Global Information Security Factors

Garry White, Texas State University - San Marcos, USA
Ju Long, Texas State University - San Marcos, USA

ABSTRACT

The Internet has changed security and because the Internet is borderless, security threats are now on a global scale. In this paper, the authors explore the global nature of information security from the perspectives of corporate professionals. Through an empirical study with corporate professionals, who have first-hand information security knowledge, the authors confirm that the proposed knowledge topics are relevant toward a comprehensive understanding of information security issues. Analyzing the empirical data, the authors found two global security factors: business protection of data and government/social issues.

Keywords: Business Data Protection, Corporate Information Security, Global Information Security, Information Security, Information Security Professionals

INTRODUCTION

Globalization, through the Internet, has allowed knowledge sharing and collaborations across countries, judicial boundaries. It makes information security more challenging and an issue for corporations. The Internet allows hackers and other criminals to roam the Internet, evading law enforcement by moving from country to country (Jung et al., 2001). Because of the global nature of the Internet, hackers and criminals can cause information security breaches from anywhere on the globe.

For instance, Symantec (2008) reported that 56% of the worldwide denial-of-service attacks were targeted towards the U.S. Most of these attacks were traced to sources outside the U.S. Symantec (2008) also reported 43% of worms (a type of malicious code) originated in Europe, Middle East, and Africa and 42% of spam detected worldwide originated outside the United States. Clearly, the information security risks have brought numerous challenges to business practices. The risk factors in international trade and the complications in bringing buyers and sellers together in a mutually trustworthy environment were close to insurmountable (DuBois, 2004). To address these information security challenges, a comprehensive understanding of the global nature of the information security is crucial.

In addition, information security is a multidisciplinary field (Cresson-Wood, 2004; Gritzalis et al., 2005; Cegielski, 2008). It is a field that involves the social aspects of legal and ethical issues (Himma, 2008). A wide range of educational experiences are required...
for information security professionals (Todd & Vickers, 2003). Information security professionals need knowledge of management, business administration, ethics, sociology, and political science, E-Commerce, software assurance, fault-tolerance and survivability, etc. (Hentea et al., 2006).

Therefore, we argue that a multidisciplinary body of knowledge and skills are needed for a comprehensive understanding of information security. Casey (2006) indicated that expertises in information security, digital forensics, penetration testing, reverse engineering, programming, and behavioral profiling are required. We propose the framework of the global information security topics include: information systems and computer science political science because of security regulations and policies cross national boundaries, criminal justice, and business knowledge.

This paper looks at what corporate practitioners think they need to know in order to better understand the issues of global information security. The theoretical model and topics used were developed from a previous research paper, Long & White (2010).

From these global information security topics, what knowledge factors can be determined? In this research, we set to explore the global factors and topics that are relevant to the corporate information security issues. Based on an empirical survey of 36 corporate professionals, our goal is to find a common set of global factors that the practitioners all regard as essential in understanding the global perspectives of information technology.

The purpose of this paper is not to discuss what global information security is, or how to meet the global information security challenges. Rather, we focus the research on empirically determine what knowledge base that the practitioners are considered as invaluable in global information security field.

Our research results provide a foundation for the development and adoption of a global information security infrastructure. Our study will also provide guidance to career development and to corporate management that focus on global information security infrastructure.

The following sections provide the theory background, propose our research framework, data collection process, and discussion of the research results. The last section discusses implications and future research directions.

LITERATURE REVIEW

Global Nature of Information Security

Internet has enabled the information exchange across judicial national boundaries, without the limit of customs, time differences, or language. It also attracts criminals to the cyber space because of its borderless feature. Criminals only need a computer and an Internet connection to be able to roam freely between the countries, covering their tracks along the way. However, this borderless feature of the virtual world also makes fighting with the criminal especially difficult. It is slow and tedious, and many times, almost impossible, to police the virtual world across national borders and jurisdictions (Ferrell, 2004). Laws from different nations are not fully compatible. Data sharing between the law enforcement agencies from different nations are not sufficient. Certain activities are permissible in one country but not in another. Each set of laws reflects the nations’ own political and economic interests and their legal systems (Oz, 1994). Without an international treaty on fighting cyber crimes, it will be up to the countries to apply their own, quite different laws (Powers, 2008). There are some early efforts in establishing such an international treaty. For example, the European Union adopted a directive requiring spammers to obtain the consumer’s consent before sending unsolicited commercial e-mail (Saunders, 2002, Himma, 2008). However, these are still very early efforts.

Moreover, the countries that are weak in the law enforcement area are often the origins of the cyber crimes (Williams, 2001). Because of the lack of specific statute or case laws in these countries, many legal problems become
Cyber Crime Control in Developing Countries' Cybercafés
[www.igi-global.com/chapter/cyber-crime-control-developing-countries/28543?camid=4v1a](www.igi-global.com/chapter/cyber-crime-control-developing-countries/28543?camid=4v1a)

Robust Image Data Hiding Technique for Copyright Protection
[www.igi-global.com/article/robust-image-data-hiding-technique-for-copyright-protection/87414?camid=4v1a](www.igi-global.com/article/robust-image-data-hiding-technique-for-copyright-protection/87414?camid=4v1a)