Chapter 13
The Role of Education and Awareness in Tackling Insider Threats

Shaun Joseph Smyth
Ulster University, UK

Kevin Curran
Ulster University, UK

Nigel McKelvey
Computer Science Department, Letterkenny Institute of Technology, Ireland

ABSTRACT

Insider threats present a major concern for organizations worldwide. As organizations need to provide employees with authority to access data to enable them to complete their daily tasks, they leave themselves open to insider attacks. This chapter looks at those who fall into the category which can be referred to as insiders and highlights the activity of outsourcing which is employed by many organizations and defines the term insider threat while pointing out what differentiates an accidental threat from a malicious threat. The discussion also considers various methods of dealing with insider threats before highlighting the role education and awareness plays in the process, the importance of tailoring awareness programs, and what the future holds for insider threats within organizations.

INTRODUCTION

In the early 1990s the United States saw a drive in the growth of business because of telecommunications networks and the Internet. Despite this growth, the dependency placed upon these networks placed the U.S. in a precarious position as it also increased their vulnerability to cyber exploitation and by the end of the twentieth century the U.S. had become the most vulnerable nation to cyber-attacks aiming to disrupt or interfere with essential services (McConnell, 2002).

DOI: 10.4018/978-1-6684-3698-1.ch013

Organizations, worldwide regardless of their size or form have all accepted that an increase in the development of their existing services is essential if they are to improve and gain a much-needed advantage over their fellow competitors. In their quest to achieve this goal organizations understand that a greater dependence is placed upon the need for information technology (IT) for them to compete successfully in the world of modern-day business (Abawajy, 2014). Businesses are already connected with the bulk of transactions taking place in an electronic format the consequence of which is a constant rise in the quantity of both personal and sensitive data produced and later collected. Sensitive data is looked upon as one of the many assets of any organization as many appreciate its significance, considering it to be the lifeblood of the processes and procedures which take place within their business (Sarkar, 2010). As many of today's organizations compete in lively and fast-moving environments which are constantly developing, they produce a large volume of sensitive data in a bid to achieve their goals which include lower prices, higher quality of products and services and a rapid development. However, the provision of new opportunities coupled with the globalization of activities in both businesses and organizations combined with the swift growth of ICT has given rise to a new problem in the form of threats (Stavrou et al. 2014).

Organizations can find themselves on the receiving end of threats as their information security is susceptible to dangers from a wide variety of sources which present in many different formats varying from the less complicated spam emails to the more structured and complex form of attack such as malwares (malicious software) which can steal or contaminate data and ultimately produce enough damage to leave systems in a condition where they are inoperable (Abawajy, 2014).

One such threat includes that caused as a direct result of online social networking (OSN) which has recently experienced a sudden rise. Certain employees within organizations are accountable for information and are later responsible for the leakage of this same information to outside parties. Careless use of social media has a harmful influence on organizations placing networks and systems at risk of malware which can result in many negative issues including copyright and defamation issues, reduced productivity which significantly affect the organization's reputation and future income (Molok et al. 2011).

Modern-day information systems are challenged by a wide range of threats and even though attacks which are started from outside such as viruses and hacking receiving much publicity the insider threat however, presents a considerably higher level of danger (Theoharidou et al. 2005). This view is shared by Baracaldo and Joshi (2012), McCormac et al. (2012), and Warkentin and Willison (2009) who all point out that Insider attacks are still one of the most dangerous threats organizations can face today.

The insider threat comes from the trusted organizational member and they can cause the greatest harm as they have access to the organization's greatest asset 'information'. Those individuals employed within an organization have the capability to either damage or destroy sensitive information using uncomplicated noncompliance of security policies, negligence, the absence of motivation in the protection of sensitive data, careless actions within the workplace or insufficient training. Including reduced productivity and revenue such actions result in the failure to protect the confidentiality of the organization, its associates, customers and ultimately the reputation of the organization's information system. This problem is often referred to as the 'endpoint security problem' as the employee is the last point of contact or endpoint of the information system (IS) and its network. It is often said that the weakest link or greatest security problem within a network lies between the keyboard and the chair (Warkentin, and Willison, 2009).

Organizations are faced with an ever-growing task in relation to computer security and face persistent attacks from both external and internal sources as there are many different threats which are all keen to breach organizational security defenses with a noticeable increase in the vulnerability to threats posed by