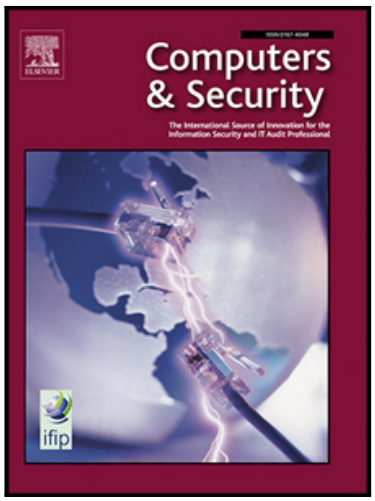

The impact of security awarness on information technology professionals' behavior

Ron Torten , Carmen Reaiche , Stephen Boyle

PII: S0167-4048(18)30465-6
DOI: https://doi.org/10.1016/j.cose.2018.08.007
Reference: COSE 1386

To appear in: *Computers & Security*

Received date: 19 October 2017
Revised date: 20 August 2018
Accepted date: 20 August 2018

Please cite this article as: Ron Torten , Carmen Reaiche , Stephen Boyle , The impact of security awarness on information technology professionals' behavior, *Computers & Security* (2018), doi: https://doi.org/10.1016/j.cose.2018.08.007

THE IMPACT OF SECURITY AWARNESS ON INFORMATION TECHNOLOGY PROFESSIONALS' BEHAVIOR

Ron Torten[a], **Carmen Reaiche**[b], Stephen Boyle[c,*] stephen.boyle@unisa.edu.au

[a]**Inphi Corporation, 2953 Bunker Hill Lane, Suite 300, Santa Clara, CA 95054**

[b]**Entrepreneurship, Commercialisation and Innovation Centre, University of Adelaide, Adelaide SA 5000**

[c]**Business School, University of South Australia, Adelaide SA 5000**

[*]Corresponding author.

ABSTRACT

Protecting digital assets is a growing concern for corporations, as cyberattacks affect business performance, reputation, and compromise intellectual property. Information technology (IT) security in general and cyber security, in particular, is a fast-evolving area that requires continuous evaluation and innovation. The objective of cyber-attacks has not changed over time however there is a shift in the attack methods through the increased use of social engineering, concentrating on the human elements as the weakest link in the security posture of any system network. This research looks at the relationship between threat awareness and countermeasure awareness on IT professionals' compliance with desktop security behaviors. The model originally put forward by Hanus and Wu (2016), was tested on a population of 400 IT professionals across a broad range of IT roles and company sizes in the United States. The overall findings show that 61.2% of the variability in desktop security behavior can be explained by threat awareness and countermeasure awareness. In addition, the research found a determinant relationship between threat awareness and countermeasure awareness with the five elements of protective motivation theory (PMT), which include perceived severity, perceived vulnerability, self-efficacy, response efficacy, and response cost. Finally, the research shows that all elements of PMT, with the exception of perceived vulnerability, significantly determine desktop security behavior.

Keywords

Information Technology Security, IT Professionals, Cybersecurity, Social Engineering, Protective Motivation Theory, Security Behavior, Human Behavior, Security Awareness Programs

THE IMPACT OF SECURITY AWARNESS ON INFORMATION TECHNOLOGY PROFESSIONALS' BEHAVIOR

INTRODUCTION

Protecting digital assets is a growing concern for corporations as cyberattacks impact reputation and compromise intellectual property. Information technology (IT) security in general and cyber security, in particular, is a fast-evolving area that requires continuous evaluation and innovation (Borrett et al. 2013). Cyber attackers increased their use of social engineering (Mickelberg et al. 2014) in an effort to combat the improvements in security systems that utilize multi-layer firewalls. The objective of cyber attackers have not changed over time as they attempt to install ransomware, violate intellectual property, steal medical records, execute unauthorized banking transactions, or misuse credit cards (Seong-kee and Tae-in 2015). An area of security that has been largely ignored is social engineering, which starts at the human/desktop interface to the network (Crossler 2010). Social engineering concentrates on the human elements, as humans are the weakest link in the security posture of any system network (Boss et al. 2009; Hinde 2001; Kumar et al. 2008). These human elements result in attacks that start at the desktop, as