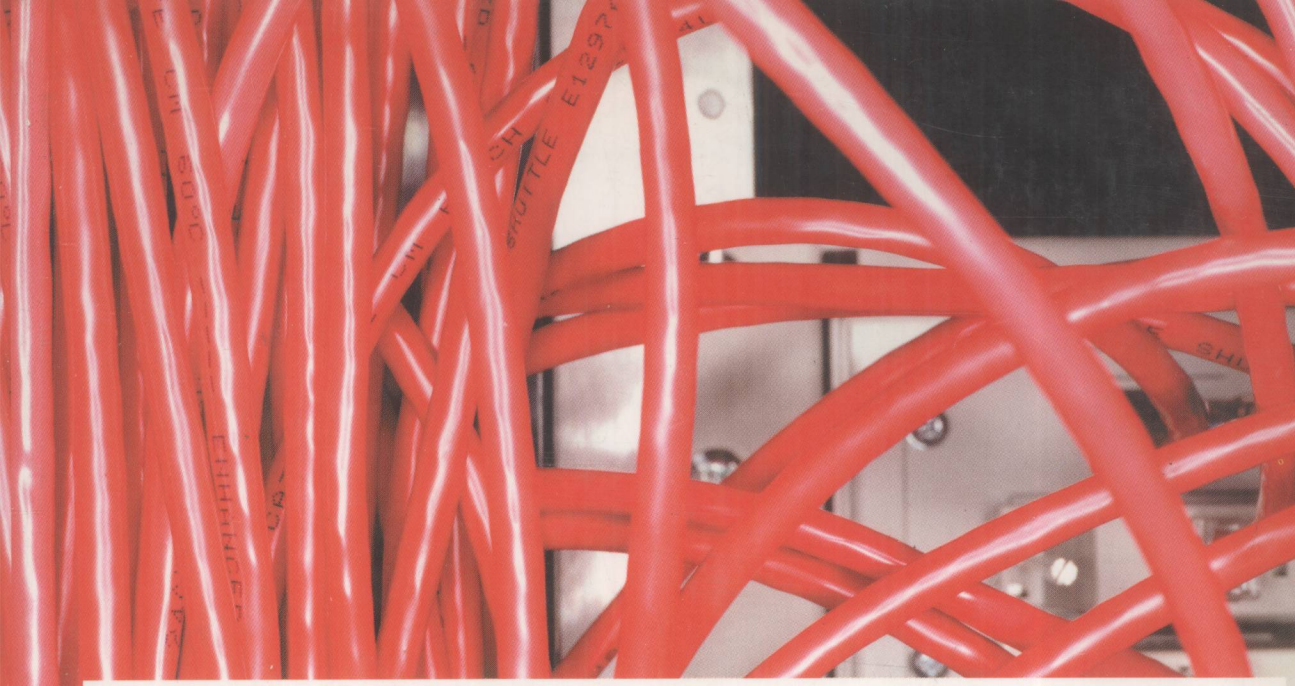
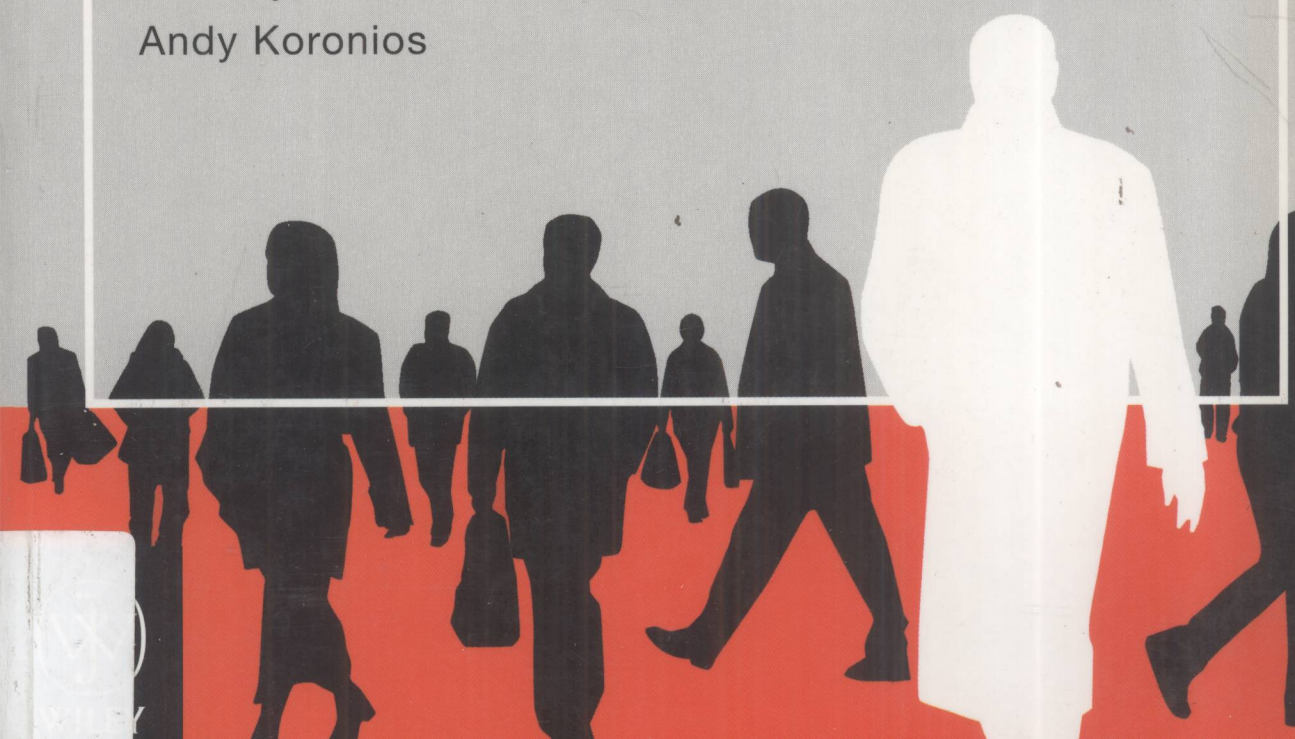


