available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

In a 'trusting' environment, everyone is responsible for information security

Patricia A.H. Williams

School of Computer and Information Science, Edith Cowan University, 2 Bradford Street, Mt Lawley, Western Australia 6050, Australia

Keywords:
Insider threats
Governance
Medical information security
Security governance
Organisations

ABSTRACT

Information security is important in any organisation and particularly where personal and medical information is routinely recorded. Further, where the organisational culture revolves around trust, as in the medical environment, insider threats, both malicious and non-malicious, are difficult to manage. International research has shown that changing security culture and increasing awareness is necessary as technical resolutions are not sufficient to control insider threats. This area of information security is both important and topical in view of the recently publicised breaches of patient health information. Ensuring that all staff assumes responsibility for information security, particularly as part of an information security governance framework, is one practical solution to the problem of insider threats.

1. Introduction

Insider threats are an important yet often overlooked aspect of security. In a highly controlled environment responsibility for security is provided predominantly by the organisation, however, in environments that rely heavily on trust, this responsibility is devolved to all members of the organisation. However, it is these very staff members that are defined as the insider threat. From a security discipline perspective, the insider threat is viewed as an antagonist within a trusted computing base, and as such the insider threat is often considered using an adversarial model which encompasses all possible malicious insiders (Magklaras and Furnell, 2005). However, these models fail to encompass the non-malicious insider threats. As Fox (1998) suggests the role of security has changed "boundaries between trusted and un-trusted entities are harder to distinguish".

The potential damage from insider threats is affected by how informed management is of the risk of security breaches. This is fuelled by the underestimation of the risks associated with an increasingly electronic and connected environment (Williams, 2007b). As more information is shared and the risk to data from authorised user increases, the insider and the associated threats are no longer clearly delineated. There is an abundance of examples in the media of security breaches from inside which have caused major corporate failure, such as Barings Bank and Enron (Hamilton and Micklethwait, 2006) to more personal events such as loss of medical records (BBC News, 2008), and unauthorised release of information (Mulligan, 2001). All of these incidents are a result of insider activity.

This paper discusses the insider threat with specific reference to the medical environment and a workplace culture that promotes trust. In the medical environment, communication plays an intrinsic part in the care of patients and is facilitated by technology and networking (Coiera and Tombs, 1998). Yet the progression in the use of information communication techniques is hampered by interruption to workflow and a reticence to adopt new computing technologies in this environment. This can be attributed to the potential impact of errors, which are more serious in the healthcare setting than elsewhere. The impact of these

E-mail address: trish.williams@ecu.edu.au
1363-4127/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2008.10.009

security threats range from mere inconvenience to seriously affecting day-to-day operations. Whilst threats and breaches of information security may not prevent the medical practice functioning in its ability to provide patient care, it can cause inconvenience and affect the efficiency with which this is delivered. Such events can be costly as patient and other information are key assets of a medical practice in the 2000s. Loss of data, loss of reliability and integrity, or breaches of confidentiality can result also in efficacy and legal problems. As many researchers have identified, it is not the technology itself that poses the problem but the effective use of the technology and the environment in which it is placed (Beresnevichiene, 2003; Furnell, 2005; Furnell et al., 2006).

Insider threats can be purposeful and malicious or accidental and non-malicious. Many attacks require little technical knowledge by exploiting business process rather than technology. Therefore organisations, particularly those with sensitive information to protect, should review their workflow and business procedures and employ a sound security governance process. This requires a holistic perspective and approach to insider threats. This paper looks at the issue of insider threats from a primarily non-malicious perspective. The issue should not be one of where the threat comes from, rather how efficient are the processes and systems in place at detecting and halting potential attacks, with the objective being to eliminate and minimise damage. The paper takes the view that several contributing factors interplay to create an insecure environment in medical practices. These factors are of both a technical and organisational nature. The insider threat need not be malicious; it may be uninformed, driven by culture, mistakes, errors, or be attributed to a lack of policy and procedures. Addressing these issues requires consideration of both technology and people; it requires an encompassing security governance approach. The governance approach is a method of pursuing strategic goals by balancing risk with return on investment. It includes accountability and allows for demonstration of appropriate practice and integrity and means that everyone in the organisation is involved. One model that will be considered as a potential solution for insider threats in the medical environment is the Tactical Information Governance for Security model. This model includes the individual as well as the corporate perspective on security.

2. Insider threats

The use of the terms ‘insider threat’ and ‘insider attack’ are generic, and whilst they have negative connotations, the terms are used in the security field to indicate both malicious and non-malicious attack vectors. Regardless of the motivation of the attacker, the general types of threat are human error, intellectual property compromises, unauthorised access, information extortion, sabotage, theft of information, disruption in availability and software attacks.

The insider threat is the intentional and unintentional harmful event caused by people with legitimate, authorised access to information systems within an organisation’s network. This is usually employees of an organisation, although in a medical environment it can be locums, associated health service administration staff and indeed patients. Locum and temporary staff are outsiders with legitimate insider access, which blurs the definitive insider/outsider threat line. One major problem with insider threats in that 99% of systems do not challenge the authenticated user (Hinde, 2003). Whilst there are more outsider attacks, there are more successful insider attacks (Schultz, 2002) and in general these are more costly to the organisation (Hinde, 2003).

It has been suggested that insider threats are impossible to control by technological means because they are often socially or organisationally based (Anderson, 1999). However, technological solutions do play a part as the US National Threat Assessment Center (2008) report that most insider attacks were by people with minimal technical skills. Potential insider threats display both technical and behavioural characteristics. Where once skill and resource was a necessity for a threat to be present, automated tools have facilitate easier intrusion, access and require little if any computer skill to function (Whitman, 2004). For the insider many of these tools may be unnecessary since gaining access is not an issue they are faced with. Therefore, a lack of technical skill may not be a limiting factor for the insider attacker (Schultz, 2002). It is possible then that some attacks may be prevented using technological means.

3. What current approaches lack

Currently, approaches to information security are primarily based on perimeter protection such as firewalls and intrusion detection systems. Also, whilst the electronic environment has facilitated efficiencies in data collection and processing, it has also allowed greater access to a wide variety of information that a user might not otherwise have been exposed to. It is therefore helpful to model attacks in the face of increased access. To assist in predicting vulnerabilities, there exist various models on insider threat prediction using attacker behaviour, intrusion detection and analysis as their underlying basis (Magklaras and Furnell, 2005; Schultz, 2002; Wood, 2002). However, small organisations are rarely sufficiently resourced to investigate and monitor the use of such models.

A consideration of a person’s sills, knowledge and motives are also important. Consequently, recommendations from RAND workshops on insider threats have acknowledged that whilst most attempts to address inside threats are technology based, there are effective non-technology based approaches (Anderson, 1999). Other research suggests that part of the approach should be to develop institutional capabilities, including consideration of the environment rather than just the individuals’ personality and motives (Willison, 2006). This implicates the organisational values and culture as a key factor in insider activity. In addition, what is often overlooked is that the organisation is a custodian and therefore legally liable for the information which it collects, uses and maintains. Such responsibility requires good internal processes and governance to be in place and executed. Even when such processes exist, it is the overriding culture of an organisation which shapes employee behaviour.