Chapter 28
Attackers: Internal and External

Eduardo Gelbstein
Webster University, Switzerland

ABSTRACT

Of the three groups of components of information security – tools, processes, and people- the last one should be considered as the weakest link. People range from the tired or unaware employee that clicks on a link that infects a computer or a network, to the security expert working for a criminal, military, or terrorist organization attacking a critical information infrastructure. This chapter examines the various classes of potential attackers and the techniques currently used to perpetrate such attacks.

THE INTERNAL THREAT

Hiding in plain view:

Place a tree in a forest – it becomes invisible.
Place a rock in a quarry – it becomes invisible.
A dishonest person within an organisation…
becomes invisible.

The insider threat has been well understood and recorded in history and literature. Two recent reports focus on the insider threat from the perspective of information systems and technology (Moore, Randazzo, Keeney, & Capelli, 2005, Doyle & Weiler, 2007).,

DOI: 10.4018/978-1-4666-4707-7.ch028

The first of these reports states that

- 62% of incidents were planned in advance
- 80% of the insiders involved showed unusual behaviour
- 60% had created backdoors or used shared accounts
- 50% had proper authorised access at the time of the incident
- 81% of the incidents resulted in significant financial losses
- 75% had high impact on business operations
- 28% damaged the reputation of the organisation

Should managers, worry about this? Absolutely!

Who Is an Insider?

The obvious answer is that "employees" of an organisation are insiders. But this is not the complete answer as there are many others that are given (or otherwise acquire) access to networks, data, systems, network hubs, computer rooms, telephone exchanges and other facilities. Among them:

Temporary employees sometimes supplied by an agency, interns (such as university students doing summer work related to their studies), contractors working on a project for the organisation, consultants and external auditors engaged for specific tasks that require them to spend time within the organisation.

Former employees who have left the organisation but whose access rights to networks, systems and services have not been cancelled. While everyone agrees that this should not happen, those responsible for maintaining access rights and systems privileges are not always informed of such departures (the same is true for changes in responsibilities within the organisation). When one of these employees had privileged rights (those of a superuser of some kind), the risk to the organisation is considerable.

Then, there are security personnel, building maintenance people and cleaners and many others of this kind who have access to the organisation's premises at various times. There are also the ICT vendors's maintenance technicians who have access to computer rooms. Increasingly, all of them are not staff but are contracted out and may change from one visit to the next.

With the trend towards outsourcing and offshoring, a new category of insider has emerged – the software developer and maintainer, the systems and network administrator that is recruited by an independent company, may reside in another country and may change without reference to the ultimate client. Background checks for such people are just about impossible to control and validate (if they take place at all).

Yet another category are visitors. In theory, such visitors are somebody's responsibility in the organisation, but when they have good social engineering skills, they can be willingly taken to visit a computer room and, depending on the security culture of an organisation, they may be allowed unescorted access to office buildings. A polite, suitably dressed person can take advantage of the basic human inclination to be helpful to gain a considerable amount of confidential information through friendly dialog and sharp observation – and if they are really good, be given access to systems.

All of these people can – at one time or another – fall into one of the following categories:

1. The good, conscientious and aware insider (the good guys);
2. The good guy having a bad day suffering from one or more of: overwork, tiredness, feeling unwell, under pressure to finish a task, inability to concentrate, stress, forgetfulness, etc;
3. The person that used to be a "good guy" and whose emotions become stronger than conscience or common sense – passed over for promotion, having personal problems or having fallen out with a colleague or a boss;
4. The not-so-competent IT professional or worse, the IT enthusiast who is given responsibility for IT management and operations, who fails to do the job to an adequate level of quality;

These people tend to be found in "job-for-life" organisations where poor performance is accepted (or at least tolerated) and where the mechanisms to ease someone from a job are too complex and troublesome to be pursued.

5. The less conscientious and/or unaware insider who, with the best of intentions may do something stupid;