Information Technology Security & Risk Management

Jill Slay
Andy Koronios



Information Technology Security & Risk Management

Jill Slay
Andy Koronios

WILEY
John Wiley & Sons Australia, Ltd

Third edition published 2006 by
John Wiley & Sons Australia, Ltd
42 McDougall Street, Milton Qld 4064

Offices also in Sydney and Melbourne

Typeset in 11.5/14 Minion

National Library of Australia
Cataloguing-in-Publication data

Slay, Jill.
Information technology security and risk management.

Includes index.
ISBN-13 9 78047080 5749.
ISBN-10 0 470 80574 9.

1. Computer security. I. Koronios, Andy. II. Title.

005.8

Edited by Cathryn Game

Printed in Singapore by
Markono Print Media Pt Ltd

10 9 8 7 6 5 4 3 2 1

About the authors

Dr Jill Slay holds a degree in mechanical engineering, graduate diplomas in applied computing and further education, and a PhD from Curtin University of Technology. Jill spent several years working as an engineer in the UK before beginning a career in applied computing, and spent many years living and working in Asia. She is a member of the Australian Computer Society and the Institute of Electrical and Electronic Engineers and a Certified Information Systems Security Professional. She has extensive teaching experience in the tertiary sector at undergraduate and postgraduate levels and is currently teaching IT security and forensic computing courses in Australia and Asia.

She is a senior lecturer in the School of Computer and Information Science at the University of South Australia and leads the Enterprise Security Management Laboratory in the Advanced Computing Research Centre of the School of Computer and Information Science. She is also an affiliate faculty member at Idaho State University and is a board member of the newly formed Colloquium on Information Systems Security Education — Asia Pacific.

Jill has published five book chapters as well as numerous research papers in such areas as science education, multimedia and intelligent tutoring systems, complex systems and culture, information and electronic commerce security and forensic computing. She is also a member of several editorial boards and conference committees.

Currently, she carries out collaborative research in forensic computing and IT security with industry and government partners in Australia and the USA.

Professor Andy Koronios holds degrees in electrical engineering and education, a Master of Letters and a PhD from the University of Queensland. He has spent a number of years consulting in the IT industry and business management. Andy has extensive computing experience in the commercial environment, especially in small to medium-sized enterprises and was managing director of several enterprises.

He has extensive teaching experience both in the tertiary sector at undergraduate and postgraduate, MBA, DBA and PhD levels as well as in the provision of executive industry seminars. He has also provided professional seminars to IT executives in South-East Asia. In 1995 he was the USQ recipient of the Award of Excellence in Teaching.

He has served in a variety of university management posts, including coordinator of studies, head of program, head of department and head of division, and is currently the Head of School of Computer and Information Science at the University of South Australia.

Andy has published five books and one chapter as well as numerous research papers in such diverse areas as multimedia and online learning systems, information security and data quality, electronic commerce and Web requirements engineering.

Andy has regularly appeared on Australian radio (4QR and Radio National) and television commenting on a variety of issues pertaining to IT.

Currently, he is the research program leader of the Systems Integration and Information Technology Program in the CRC for Integrated Engineering Asset Management. Professor Koronios is the director of Strategic Information (SIM) Laboratory in the Advanced Computing Research Centre of the School of Computer and Information Science at the University of South Australia.

Preface

Modern society owes a lot to the Internet and related technology. This technology, on one hand, enriches the economic, political and social lives of the global population and on the other hand has rendered the security of communities, businesses and nation states vulnerable. Be it competition among businesses or a full-scale military conflict, new forms of intrusion into information systems and manipulation of information contained in them are being devised by businesses, communities, nation states and even individuals to impose their will on their adversaries.

Until recently, computer security was regarded as a non-productive activity. It was broadly accepted as 'support activity', where keeping back-ups of data was all that was deemed necessary, except for the military and the banking and aerospace industries. However, recent political developments have shown the corporate world that computer security is as important to it as ideological and physical security is to a sovereign country. Natural disaster, wars and terrorist attacks disrupted millions of computer operations and had a telling effect on business execution; in certain cases even on the survival of the business. Businesses have now realised that computer security actually maintains their lifeline and that they cannot afford any breach of computer security. Consequently, they are increasingly endorsing defensive measures to protect their information and information-related resources from breaches of security occurring inside and outside the organisation. However, a fundamental issue with information technology is that its security concerns are evolving alongside the development of technology; therefore it is difficult for a business manager to fully appreciate the scale of the problem at hand.

