), to the authors' knowledge there is little empirical work exploring, articulating, or measuring the role of human operators during cyber breaches. The need for such empirical work has been the topic of several recent cyber research articles (Bowen et al. 2012, Boyce et al. 2011, Knott et al. 2013). More specifically, there is a need to understand the human-level trait and state factors at play when cyber attacks occur. To address this gap, the current paper views cyber attacks through the lens of suspicion. In order to reduce the human errors described above, computer users must learn to properly transition from normal working behavior to behavior under cyber attack (e.g., call IT, run antivirus software) at appropriate times. We hypothesize that suspicion plays an integral role as the conduit between these normal working behaviors and behaviors associated with detecting and appropriately reacting to a cyber attack.

This paper makes several contributions to the cyber security domain. We (i) describe and explore how the construct of suspicion operates during cyber attacks, (ii) empirically develop a suspicion-based, latent structure of cues that occur during cyber attacks, (iii) demonstrate how the derived latent structure can be used to develop and test hypotheses about the effects of those cues on users' cognitive and emotional reactions, (iv) suggest and describe techniques to better train operators to detect, report, and appropriately react to security breaches, and (v) describe recent research with non-invasive physiological sensors that has the potential to monitor the mental states of operators in order to ensure optimum situation awareness in the cyber domain.

BACKGROUND, LITERATURE REVIEW, AND HYPOTHESES

The Construct of Suspicion

In a recent review of the "suspicion" literature, Bobko, Barelka, and Hirshfield (2014) synthesized literature across the social sciences, including management, marketing, communication, human factors, and psychology (consumer, counseling, and social). Their focus was on state suspicion in IT contexts. They found that many researchers who used the term did not define the concept, or definitions that were provided were of questionable use (see their page 490 for examples).