Principles for Managing Information Security

Rana Tassabehji
University of Bradford, UK

A BRIEF HISTORY

Information security has traditionally been the responsibility of information technology (IT) departments, where information security has commonly been perceived to have a technological solution. During the 1980s, computer usage was mainly concentrated in computer centres, where the implementation of computer security focused largely on securing the physical computer infrastructure of the organisation (Mutsaers et al., 1998), which proved highly effective.

The advent of cheaper and more powerful microprocessor, computing and networking technology dramatically changed the nature of computer usage in organisations. In the 1990s, the majority of employees had a workstation or personal computer through which they could directly access, process and manage any number of available corporate resources, such as software, hardware and information, to execute a wide range of tasks. In line with this, IT security developed additional technical measures that incorporated software residing on IT systems. These were able to deal with the increasingly new and varied attacks resulting from the wide use of distributed and inter-networked computers (Von Solms 1999; Vermeulen & Von Solms, 2002).Examples of these developments in IT security included user identification and authentication, memory clearance and access control to data.

The ubiquity of the Internet and e-mail has continued to increase the importance of information and related technology in organisations. In today's information economy, information is one of the most important assets for an organisation (Turner, 2000). Possession of strategic information can make the difference between an organisation's success and failure (Forcht, 1994). Not only information, but also the systems that support it, have become a critical part of an organisation's business and assets — a fact of which many attackers are well aware. According to a number of surveys (PricewaterhouseCoopers, 2002, 2004; Computing Technology Industry Association, 2003, 2004; Richardson, 2003), attacks on corporate information systems have been increasing year after year, with the costs of the security breaches in terms of disruption, damage and loss also increasing. These surveys are probably an underestimation of the total number of security breaches that have occurred, since breaches can go undetected or are unreported and not publicised for fear of repercussions (negative publicity or lawsuits). One of the cardinal rules for effective management of security is to say nothing about security. So with the prominence of information also comes the heightened importance of securing information and managing the security process.

THE INTERNET AGE

As well as being a core business asset, information systems are increasingly recognised as socio-technical infrastructures that rely heavily on people. In recent years, it has become more widely acknowledged that human factors play a part in many security failures (Weirich & Sasse, 2002). As such, managing information security has begun to move out of the technology department as the sole source of responsibility and solutions to a more holistic organisational approach that incorporates business processes, controls and policies; corporate governance; systems and technology infrastructures; human resource management and training; and organisational culture (Higgins, 1999; Gelbsein, 2001; Eloff & Eloff, 2003; Tassabehji, 2003). Empirical evidence supports this view: a survey by McKinsey (McKinsey Quarterly, 2002) found that although only 6% of Fortune 500 companies had appointed a senior business executive to oversee information security, this figure was expected to rise over the next few years, as strategic, operational and organisational safeguards are added to the technological measures being employed to protect corpo-

rate information. One of the main catalysts that has mobilised organisations to think more seriously about information security is the introduction of new and modified legislation (such as the Data Protection and other Electronic Communications Acts). There is now international legal recognition of the importance of information and the need to secure it. Organisations must ensure that data is protected as the legal responsibility for protection falls fully on the organisations that collect, store, share and use the data.

THEORY

There is very little academic theory that deals solely with managing information security. The majority of publications on the topic are largely practitioner based, relying on standards, benchmarks, best practice, technical specifications, security frameworks and models. Hong et al. (2003) identify five theories that define approaches to the management of information security:

- **Security policy theory:** aims at establishing, implementing and maintaining an organisation's information security requirements through a security policy.
- **Risk management theory:** evaluates and analyses threats and vulnerabilities of information assets in an organisation. It also includes the establishment and implementation of control measures and procedures to minimise risk.
- **Control and audit theory:** suggests that organisations should establish control systems (in the form of security strategies and standards) with regular auditing to measure control performance.
- **Management system theory:** establishes and maintains a documented information security management system. This includes an information security policy that incorporates factors internal and external to the organisation; the scope of the policy; risk management and implementation of the process.
- **Contingency theory:** information security is a part of contingency management that prevents, detects and reacts to threats and vulnerabilities internal and external to an organisation. This incorporates all the other approaches identified above in order to manage the threats.

Although these are presented as separate theories or approaches, they are not mutually exclusive. Each of the above approaches incorporates one or more of the other elements but from different perspectives that emphasise specific issues. Hong et al. (2003) highlight some limitations of each of the theories — for instance, all except contingency theory take a top-down approach, which may not be consistent with reality. They posit an "integrated system theory" based on contingency management and which also integrates information security policy, risk management, internal control and information auditing theories to form an Information Security Architecture consistent with organisational objectives. However, this integrated theory does not detail the measures under which each of the approaches functions or interacts with the other. It is an outline framework that attempts to take a holistic approach to information security management in the same vein as other information security academics such as Eloff (1998), Van Solms (1999) and Higgins (1999) but focusing on the development of a more "theoretical" framework.

THE MAIN COMPONENTS

Whatever the emphasis that an organisation places on managing information security, the main components that must be included are organisation and IT infrastructure; risk assessment and management; security policy, standards and procedures; security awareness and training programmes; monitoring, auditing, reviewing; and updating policies and processes.

Each of these five major components is linked together in a cyclical feedback process, where they are all interdependent and as a holistic process contribute to the overall security of the organisation's information. Each of the five components will be discussed in detail in the following sections.

Organisation and IT Infrastructure

It is widely recognised in management theory that commitment and support from top management is