IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB7097

Chapter VIII

Aggression on the Networks: An Australian Viewpoint

William Hutchinson
Edith Cowan University, Australia

Matthew Warren
Deakin University, Australia

This chapter examines the attitudes of Australian IS/IT managers to the concept of cyber-vigilantism. Also, it explores the policies and procedures which have been set in place by various organizations to cope with concerted attacks on their systems. It finds that although a majority of managers do approve of the concept of "striking back', only a minority are prepared for this eventuality. There appears to be complacency about the threats posed by organized, offensive attackers.

INTRODUCTION

This exploratory research was undertaken to establish a general impression of the attitudes of professionals in business and government to the concept of cyber-vigilantism. It was undertaken as an initial project to provide the context for a larger, formal international survey. Cyber-vigilantism is the proactive process of responding to information attacks by hackers (from whatever source) with corresponding attacks on them. In short, it is hacking the hackers. The military and intelligence services have developed much of the technology for this. It is bringing the military concept of "information warfare' (Schwartau, 1996; Dearth, Williamson, 1996; Knecht, 1996; Waltz, 1998; Denning, 1999) into the civilian world. The survey was based on an initial, informal survey carried out by Schwartau (1999) using an

This chapter appears in the book, Social Responsibility in the Information Age: Issues and Controversies by Gurpreet S. Dhillon.

Internet site to gauge the attitudes of (mostly) American managers toward non-passive strategies against hackers. The survey described in this paper, attempts to specifically seek out the attitudes of Australian IT managers to this "offensive" method of information security. To obtain as wide a range as possible, the sample included organizations of as many sizes and industry types as could be found.

BACKGROUND

Cobb (1998) has outlined the potential threats to the Australian economy from information warfare attacks. In a world, where hackers claim they can easily crash the whole Internet (Mosquera, 1998), "hackivists' manipulate the Web sites of companies to discredit them (Goldberg, 1999), and the American Army's director of information systems says that the military does not "have a prayer or hope defending ourselves" against hacker attacks (Elvin, 1999), then there is potentially a very serious security problem for management. Wray (1999) feels that "electronic civil disobedience" will increase in volume and effectiveness. Many types of organizations can be targets of interest groups, for example, government departments (numerous issues), mining (environmental issues), pharmaceutical companies (animal rights issues), and banks (various issues). This list is easily expanded. As this is a new source of threat, it appears that many Australian businesses and government departments have not seriously considered it. The level of "passive" security is highly developed, but the potential for concerted, organized, and aggressive attacks from other than sole hackers has not been included in management thinking. The survey results outlined below tend to support this assertion.

A problem with the area of computer crime in Australia is ambiguity of the law. This is also confused by the potential international legal implications of foreign attacks. For instance, in the state of New South Wales, the Crimes Act 1900 (NSW), Section 310, states it is illegal to "destroy, erase, insert, or alter data in a computer system or interfere with, interrupt, or obstruct the lawful use of a computer" (Internet Law Bulletin, 1998, p.14). However, it is rare for these offenses to be detected, prosecuted, or proven.

Schwartau (1999, p.1) outlines the frustration of management in the American context and lists the following as the main causes:

- hacking events are increasing by huge numbers;
- the assaults are becoming more aggressive and hostile;
- the attack tools are automated and require few technical skills;
- political and social motivations have invited civil disobedience;
- investigation of hacking events is very difficult;
- law enforcement is not up to the task of investigating cyber crimes for lack of manpower, resources, and interest;
- corporate America distrusts law enforcement to prosecute and keep any investigations secret.

At this point, the definition of a "hacker' should be introduced. This has been the subject of debate in computing circles. Caelli et al. (1989) provide two