Chapter 58

Information Security and Information Assurance:

Discussion about the Meaning, Scope, and Goals

Yulia Cherdantseva
Cardiff University, UK

Jeremy Hilton
Cranfield University, UK

ABSTRACT

Despite great interest of researchers and professionals in Information Security (InfoSec) and Information Assurance (IA), there is still no commonly agreed understanding of the disciplines. This chapter clarifies the meaning, scope, and goals of InfoSec and IA as well as the relationship between the disciplines. Clarity of the scope and goals of InfoSec and IA is important because this knowledge serves as a foundation for the definition of (1) curricula for the InfoSec and IA education programs, (2) responsibilities of practitioners, and (3) organisations' InfoSec strategy and policies. The study analyses US and European InfoSec- and IA-related official publications and standards and discusses the perception of the disciplines in academic and industry works. The study highlights the importance of clear and precise definitions of InfoSec and IA and a need for the definitions to promote open-mindedness among practitioners and researchers. Since the existing definitions of InfoSec and IA do not fully reflect the complexity and the evolving nature of the disciplines, the contemporary adapted definitions of InfoSec and IA are elaborated in the chapter.

1. INTRODUCTION

The beginning of wisdom is the definition of terms. - Socrates

Information Security (InfoSec) and Information Assurance (IA) have become increasingly important in an era in which information is recognised as a key asset by many organisations. The rapid advancement of Information and Communication Technology (ICT), and the growing dependence of organisations on IT infrastructure continuously intensify the interest in these two disciplines. Organisations pay increasing attention to information

DOI: 10.4018/978-1-4666-8111-8.ch058

protection also because the impact of security breaches today has a more tangible, often devastating effect on business (Dlamini et al., 2009).

The number and severity of security breaches grows. In 2007, the TJX Company lost, according to different sources, from 36.2 to 94 million customers' credit and debit cards records (Shaw, 2010). In 2011, Sony reported a data breach that had resulted in the loss of personal details of 77 million customers (Sony, 2011). According to the *Information Security Breaches Survey 2010* (PwC, 2010), the number of large companies in the UK that suffered a security incident during 2010 increased up to 92%, in comparison to 72% in 2008. The average cost of the worst security incident in large UK companies increased from £170,000 to £690,000. In the US, the number of security breaches detected by law enforcement increased up to 33% in 2011, against 7% in 2010 (Trustwave, 2012). The spending on InfoSec worldwide stayed stable in 2011 (ISC, 2011), even despite the economic downturn. In 2012, security budgets received higher priority worldwide compared with 2011 (Gartner, 2012). Gartner predicts a stable (at the annual rate of 9%) growth of security market until 2016. As a result, the spending on security is expected to grow from $55 billion in 2011 to $86 billion in 2016 (Gartner, 2012).

In response to the growing interest, a significant amount of research has been conducted over the past two decades to cover various perspectives of InfoSec and IA: the technical side (Anderson, 2001a); the human factor (Lacey, 2009); the business and economic perspectives (Pipkin, 2000; Anderson, 2001b; Sherwood et al., 2005); and the governance (SANS, 2004; FRC, 2004; Sherwood et al., 2005). Despite great interest in InfoSec and IA, there is still no commonly agreed understanding of the disciplines. Every author makes a unique interpretation of InfoSec and IA by identifying the divergent scopes and goals of the disciplines. The approaches to InfoSec and IA vary, depending on the background of the author and on the nature of the author's occupation. InfoSec and IA remain open to diverse interpretations, partly due to the fact that both disciplines are inevitably evolving. Many studies highlight the continual changes of InfoSec (Parker, 1998; Pipkin, 2000; Anderson, 2001a; Lacey, 2009; ISACA, 2009). Therefore, a revision of the meaning, scope and goals of the disciplines has to be conducted periodically to reflect this fluctuating environment.

The motivation of this study stems largely from the lack of a consistent, clear approach to InfoSec and IA, and, furthermore, from the existing misinterpretations of the terms. Despite the fact that both, InfoSec and IA, have been intensively discussed, there are still no commonly accepted definitions of the terms. The relationship between InfoSec and IA remain disputable. This study also originates from the necessity to resolve the controversy within InfoSec and IA concerning the overall goals and scope of the disciplines. This paper analyses different approaches to InfoSec and IA in order to draw a state-of-the-art picture of the disciplines in the permanently changing landscape.

The main objectives of this study are, first, to outline the up-to-date and precise realms of InfoSec and IA and, second, to develop a refined definition of each discipline in light of these findings. The paper aims to answer the following questions:

- What is Information Security: its meaning, scope and main goals?
- What is Information Assurance: its meaning, scope and main goals?
- What are the differences, similarities and relationship between the disciplines?

The clarity and unambiguity of the scope and goals of InfoSec and IA are important because this knowledge serves as a foundation for the definition of (1) curricula for the InfoSec and IA education programs, (2) responsibilities of practitioners,