Chapter III

Information Systems Security:
Cases of Network Administrator Threats

Hamid Jahankhani
University of East London, UK

Shantha Fernando
University of Moratuwa, Sri Lanka

Mathews Z. Nkhoma
University of East London, UK

ABSTRACT

In today’s business environment it is difficult to obtain senior management approval for the expenditure of valuable resources to “guarantee” that a potentially disastrous event will not occur that could affect the ultimate survivability of the organization. The total information network flexibility achieved depends to a great extent on how network security is implemented. However, this implementation depends on the network designers at the initial stage and the network administrators in the long term. Initial security level designed can be later changed, improved or compromised by the network administrators who look after day-to-day network and system functions. Their competencies and the motivation contribute in achieving the desired security objectives that are aligned with the business goals. Incompetent network administrator may pave the way to attacks that could take place either at once where an obvious vulnerability may exist or in several phases where it requires information gathering or scanning in order to enter into the target system. De-motivated network administrator may ignore the possible threats or find strategies to make his/ her presence vital for the existence of the network services. The latter may be an example of a competent network administrator who is not rewarded due to the lapses of the senior management, in which case backdoors or logic bombs may be deployed so that the administrator may take vengeance in case the career is terminated or someone else is given undue recognition. Two studies on real cases given in this paper highlights the influence of such network administrators. To preserve the confidentiality, the names of personnel or organizations are not revealed.
INTRODUCTION

Security threats to business-technology systems keep growing and despite this increase, fewer businesses rank security as a high priority, fewer plan to boost security spending, and a growing number say money isn’t the biggest barrier to better security.

What do we want from secure computer systems? The advent of information technology has changed the face of doing business. Today, people through the information revolution can look at any part of business – whether an investment decision, an office building or an individual product – and examine all the individual costs to a single activity or good. Because of the convenience that IT provides, businesses had begun embracing it at an astonishing rate. The public and private sectors increasingly depend on information and telecommunications systems capabilities and services. In the face of rapid technological change, public and private organizations are undergoing significant changes in the way they conduct their business activities, including the use of wide area networking via public networks. These changes include mandates to reduce expenses, increase revenue, and, at the same time to compete in a global marketplace, (Potter, 2004).

Computers have found their way into all areas of business, industry, education, and government. Increasingly far-reaching information networks linking computers and databases provide important benefits, including greater staff productivity and a sharper competitive edge. The more that we expand the reach of our information networks, the more important network security becomes. The computer is the symbol of the modern, automated business. Its growing popularity plus the powerful business software, has resulted in an explosion of stand-alone data processing systems in many different departments of organizations throughout the world.

Further advancing the technology, information networks are now solving many work and productivity problems. Networks promote information exchange by interconnecting distributed departmental computers and associated terminals, printers, and other devices with centralized computers so that all units function as part of a single, unified communications system. Ideally, the result will be one, cohesive network in which authorized personnel can speedily and efficiently access computers and other system resources from any terminal or other device, whether they are in the same room, building, city, or even country. But whether this total information network flexibility is achieved depends to a great extent on how network security is implemented.

In today’s business environment it is difficult to obtain senior management approval for the expenditure of valuable resources to “guarantee” that a potentially disastrous event will not occur that could affect the ultimate survivability of the organization.

The need for a reliable security network was also heightened by the issue of cyber-crime, which involves hacking into computers, creating and spreading computer viruses, perpetrating online fraud schemes, and stealing trade secrets and other intellectual property.

Advanced level of network security provides maximum network flexibility as well as an additional layer of protection against unauthorized computer access. Moreover, this advanced security level also makes possible an audit trail of network usage. Another benefit is that a user authorization can be quickly and efficiently rescinded from the network. In general, this advanced security level can help reduce, if not eliminate, the need for costly additional security hardware such as data encryption devices.
