AN INSIDER THREAT NEUTRALISATION MITIGATION MODEL PREDICATED ON COGNITIVE DISSONANCE (ITNMC\textsuperscript{CD})

Keshnee Padayachee

School of Computing

UNIVERSITY OF SOUTH AFRICA

padayk@unisa.ac.za

Abstract

The insider threat concern is a complex issue as the problem domain intersects the social, the technical and the socio-technical dimensions. Consequently counteracting the insider threat involves influencing the insider’s perceptions and behaviour in order to ensure compliance. When an individual’s actions and beliefs are incongruent, this induces a phenomenon known as cognitive dissonance. In this state, individuals are self-motivated to change either their behaviours or beliefs or they may rationalise their behaviour to reduce this dissonance. Neutralisation is a technique used by criminals to rationalise maleficence. In terms of the insider threat, it has been proposed that if the justifications for committing an offence are eliminated then the insider is less likely to commit the offence. This process is known as neutralisation mitigation. This research proposes that inducing cognitive dissonance may be a means of mitigating the neutralisations that the insider may use to justify maleficence. To integrate these concepts into an implementable solution – the Insider Threat Neutralisation Mitigation model predicated on Cognitive Dissonance (ITNMC\textsuperscript{CD}) is proposed.

INTRODUCTION

The insider threat is more hazardous than external threats, as an insider may use the skills and knowledge gained through legitimate work duties for illegitimate gain [Willison and Siponen 2009]. Counteracting the insider threat’s behaviour involves influencing the insider’s perceptions in order to ensure compliance. From a social psychology perspective, it is evident, that when an individual is in an environment that causes cognitive dissonance, self-persuasion [Arson 1999] is more effective than direct manipulation in changing behaviours and beliefs. When an individual’s actions and beliefs are incongruent, this induces a phenomenon known as cognitive dissonance [Festinger 1962]. In this state, individuals are self-motivated to change either their behaviours or beliefs or they rationalise their behaviour to reduce this dissonance. Neutralisation is a technique used by criminals to rationalise maleficence [Sykes and Matza 1957]. In terms of the insider threat, it has been proposed that if the justifications for committing an offence are eliminated then the insider is less likely to commit the offence [Barlow et al. 2013]. This process is known as neutralisation mitigation. This research proposes that inducing cognitive dissonance may be a means of challenging the insider’s perceptions, behaviours and rationalisations. This would involve simulating an environment where an insider in the process of committing maleficence, is simultaneously challenged by neutralization mitigation. In order to simulate such an environment, honeypots will be deployed to bait the insider into maleficence. It is envisaged that the insider will no longer be subject to those preconceived rationalisations when a real opportunity to commit maleficence is evident. To integrate these concepts into an implementable solution – the Insider Threat Neutralisation Mitigation model predicated on Cognitive Dissonance (ITNMC\textsuperscript{CD}) is proposed.
THE INSIDER THREAT NEUTRALISATION MITIGATION MODEL PREDICATED ON COGNITIVE DISSONANCE

As the problem domain intersects with the technical, socio-technical and sociological dimensions – these perspectives are categorised into three distinct processes within the model concept: that is the sociological indicators and the socio-technical interventions, technical indicators.

A. The Sociological Indicators

Cognitive dissonance is a sociological indicator that directs the tension experienced when simultaneously holding two or more conflicting cognitions: ideas, beliefs, values or emotional reactions [Festinger 1962]. For example, introducing information security policy via neutralisation mitigation perspective will create cognitive dissonance between an insider’s act of maleficence and the rules. This forces the insider to change their actions or readjust their perception (a sociological indicator) to account for this new information. The changes caused by cognitive dissonance has been found to be more effective if the individual is intrinsically motivated to change [Turban and Aronson 1998]. However cognitive dissonance may also result in the individual rationalising their behaviour or perceptions. According to Barlow et al.[2013], insiders may rationalise their maleficence by claiming for example, it was a victim less crime or that it was necessary to meet a deadline. This rationalisation process is known as neutralisation [Sykes and Matza 1957]. Neutralisation techniques, which is also a sociological indicator include: ‘denial of responsibility’, ‘defence of necessity’, ‘denial of injury’ and ‘metaphor of ledger’, ‘condemnations of the condemners’, and ‘appeal to higher loyalties’ [Sykes and Matza 1957]. However, it has been posited that if the rationalisations are removed then the insider threat can be circumvented [Barlow et al. 2013]. However, this issue intersects both the technical and sociological; hence, this model is predicated on socio-technical interventions to challenge the rationalisations of an insider threat.

