

## Accepted Manuscript

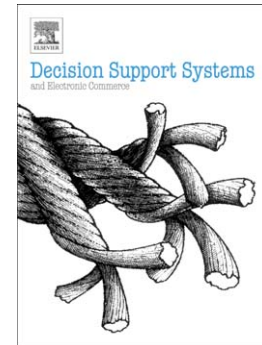
An Assessment of Opportunity-Reducing Techniques in Information Security:  
An Insider Threat Perspective

Keshnee Padayachee

PII: S0167-9236(16)30161-0  
DOI: doi:[10.1016/j.dss.2016.09.012](https://doi.org/10.1016/j.dss.2016.09.012)  
Reference: DECSUP 12769

To appear in: *Decision Support Systems*

Received date: 13 September 2015  
Revised date: 1 August 2016  
Accepted date: 13 September 2016



Please cite this article as: Keshnee Padayachee, An Assessment of Opportunity-Reducing Techniques in Information Security: An Insider Threat Perspective, *Decision Support Systems* (2016), doi:[10.1016/j.dss.2016.09.012](https://doi.org/10.1016/j.dss.2016.09.012)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

**AN ASSESSMENT OF OPPORTUNITY-REDUCING TECHNIQUES IN INFORMATION  
SECURITY: AN INSIDER THREAT PERSPECTIVE**

Keshnee Padayachee (Email: padayk@unisa.ac.za)

Institute for Science and Technology Education, UNISA, 0003, Pretoria, South Africa

**ABSTRACT**

This paper presents an evaluation of extant opportunity-reducing techniques employed to mitigate insider threats. Although both motive and opportunity are required to commit maleficence, this paper focuses on the concept of opportunity. Opportunity is more tangible than motive; hence it is more pragmatic to reflect on opportunity-reducing measures. To this end, opportunity theories from the field of criminology are considered. The exploratory evaluation proffers several areas of research and may assist organizations in implementing opportunity-reducing information security controls to mitigate insider threats. The evaluation is not definitive, but serves to inform future understanding.

**KEYWORDS:** Insider Threat; Situational Crime Prevention Theory; Cybercrime; Delphi Technique

**1. INTRODUCTION**

According to the CyberSecurity Watch Survey (2011), 46% of the respondents considered the maleficence caused by insider attacks to be more damaging than those caused by outsider attacks. The Boardroom Cyber Watch 2013 Survey (2013) in fact cautioned that this figure may be higher than 50%. An 'insider' is any individual who has legitimate access to an organization's information technology (IT) infrastructure (Magklaras & Furnell, 2005), while an 'insider threat' uses the authority granted to him/her for illegitimate gain (Schultz, 2002). Although both motive and opportunity are required to commit maleficence, this paper focuses on the concept of opportunity. Opportunity is more tangible than motive; hence it is more pragmatic to reflect on opportunity-reducing measures. According to Willison (2006), it is valuable for researchers to reflect on cybercrimes in terms of criminology theories as they are, after all, crimes. In criminology, four theories of crime embody the opportunity theory perspective: Rational Choice theory, Routine Activities theory, Crime Pattern and, more recently, Situational Crime Prevention (SCP) theory (Padayachee, 2015). As SCP theory is the one that has evolved most directly from the aforementioned

Download English Version:

<https://daneshyari.com/en/article/4972539>

Download Persian Version:

<https://daneshyari.com/article/4972539>

[Daneshyari.com](https://daneshyari.com)