Security Protection for Critical Infrastructure

M. J. Warren
Deakin University, Australia

T. B. Busuttil
Deakin University, Australia

INTRODUCTION

Understanding and managing information infrastructure (II) security risks is a priority to most organizations dealing with information technology and information warfare (IW) scenarios today (Libicki, 2000). Traditional security risk analysis (SRA) was well suited to these tasks within the paradigm of computer security, where the focus was on securing tangible items such as computing and communications equipment (NCS, 1996; Cramer, 1998). With the growth of information interchange and reliance on information infrastructure, the ability to understand where vulnerabilities lie within an organization, regardless of size, has become extremely difficult (NIPC, 1996). To place a value on the information that is owned and used by an organization is virtually an impossible task. The suitability of risk analysis to assist in managing IW and information infrastructure-related security risks is unqualified, however studies have been undertaken to build frameworks and methodologies for modeling information warfare attacks (Molander, Riddile, & Wilson, 1996; Johnson, 1997; Hutchinson & Warren, 2001) which will assist greatly in applying risk analysis concepts and methodologies to the burgeoning information technology security paradigm, information warfare.

Risk analysis provides a basis for evaluating vulnerabilities of information systems and was attractive because the need for countermeasures could be justified.

Development

The problem is that traditional risk analysis methods are not able to deal with the complexities An exception to this is the development of RAND Corporation's "Day Of…Day After…Day Before…" approach (Molander et al., 1996). This approach to impact modeling allows the analyst to take a three-step look at how IW can be perceived and therefore possibly countered. The proposed first step is to look at what occurs on the "Day Of…" the IW attack and to fully understand what is happening to all stakeholders involved in the system being reviewed. We must then look at "Step Two—The Day After…" and "Step Three—The Day Before…" which will allow us to see exactly what has happened, is happening, and what will happen, within the scenario being reviewed, in an easy-to-understand format.. Other research in this field (Shedden, Ruighaver, & Ahmad, 2006; Koh, Ruighaver, Maynard, & Ahmad, 2005) is exploring the possibility of extending the existing security risk analysis paradigm to deal with IW security issues. This research relates to the new development of a new SRA method (Busuttil & Warren, 2002a) with a view toward an SRA methodology for organizational information infrastructure (OII).

SRA AND INFORMATION INFRASTRUCTURE PROTECTION

The major characteristics of IW which set it apart from information security (IS) are the need to deal with:

- scalability
- flexibility
- difficulty in cost evaluation of threats, vulnerabilities, and attacks

The methods offered to deal with these shortfalls are offered in research which forms a basis for these further investigations (Busuttil & Warren, 2002a). One of the major advantages of LTMs are the ability to build security into information systems in an adaptable manner (Baskerville, 1993). It is also important to build security in across the breadth and depth of the organiza-

Table 1. Infrastructure-level notations (Busuttil & Warren, 2002a)

Infrastructure Level	Notation
Global Information Infrastructure	GII
National Information Infrastructure	NII
Organizational Information Infrastructure	OII
Personal Information Infrastructure	PII

tion, as focusing on one major area to secure can often be a downfall of organizations (Cramer, 1997).

The proposal of the idea of a fourth generation of SRA model comes about as a result of the lack of suitability of the aforementioned SRA methodologies to information warfare (Busuttil & Warren, 2002a) and the infrastructure level scalability issues discussed earlier. The notation of different levels of infrastructure is shown in Table 1.

CASE STUDY: APPLICATION OF CONCEPTUAL MODEL TO REAL-LIFE SCENARIO

This case study shows the application of Layered Logical Transformation Models (LLTMs) to an organization. The organization we will focus on is the Australian Internet service provider, Alphalink. The reasons for the selection of Alphalink are that it relies on the NII for business continuity while also providing connection infrastructure for its customers' PII. Alphalink runs its business within an organizational infrastructure and relies on the national and global II to provide the underlying communications and computing support necessary for it to conduct business. Alphalink should not do anything to actively compromise its connections to the NII/GII or the actual NII/GII. Customers of Alphalink rely on a dependable method of connection to Alphalink's OII, while they should also be able to ensure that they do not actively attempt to compromise the connection to Alphalink's OII or the actual OII. The following list shows the five major principles that need to be upheld (Busuttil & Warren, 2002a):

1. Alphalink can expect a certain level of service from the level of infrastructure above.
2. Alphalink should do all it can to ensure that the links between itself and any higher-level infrastructure entities are secure.
3. Alphalink should focus on securing itself to the best of its abilities in four major categories, defending against:
   - high-level infrastructure attacks,
   - internal attacks,
   - low-level infrastructure attacks, and
   - partnership attacks.
4. Alphalink must ensure that the connection to the lower infrastructure level is not compromised and should also expect a degree of care to be exercised by the user.
5. Alphalink should ensure that the integrity of lower-level infrastructure components is upheld during any interaction with customers and should also expect users to maintain II entities.

The conceptual diagram of this case study application, including references to the implied steps and the level of hierarchy they must take place within, is shown in Figure 1.

Figure 1. Alphalink's application of the LLTM concept