B. Socio-Technical Interventions

The ‘remove excuses’ category from Situational Crime Prevention provide socio-technical interventions that will be used by the model concept to decrease the rationalisations that criminals may use to justify their behaviour [Clarke 1980]. The strategies proposed are ‘setting rules’, ‘posting instructions’, ‘alerting conscience’, ‘assisting compliance’ and ‘controlling drugs and alcohol’. In terms of ‘setting rules’, the typical information security policies, agreements, procedures have been proposed. In terms of ‘posting instructions’, e-mail disclaimers [Beebe and Roa 2005] are recommended as a comparable information security control, aside from the typical controls like information security policy. Single sign-on [Willison 2006] and ‘a single point of reference for security’ [Coles-Kemp and Theoharidou 2010] have been proposed as information security controls to realise the ‘assisting compliance’ technique. In terms of ‘alerting conscience’, the information security controls that are recommended include copyright protection [Coles-Kemp and Theoharidou 2010]; a code of ethics [Coles-Kemp and Theoharidou 2010] and ‘multi-level warning banners’ [Beebe and Roa 2005]. The ‘controlling drugs and alcohol’ technique is incongruent with the domain of information security and will not be considered in this research. The ‘setting rules’ technique was renamed to ‘promoting policy’ to be more congruent with the cyber domain. However, there has to be a means to detect when to activate these inventions. Consequently, honeypots are a useful technical indicator in detecting the insider threat and activating the interventions in a controlled environment.

C. The Technical Indicators

Honeypots are more than just a computer or a physical resource. A honeypot may be anything from a Windows program, to an entire network of computers [Spitzner 2003]. However, in its most rudimentary form it may be a credit card number, an Excel spreadsheet, or a record in a database [Spitzner 2003]. In this form a honeypot is called a honeytoken [Spitzner 2003]. Honeytokens are easily customizable and easily integrated [Spitzner 2003] hence the proof-of-concept of the model will be based on honeytokens. A honeypot will not be effective if the insider threat decides not to select it as they recognize that the luring honeypot is in fact a
trap. Hence interactions with a honeypot should be detectable to the system administrator but not to the insider threat. The model is based on a luring strategy where the insider is baited by honeypots instead of attacking real data during their daily operations.

D. The Model Overview

Honeypots are technical indicators that are used to detect an insider threat and activate the socio-technical interventions. The sociological indicators of cognitive dissonance, forces an insider either to use neutralisation techniques (i.e., rationalisations) or to change their perception, or behaviour. The neutralisation mitigation mechanisms encompass the socio-technical interventions: ‘promoting policy’, ‘posting instructions’, ‘alerting conscience’ and ‘assisting compliance’. This implies that neutralisation mitigation may be implemented from both a technical and a sociological perspective depending on the context. The neutralization mitigation techniques are a way of removing the rationalizations that criminals use to commit a crime by propagating the organization’s information security policy. The conflict between the insiders’ neutralisation techniques and the neutralisation mitigation causes cognitive dissonance. This forces the insider to change either their behaviour or their beliefs positively towards compliance. However, the insider may choose to further rationalise their behaviour or beliefs by choosing an alternative neutralization technique hence compromising compliance (see Figure 1).

Figure 1: A First-Order Overview of the ITNM\textsuperscript{CD} Model

CONCLUSION

This paper presented the ITNM\textsuperscript{CD} model, which is intended to mitigate the rationalisations that insiders use to commit maleficence. Sykes an Matza [1957] hypothesised that criminals use neutralisation techniques before committing an act. However, research has shown that neutralisation techniques could be used prior, during, or after criminal involvement [Andrews and Bonta 1998]. Further research will involve revisiting the model from a timeline perspective. Additionally, the next stage of the research will involve evaluating the model concept
REFERENCES


This article is a work-in-progress, if you wish to cite it; you must contact the author for permission.

UNISA ©