Introduction

This book explains how.

CHAPTER 1: INFORMATION ECONOMY, INTELLECTUAL CAPITAL

Executive summary

In the information economy, businesses depend on information and a substantial proportion of their value is made of intangible and information assets. The board has a fiduciary duty to protect and preserve these assets.

The information economy

The new information, or knowledge, economy is (as we all know) fundamentally different from the old manufacturing one. Information interchange has speeded up the globalization of markets, products and resourcing. This has lead to increasingly similar shopping streets selling increasingly similar products throughout the developed world. Over 70% of workers in developed economies are now knowledge, rather than manual, workers – including those factory and farm workers whose work depends on understanding and using information technology. Information networking and telecommunications connectivity make this ‘global village’ possible – and bring a number of specific business threats and challenges at the same time.

The key characteristics of the global information economy, in contrast to those of the older manufacturing one, are:

- Information and knowledge are not depleting resources to be protected; on the contrary, sharing knowledge drives innovation;
- Effects of location and time are diminished – virtual organizations now operate round the clock in virtual marketplaces, and organizations based on East Coast

CHAPTER 3: INFORMATION THREATS

Executive summary

All organizations possess information, or data, that is either critical or sensitive. This information is a substantial component of the organization's intellectual capital. 'Information is widely regarded as the lifeblood of modern business.'[5] 87% of businesses now identify themselves as 'highly dependent' on electronic information and the systems that process it. This information faces a range of threats, some simple, some complex, and all with the potential to significantly damage an organization.

Threats

Threats in the digital world, as in the analogue one, originate with people. These people fall into five groups:

- Criminals (thieves, fraudsters, organized crime),
- Malefactors (hackers, vandals, terrorists, cyber-warriors, some ex-employees and other disgruntled or vengeful individuals),
- Spies (commercial and governmental),
- Undesirables (scam artists, spammers, 'ethical' hackers and nerds), and
- The incompetent, or the simply unaware (staff, contractors, customers and other third parties).

From an organizational perspective, these people are found both inside and outside the organization (the balance overall is probably 50:50). There are a substantial number of people in each category

[5] Information Security Breaches Survey 2004, from the UK's Department of Trade and Industry

4. Insecurity impacts

ISO 27001

Deployment of an ISMS developed in line with the international standard of information security best practice is the fundamental step toward effective information security governance.

organized crime groups can operate…High technology crime will continue to represent one of the major areas of crime in the future, paralleling the development of e-commerce and internet banking.'

The Computer Security Institute (CSI), with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, has now conducted nine annual surveys into information security at the CSI member firms. The results of the most recent survey showed that 2004 total financial losses to criminal abuse, across the 269 respondents who participated, was $141 million. While the biggest loss arose from virus attacks ($55 million) and denial of service attack ($26 million), $11 million of these losses was from theft of proprietary information against $8 million for financial fraud and $7 million in laptop thefts. It was clear that nearly half of those who took part in the overall survey were unable (because they had no method of tracking) or unwilling (because of the possible reputational damage) to provide estimates of their financial losses from the successful attacks they had experienced. Equally clear is the fact that incidents of cybercrime originate equally from outside and inside the attacked computer systems.

The conclusions of the Confederation of British Industry's (CBI) 2001 Cybercrime Survey, which polled 154 member firms and found that two-thirds of them had suffered serious computer crime in the previous twelve months, are even more valid today. Nearly 60 per cent predicted that cybercrime would become even more of a problem in the future. The Director-General of the CBI, Sir Digby Jones, was quoted as saying, 'Fears about potential losses and damage to reputation from cybercrime are stalling the growth of e-business, especially for b2b transactions. That growth will only come when all parties are reassured that adequate security is in place to protect them.'

'Over its seven-year lifespan' concluded the CSI, 'the survey has told a compelling story. A sense of the "facts on the ground" has emerged. There is much more illegal and unauthorized activity occurring in cyberspace than corporations admit to their clients,

CHAPTER 15: RECORD RETENTION AND DESTRUCTION

Executive summary

Legislation, regulation, business contracts and prudence mandate the retention of specific records. These records are largely electronic (including e-mail) and their confidentiality and integrity needs to be protected throughout the period of retention, and they need to be accessible – in spite of intervening technology upgrades and system changes.

Records

An increasingly wide range of organizational and individual records (including e-mail, voice mail and Instant Message communications) must be retained to meet statutory or regulatory requirements, while others may be needed to provide adequate defence against potential civil or criminal action or to prove the (current and historic) financial status of the organization to a range of potential interested parties, including shareholders, tax authorities, auditors and to meet contractual liabilities. Records should be kept in a format that can prove they have not been tampered with, and so that they can be found many years later. This implies that organizations need an effective archive management policy and, inevitably, appropriate technology. Records do not (and should not) be kept for ever – this can make it difficult to find what is required as and when it is required, and the cost of storage is likely to be increasingly expensive.

Therefore, time limits – based, in each instance, on the maximum retention period identified in any of a statute of limitations, relevant legislation (including tax and company legislation) or specific regulatory requirements - should be set for the retention of each individual category of information. Information lifecycle management automates the process of moving information from