Journal of Information Security and Applications 000 (2017) 1–11

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Motivation and opportunity based model to reduce information security insider threats in organisations

Nader Sohrabi Safa[a,b,*], Carsten Maple[a], Tim Watson[a], Rossouw Von Solms[b]

[a] Cyber Security Centre at WMG, University of Warwick, Coventry, United Kingdom
[b] Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Information security
Insider threat
Organisation
Risk
Human factors

ABSTRACT

Information technology has brought with it many advantages for organisations, but information security is still a major concern for organisations which rely on such technology. Users, whether with intent or through negligence, are a great source of potential of risk to information assets. A lack of awareness, negligence, resistance, disobedience, apathy and mischievousness are root causes of information security incidents in organisations. As such, insider threats have attracted the attention of a number of experts in this domain. Two particularly important considerations when exploring insider threats are motivation and opportunity. Two fundamental theories relating to these phenomena, and on which the research presented in this paper relies, are Social Bond Theory (SBT), which can be used to help undermine motivation to engage in misbehaviour, and Situational Crime Prevention Theory (SCPT), which can be used to reduce opportunities for misbehaviour. The results of our data analysis show that situational prevention factors such as increasing the effort and risk involved in a crime, reducing the rewards and removing excuses can significantly promotes the adoption of negative attitudes towards misbehaviour, though reducing provocations does not have any effect on attitudes. Further, social bond factors such as a commitment to organisational policies and procedures, involvement in information security activities and personal norms also significantly promotes the adoption of negative attitudes towards misbehaviour. However, attachment does not significantly promote an attitude of misbehaviour avoidance on the part of employees. Finally, our findings also show that a negative attitude towards misbehaviour influences the employees' intentions towards engaging in misbehaviour positively, and this in turn reduces insider threat behaviour. The outputs of this study shed some light on factors which play a role in reducing misbehaviour in the domain of information security for academics and practitioners.

1. Introduction

Modern society is highly dependent on information technology systems. Air traffic, defence, telecommunication, and water distribution systems are all examples of pieces of critical infrastructure that rely on information and with respect to which information security is extremely important. Experts have, for many years, focused on the technological aspects of information security to guarantee a secure environment for information. However, it is acknowledged that the human aspects of information security play a vital role in this domain and should be taken into consideration along with technological aspects [26,39]. Effective information security management cannot be realised without considering the roles of users and organisations [36]; attacks originating from insiders, for example, can have serious consequences on the appropriate functioning of computer systems [30]. There are many types of insider: auditors, customers, permanent or temporary employees, ex-employees, and vendors, for example, and many of these will typically have the legitimate capability to access one or many systems, for example by the use of an authentication mechanism. An insider does not need to spend as much effort and time in accessing the targeted information in comparison to external attackers. Organisations often trust them, and anonymity is a characteristic that can decrease the risk of their being identified [33].

The Verizon Data Breach Investigations Reports (DBIR) [48] presents a view of the threats, vulnerabilities and actions that lead to security incidents and the resulting impact on organisations based on real security data. DBIR 2016 asserts that 60% of threats can compromise organisations within minutes. In this report, 55% of the incidents were the result of internal actors in organisations, and 40% were perpetrated because of financial

[*] Corresponding author at: Cyber Security Centre at WMG, University of Warwick, Coventry CV4 7AL, United Kingdom.

E-mail addresses: n.sohrabi-safa@warwick.ac.uk (N.S. Safa), cm@warwick.ac.uk (C. Maple), tw@warwick.ac.uk (T. Watson), rossouw.vonsolms@nmmu.ac.za (R. Von Solms).

https://doi.org/10.1016/j.jisa.2017.11.001
2214-2126/© 2017 Elsevier Ltd. All rights reserved.

