Chapter IX
Human Factors in Security: The Role of Information Security Professionals within Organizations

Indira R. Guzman
TUI University, USA

Kathryn Stam
SUNY Institute of Technology, USA

Shaveta Hans
TUI University, USA

Carole Angolano
TUI University, USA

ABSTRACT

The goal of our study is to contribute to a better understanding of role conflict, skill expectations, and the value of information technology (IT) security professionals in organizations. Previous literature has focused primarily on the role of information professionals in general but has not evaluated the specific role expectations and skills required by IT security professionals in today’s organizations. In this chapter, we take into consideration the internal and external factors that affect the security infrastructure of an organization and therefore influence the role expectations and skills required by those who are in charge of the security of network infrastructures in organizations. First, we describe the factors discussed in the literature and support them with quotes gathered from interviews conducted with information security professionals in small organizations in Central New York. Then, we present a set of common themes that expand the understanding of this role and finally we provide practical recommendations that would facilitate the management of these professionals within organizations.
INTRODUCTION

Research in the area of information systems has acknowledged that information technology human capital is a strategic resource within organizations and that its “effective management represents a significant organizational capacity” (Ferratt, Agarwal Brown and Moore, 2005, p.237). Most of the research done on human resources management (HRM) within the field of information systems has focused on the role of information technology professionals in general, but little research has been conducted about the role of a more specific group, the information technology security professional. In this book chapter, we will discuss the role, challenges and opportunities of this particular type of job within organizations.

In previous research, Information Technology (IT) professionals in general have been defined as a diverse group of workers trained formally or informally and engaged primarily in the following activities related to information and communication technology systems, components, or applications: conception, selection, acquisition, design, development, adaptation, implementation, deployment, training/education, support, management and documentation (Kaarst-Brown and Guzman, 2005). IT professionals have direct responsibility for the quality of the information available to decision-makers (Prior, Rogerson, and Fairweather 2002). As organizations become more strategically reliant upon information systems, IT professionals’ management, recruitment and retention have an increasingly significant impact on the future of their companies. To address these increasing HRM challenges, research has been conducted to improve understanding of the roles and skill requirements of the IT professional. Likewise, it is also important to understand the role of IT security professionals because their position within organizations and the importance of their jobs is crucial and has a set of specific challenges that shape this role. In this chapter, we summarize the range of factors that influence the role expectations of IT security professionals, the necessary skills that they should have in order to perform an effective job of securing the network infrastructure of an organization, and the challenges and satisfactions these professionals face in fulfilling this vocation.

ROLES AND RESPONSIBILITIES OF IT SECURITY PROFESSIONALS

The job of IT security professionals is to ensure that the networks, infrastructure, and computer systems within organizations are properly and adequately secure by protecting information assets, such as customer data, financial information and critical network infrastructures. Information security refers to the process of protecting information, specifically its availability, confidentiality and integrity. On the other hand, information technology security refers to the process of controlling the technology that allows access to information making it accessible only to those who are legitimately allowed to do so. As stated by Belsis et al. (2005), IT Security refers to the set of principles, regulations, methodologies, measures, techniques, and tools we use to protect an information system from potential threats. The IT security professionals are the ones in charge of the selection, acquisition, design, development, adaptation, implementation, deployment, training/education, support, management and documentation related to IT security of an information system within the network. All these strategies are now a subsection of the organization’s strategic policy (Layton, 2007). This includes, but is not limited to, security threat and risk analysis; security technologies; detection techniques; policies, laws, and regulations governing the procedures used by the IT staff; end user and client user policies for Web access and e-mail; design and implementation of system analysis; and controlling traffic flow through the network. Network security is defined as the protection of networks...
Related Content

Security Risks of Mobile Commerce
www.igi-global.com/chapter/security-risks-of-mobile-commerce/150080?camid=4v1a

A Rule-Based and Game-Theoretic Approach to Online Credit Card Fraud Detection
www.igi-global.com/article/rule-based-game-theoretic-approach/2465?camid=4v1a

Determinants of Financial Failure in Ghana: Probit Analysis of UniBank Loan Defaults
www.igi-global.com/article/determinants-of-financial-failure-in-ghana/111125?camid=4v1a

A More Secure Image Hiding Scheme Using Pixel Adjustment and Genetic Algorithm
www.igi-global.com/article/a-more-secure-image-hiding-scheme-using-pixel-adjustment-and-genetic-algorithm/95139?camid=4v1a