Chapter 5
Threats, Vulnerability, Uncertainty, and Information Risk

Eduardo Gelbstein
Webster University, Switzerland

ABSTRACT

This chapter explores the challenges of managing the risk associated with information assets. The word "challenges" is used to represent the complexity of the range of risks to consider and the fact that the management of information risk is not a skill commonly found among IT practitioners who are more likely to be "optimists" than "risk aware".

Two other matters complicate this topic: the lack of statistical data relating to cyber-attacks and the vulnerabilities inherent in hardware, software and networks, many of which are unknown until someone exploits them.

1. INTRODUCTION: THREATS AND ATTACKS

I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive.

We've created life in our own image. (Stephen Hawking (n.d.))

DOI: 10.4018/978-1-61520-831-9.ch005

Electronic devices – computers of all kinds, personal digital assistants and cellular telephones have been the targets of theft and electronic attacks for many years. The latter take many forms and are continuously becoming more sophisticated.

The forms of attack experienced so far, can be grouped in several categories: Vandalism, Infection, Disruption, Concealment and Data theft. In addition, there is a wide range of illegal and/or criminal activities such as espionage, interception, fraud and extortion.

Human ingenuity and creativity will undoubtedly find new ways to interfere with the smooth operation of information systems and data.

Vandalism attacks tend to cause little damage (apart from bruised egos and reputations) and can be quickly repaired, typically these involve defacing websites, which is relatively easy to do.

Infection attacks involve malicious software such as viruses, worms and spyware. While antivirus software has been effective in preventing and containing such infections, more recent malicious software (also known as malware) is reported to be able to bypass such defences.

Infection attacks have two components – a vector or delivery mechanism and a payload that causes damage. The vectors take many forms – from infected files (music, text, photographs) to infected CDROMs and USB flash memories – the latter, often together with social engineering, create an illusion of trust and result in an infected device used in a computer or photographic camera thus creating a chain of infection.

The payload can take many forms and may corrupt or delete data, capture keystrokes, track activity, send confidential information to a third party and more. Well designed payloads leave little or no trace of their activity.

Disruption attacks are intended to render the operation of a system, service or website impossible. Denial of Service Attacks, for example, swamp a network or a website with messages and cause to become inoperable. Infection attacks can also be disruptive as normal operations require all affected components to be sanitized and tested, both time an labor intensive.

Concealment attacks are designed not to be detected and allow those who launch them to take control of the target computer or device without the owner being aware of it. The payloads used for this purpose have names such as Trojan Horse, Rootkit and Backdoor. Professionally designed or "military strength" malware of this kind is difficult to detect and remove.

In October 2008 it was reported (Chip & Pin terminals, 2008) that Joel Brenner US National Counterintelligence Executive and Mission Manager for Counterintelligence, stated that point of sale equipment manufactured in China had been compromised by international criminal gangs by tampering during the manufacturing process:

It is believed an extra chip fixed to the back of the motherboard during manufacturing could have been responsible for large sums of money being taken from European customers' accounts. Customer card details, along with Personal Identification Numbers (PIN), were said to have been copied over a period of nine months and transmitted via mobile phone networks to fraudsters in Pakistan and that these may have raised funds to support terrorist activities. See also the Chapter in this book "What is Cyberterrorism and How Real is the Threat? - A Review of the Academic Literature, 1998 – 2008" by Maura Conway.

Data theft attacks are mainly conducted by industrial (and other spies) and organised crime with a profit motive. Terrorist and cyber-war attacks could use similar techniques to modify and corrupt data in critical information infrastructures.

2. TAKING THE MYSTERY OUT OF RISK TERMINOLOGY

"Risk" is a word in common use by both professionals and the general public. However, it means different things to different people and there is no shortage of definitions and methodologies to – perhaps optimistically – *manage* risk.

Traditionally, in statistical analysis and finance, risk is used to denote a probability of specific outcomes. In this approach "risk" is independent from the notion of value and, as such, outcomes may have both beneficial and adverse consequences – the classical expression being

Risk = (probability of an event occurring) * (impact of the event):