Article

Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees

Nikki Rajakaruna*, Pamela J Henry* Adrian J Scott*,**

Abstract Police information systems (ISs) contain highly sensitive data. Misuse of these systems poses a significant risk to agency integrity and personal privacy. In order to prevent this form of misconduct, police agencies must implement strategies that address factors associated with employee misuse. The aim of this research was to determine factors associated with the perceived likelihood of engaging in IS misuse among a sample of employees from an Australian police agency. Two hundred and eighty-seven unsworn police staff completed an online survey that investigated a number of factors, shown in previous research, to be relevant to IS misuse. Findings demonstrated that access to the IS, perceived appropriateness of and concern regarding IS misuse, and perceived certainty of punishment were relevant in explaining the perceived likelihood of IS misuse. Implications are discussed in relation to the focus of agency prevention strategies and the need for future research in the area.

Introduction

The misuse of information systems (ISs) is a concern for many organizations given an increasing reliance on information technology to record, store, and manage data. The misuse of police ISs poses significant concern given the sensitive and potentially compromising nature of information that is contained on these systems (e.g. arrest details, nature of violations, prior convictions, details of potential witnesses, evidence against suspects, and criminal associates). Given the sensitive nature of data that are contained on police ISs it is crucial that systems are accessed only by those authorized to access them, and only for purposes related directly to their work. Despite this, breaches of police ISs continue to appear in media reports, highlighting severe instances of IS misuse by both police officers and staff (Yorkshire Post, 2010; The West Australian, 2011; Kaila, 2013; Coyne, 2017; O'Maloon, 2017; Smee, 2018). It is disconcerting that these cases are likely to represent only a fraction of the breaches that occur, given that only a minority of security incidents are likely to be detected (Hoffer and Straub, 1989). Of particular concern, is the potential for members of organized crime syndicates to manipulate police employees

*Sellenger Centre for Research in Law, Justice and Social Change, Edith Cowan University, 270 Joondalup Drive, Joondalup WA 6027, Australia. E-mail: n.rajakaruna@ecu.edu.au
**Department of Psychology, Goldsmiths, University of London, London SE14 6NW, UK

Policing, Volume 0, Number 0, pp. 1–15
doi:10.1093/police/paz034

punishment is considered to outweigh the benefits of the behaviour (punishment severity; Bartollas, 2002; White and Haines, 2008). Much of the research regarding IS misuse has considered the effectiveness of organizational strategies employed on the basis of these principles of general deterrence (certainty and severity of punishment) and employee intentions to engage in IS misuse.

A basic deterrent strategy implemented in many organizations is the formulation of policy which outlines appropriate and inappropriate behaviour. The presence of policy enables employees to place parameters around their behaviour, ensuring that they behave in accordance with agency expectations. From the perspective of general deterrence theory, policy serves as a deterrent by increasing awareness of the negative consequences associated with a breach of the policy (Lee and Lee, 2002; Kankanhalli *et al.*, 2003; Ugrin and Pearson, 2008). Research by Ugrin and Pearson (2008) demonstrated the importance of agency policy in reducing employee intention to engage in non-work-related computing. Their research, conducted with a sample of 87 employees across 12 US companies, demonstrated that the presence of policies that outline acceptable behaviour and potential sanctions were important in lowering the IS misuse intentions. In contrast, research by Foltz *et al.* (2005) demonstrated that the presence of policy was, in itself, unlikely to deter IS misuse. In examining awareness of IS policies among university students, Foltz *et al.* (2005) established that although a computer usage policy was in place, students were not aware of the policy, nor the consequences of breaching the policy. The authors found that a single exposure to policy increased awareness of the policy and consequences of misuse, but concluded that repeat exposure was required to ensure the necessary deterrent effect. Further supporting the importance of staff awareness of agency deterrent as well as preventive strategies, D'Arcy and Hovav (2007) found that employee awareness of security policy, security training programmes, and preventive security software played an important role in lowering intention to engage in IS misuse.

In addition to deterrent and preventive strategies, research has considered employee awareness of detection strategies in reducing IS misuse. While Ugrin and Pearson (2008) found that awareness of detection systems capable of monitoring computer use was important in lowering intention to engage in IS misuse, D'Arcy and Hovav (2007) found that awareness of monitoring systems was not related to IS misuse intention. In explaining this finding, D'Arcy and Hovav (2007) proposed that despite an awareness of monitoring systems, employees may not perceive certainty of detection (and thus perceived no certainty of punishment) due to irregular auditing practices. Alternatively, D'Arcy and Hovav (2007) proposed that despite an awareness of monitoring systems, employees may not perceive punishment for misuse to be severe, and so, awareness of computer monitoring had no effect on behavioural intentions. Both explanations highlight the importance of measuring the certainty and severity of punishment (constructs central to the TGD), to consider whether IS strategies achieve their intended theoretical purpose of deterring misuse through the threat of punishment.

The importance of these constructs was considered by D'Arcy *et al.* (2009) who examined the relationship between awareness of security measures, the perceived certainty and severity of punishment, and subsequent relationships with intention to engage in IS misuse. Results revealed that employee awareness of security policy, security training programmes, and company monitoring of computer use were each related to perceived certainty and severity of punishment. However, inconsistent with expected findings and the TGD, only perceptions of punishment severity were related to intention to engage in IS misuse while perceptions of punishment certainty were not. The authors concluded that the influence of punishment certainty was moderated by moral commitment (i.e. the degree to which IS misuse was perceived to be morally acceptable), highlighting the relevance of