

CONTENTS

INTRODUCTION

CHAPTER 1: INFORMATION ECONOMY, INTELLECTUAL CAPITAL

CHAPTER 2: INFORMATION, IT AND COMPETITIVENESS

CHAPTER 3: INFORMATION THREATS

CHAPTER 4: INSECURITY IMPACTS

CHAPTER 5: 'TRADITIONAL' THREATS

CHAPTER 6: INFORMATION RISK IN LARGE ORGANIZATIONS

CHAPTER 7: ORGANIZED CRIME

CHAPTER 8: TERRORISM

CHAPTER 9: EVOLVING THREAT ENVIRONMENT

CHAPTER 10: REGULATORY COMPLIANCE

CHAPTER 11: DATA PROTECTION AND PRIVACY

CHAPTER 12: ANTI-SPAM LEGISLATION

CHAPTER 13: COMPUTER MISUSE LEGISLATION

CHAPTER 14: HUMAN RIGHTS

CHAPTER 15: RECORD RETENTION AND DESTRUCTION

CHAPTER 16: INFORMATION SECURITY GOVERNANCE

CHAPTER 17: BENEFITS OF AN ISO 27001 ISMS

CHAPTER 18: ISO 27001 IN THE PUBLIC SECTOR

CHAPTER 19: IS ISO 27001 FOR YOU?

CHAPTER 20: HOW DO YOU GO ABOUT ISO 27001?

CHAPTER 21: SELECTION OF A CERTIFICATION BODY

APPENDIX: ISO 27001 – PAST, PRESENT AND FUTURE

Links to other standards and regulatory frameworks

Useful websites

INTRODUCTION

The replacement, in late 2005, of BS 77799 by the international information security management system standard ISO 27001 marks the coming of age of information security management.

In the first eight years that BS7799 existed as a standard against which organizations could gain an external certification, about 1,000 were successful, worldwide. This number doubled in the subsequent twelve months. With the internationalization of BS 7799, that number will grow geometrically. This books looks at why organizations are increasingly turning to this information security management standard.

By far the most common drivers for organizations that have, historically, been successful in achieving BS 7799, “were commercial: to increase the confidence of customers, or possibly to encourage suppliers, when dealing with the organization.”¹ For others, according to the same survey, an information security management standard is “becoming an increasing requirement in tender documents, as well as contracts” and, for a very sizable minority, gaining a competitive advantage over their competitors has been equally important.

Technology – specifically information technology - is transforming the economic and social worlds in which we work, play and live. Whether or not this is a good thing is irrelevant. The fact is that, for most people, information was stored, twenty years ago, on pieces of paper. Small numbers of large mainframe computers batch-processed mundane transactions and a credit card application could take several weeks. Corporations wrote their own computer programs and avoiding GIGO (garbage in, garbage out) was the Head of IT’s

¹ Information Security BS7799 Survey 2005 – Information Security Ltd

objective. Fax machines were transforming a business communication infrastructure that still depended on expensive fixed telephone lines. Information, when it existed, was hard to lay your hands on and even harder to use, manipulate or transform.

Today, ‘information overload’ is a commonplace complaint. Computers are ubiquitous, communication can be globally instantaneous, and someone else can get a credit card in your name in a matter of minutes.

As we’ve shifted from a manufacturing to an information economy, the structure of organizational value has changed dramatically. The intangible assets (mostly intellectual capital) of most OECD organizations are now worth substantially more than their tangible assets and this trend is unlikely to reverse.

Information is the life blood of the modern business. All organizations possess and use critical or sensitive information. Roughly nine-tenths of businesses now send e-mail across the Internet, browse the web and have a website; and 87% of them now identify themselves as ‘highly dependent’ on electronic information and the systems that process it.. Information and information systems are at the heart of any organization trying to operate in the high-speed wired world of the 21st Century.

Business rewards come from taking risks; managed, controlled risk taking, but risk taking nonetheless. The business environment has always been full of threats, from employees, and competitors through criminals and corporate spies to governments and the external environment. The change in the structure of business value has led to a transformation to the business threat environment.

The proliferation of increasingly complex, sophisticated and global threats to this information and its systems, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is forcing organizations to take a more joined-up view of information security. Hardware-, software- and vendor-driven solutions to individual information security challenges

no longer cut the mustard. On their own, in fact, they are dangerously inadequate.

News headlines about hackers, viruses and online fraud are just the public tip of the data insecurity iceberg. Business losses through computer failure, or major interruption to their data and operating systems, or the theft or loss of intellectual property or key business data, are more significant and more expensive.

Organizations face criminal damages, reputation loss and business failure if they fail to adequately secure their information. Directors face loss of personal reputation and jail time if they fail in their duty to protect the information their organizations are holding.

But computer security technology, on its own, simply does not protect information. On its own, it just wastes money, gives a false sense of security and decreases business efficiency. What organizations need is a structured method for identifying the real information risks they face, the financial impact of those threats, and appropriate methods of mitigating those specific, identified risks. Securing information is not rocket science, whatever the technology vendors might say. Information is at risk as much through human behaviour (and inattention) as it is through anything else. Securing information therefore requires an approach that is as much about process and individual behaviour as it is about technological defences.

And no organization has either the time or the resources to try and work out, on its own and from first principles, how to do this effectively. Apart from anything else, the time and error profile is likely to be unattractive.

No organization needs to. ISO27001 already exists. This standard, which contains current information security international best practice that has already been successfully implemented in more than a thousand organizations around the world, gives organizations a reliable and effective framework for deploying an information security management system that will preserve its assets, protect its directors and improve its competitiveness.

This book explains how.