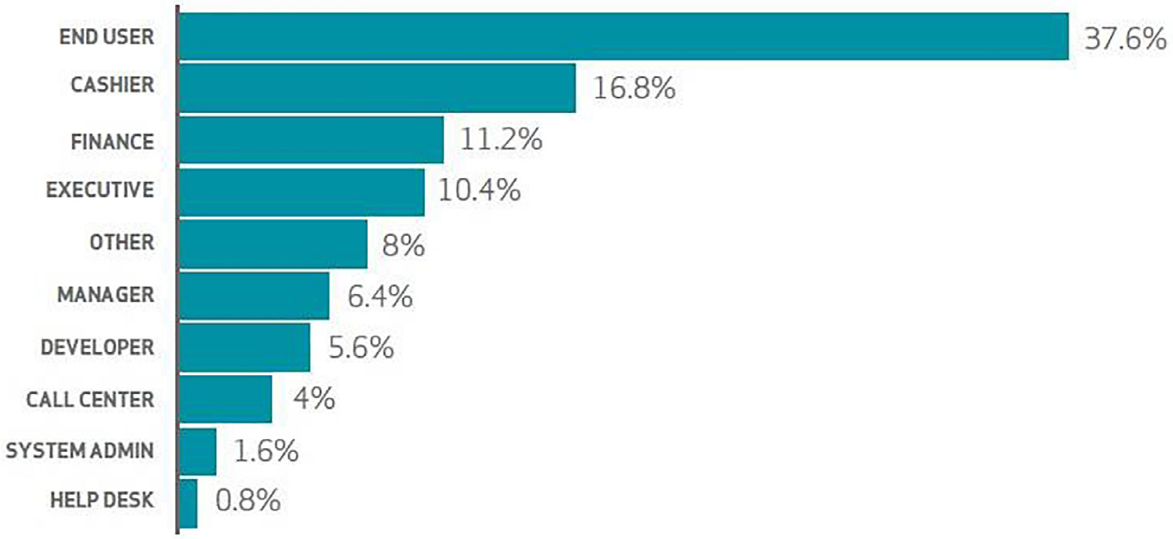

Fig. 1. Internal Misuse Pattern (DBIR 2016).

motivations, whether the insider planned to monetize the stolen data by selling it to others or by directly competing with their former employer. Fig. 1 shows the variety of internal misuse patterns in 125 organisations.

Insider threats compromise information confidentiality, integrity and its availability. Deletion, duplication, exfiltration and unauthorized extraction of critical information are examples of information security threats in this domain and the roots of these threats include apathy, bribery, corruption, espionage, embezzlement, extortion, ignorance and sabotage [47]. It is acknowledged that both motivation and opportunity play crucial roles in the violation of information security rules and regulations [34].

The domain of information security insider threats in organisations focuses mainly on the attitudes, intentions, and behaviour of employees. The convenience of engaging in crime and having motive for doing so play important roles in the aetiology of the employees' criminal behaviour [32]. In this research, a model has been presented for mitigating insider threats which is based on two important approaches: the approach of reducing opportunity to engage in crime and the approach of making employees motivated to avoid misbehaviour. This study aims to investigate whether increasing the effort and risk associated with information security misbehaviour, reducing reward and provocations, and removing excuses or rationalisations for misbehaviour, where these factors originate from Situational Crime Prevention Theory, functions to mitigate insider threats in organisations. In addition, this research endeavours to examine whether the employees' attachment and commitment to their organisation, their involvement in information security activities and their personal norms regarding insider threats, where this second set of factors comes from Social Bond Theory, functions to influence the attitude of the employees so as to reduce insider threats.

The structure of the paper is as follows: The definition of insider threats and why this subject is important has already been presented in this introductory section. The effective factors that mitigate insider threats originate from the two aforementioned fundamental theories, and these theories, along with their associated factors, are explained in section two. The research methodology we adopted, along with information concerning our data collection and the demography of our participants is presented in section three. The results of our data analysis (including our measurement and structural models) are discussed in section four. The contribution and implementation of the findings are discussed in section five, and finally the limitations of this research, as well as directions for future research, are explored in section six.

2. Theoretical background and research model

It has been acknowledged that social bond factors have a significant effect on the behaviour of individuals [11]. On the other hand, opportunity for crime can motivate offenders to conduct a crime or otherwise transgress rules and regulations [49]. That is why this research investigates the effect of the employees' attachment and commitment to organisations, their involvement in information security activities and their personal norms concerning information security misbehaviour, where these factors originate from Social Bond Theory, on one hand, and the effect of increasing effort and risk, decreasing rewards and provocation and removing excuses for violating information security rules and regulations, where these factors are based on Situational Crime Prevention Theory, on the other. These two theories, along with their associated factors, are explained in Sections 2.1 and 2.2 respectively.

2.1. Situational crime prevention theory

Reducing or stopping criminal activities is the main concern in the context of crime prevention. Situational Crime Prevention Theory focuses on opportunity-reduction mechanisms for different types of crime, and is a common approach to decreasing the opportunities for many types of crime or delinquent behaviour that occur across a variety of settings [15]. Situational Crime Prevention helps organisations to control or design an environment conducive to the reduction of crime or threats and is used in areas such as society, schools, organisation, social networks, and e-commerce, amongst others. Situational Crime Prevention purports to make crime more difficult and risky, to lower the rewards that comes along as the consequences of the crime, and purports to reduce excuses for conducting crime [32]. Rationalisation and available opportunities for offending play vital roles in the aetiology. It is argued that if offending is difficult, as a consequence the propensity to offend will be reduced. For instance, if we do not use a lock for the door of our house, our house will be more likely to be robbed, because the amount of effort the prospective thief needs to put into breaking in is lowered. Easy access to a target and its benefits encourage robbery. When deliberating about whether to commit a crime, offenders engage in an estimation of the benefits of their

Please cite this article as: N.S. Safa et al., Motivation and opportunity based model to reduce information security insider threats in organisations, Journal of Information Security and Applications (2017), https://doi.org/10.1016/j.jisa.2017.11.001