For this reason, this book provides a comprehensive approach to ensuring computer security. It serves the purpose of being a textbook as well as a reference book. Its intended audience is undergraduate and graduate students as well as practitioners. The layout of this book helps readers in understanding the way various security issues are identified in routine business activities, and it provides recommendations on the tried and tested security controls and safeguards. Although no background knowledge in computer security is necessary, we assume that readers are familiar with basic concepts, such as operating systems, and different communication and hardware architecture.

This book has four major goals. The first and foremost goal is to provide clear and precise understanding of the theory and practice of computer security in the emergent business paradigm. It is essential for business managers to recognise the theoretical underpinnings to computer security, such that they are able to apply best available controls to safeguard capture, exchange and storage of information and information-related resources. Computer security theory presented in the book equips readers to evaluate different security strategies, mechanisms and procedures according to business needs, thereby helping them to make informed decisions about security management. For example, the discussion on security models, such as the lattice and Clark-Wilson models, is followed by the tools and techniques available to implement these models. In this way, security designers not only have an understanding of the available security frameworks but also have an appreciation of the building blocks for their implementation.

The second goal is to provide insights into intranet- as well as extranet-based electronic commerce security issues and their defence, such as secured electronic payment systems, mobile commerce security issues, cryptography and its application to the electronic business environment. The book examines the foundations of network security

and looks at system security issues, such as securing information flow by appropriate hardware and software controls, which include routers, firewalls, intrusion detection systems, network separation, operating systems and anti-virus software. Quite appropriately, the book also discusses security risks arising from the use of wireless networks and mobile and wireless devices. This discussion paves the way for understanding and implementing cryptography, under which the book discusses the popular types of cryptographic ciphers and provides comparisons of fundamental symmetric and asymmetric cryptography by looking at common algorithms.

The third goal is to reveal that computer security is not just a collection of technological controls; in fact it is strategic business activity and should be treated as such. The book clearly entails that a technological solution to computer security alone cannot insulate an organisation from security breaches, and therefore a comprehensive security plan must, in addition to technological controls, include security policies and procedures, policies or codes of conduct aimed at educating and enlightening employees on security assurance. These policies and procedures should reflect the business environment, such as elucidating how people within an organisation as well as from outside it gain access to the organisation's information resources. How can employees ensure that their information technology privileges are not abused by themselves or by other unauthorised third parties? What are the confidentiality requirements and provisions that an organisation demands from its employees?

The fourth goal is to provide an understanding of the issues that the public at large is facing from the masking of information semantics and forensics in Australia. Ever since the emergence of the Internet, the general public has been at the risk of being overwhelmed by the many ways in which information could be manipulated for unlawful and unethical purposes. Apart from discussing privacy and fraud issues on the Internet, the book particularly discusses the application of computer technology to the investigation of computer-based crime with a view to providing readers with an understanding of the field of forensic computing. Nevertheless, any discussion on security will be incomplete without touching on its future trends; therefore the book discusses emerging technology and related security issues.

Jill Slay
Andy Koronios
November 2005

Acknowledgements

As teachers, we have made use of ideas workshopped and tested in our undergraduate and postgraduate teaching in writing this book, and we are particularly grateful for the insights shared by many students over the past few years in the School of Computer and Information Science at the University of South Australia. As researchers, we have drawn on concepts developed as part of continuing research projects, particularly those centred in our labs in the Advanced Computing Research Centre. We are particularly grateful to Ben Turnbull, Phil Pudney and Tom Wilsdon, who allowed us to draw on their research, and to Eliud Kamau and Jing Gao, who both supported us in the preparation of this book. Abrar Haider has been of invaluable assistance to Andy.

The author and publisher would like to thank the following copyright holders, organisations and individuals for their permission to reproduce copyright material in this book.

Images

Pp. 8–9: 2004 Australian Computer Crime & Security Survey, page 17, reproduced with the permission of the copyright owner, The University of Queensland trading as AusCert; **p. 24:** 2004 Australian Computer Crime & Security Survey, page 7, reproduced with the permission of the copyright owner, The University of Queensland trading as AusCert; **p. 25:** 2004 Australian Computer Crime & Security Survey, page 8, reproduced with the permission of the copyright owner, The University of Queensland trading as AusCert; **p. 14:** *Business Continuity Management Better Practice, A Guide to Effective Control — January 2000.* Australian National Audit Office, © Commonwealth of Australia reproduced by permission; **p. 147:** Microsoft Corporation; **p. 112:** Symantec, http://securityresponse.symanted.com/avcenter/venc/data/pf/w32.mimail.s@mm.html; **p. 285:** © 2002 World Wide Web Consortium, (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All rights Reserved http://www.w3org/Consortium/Legal/2002/copyright-documents-20021231.

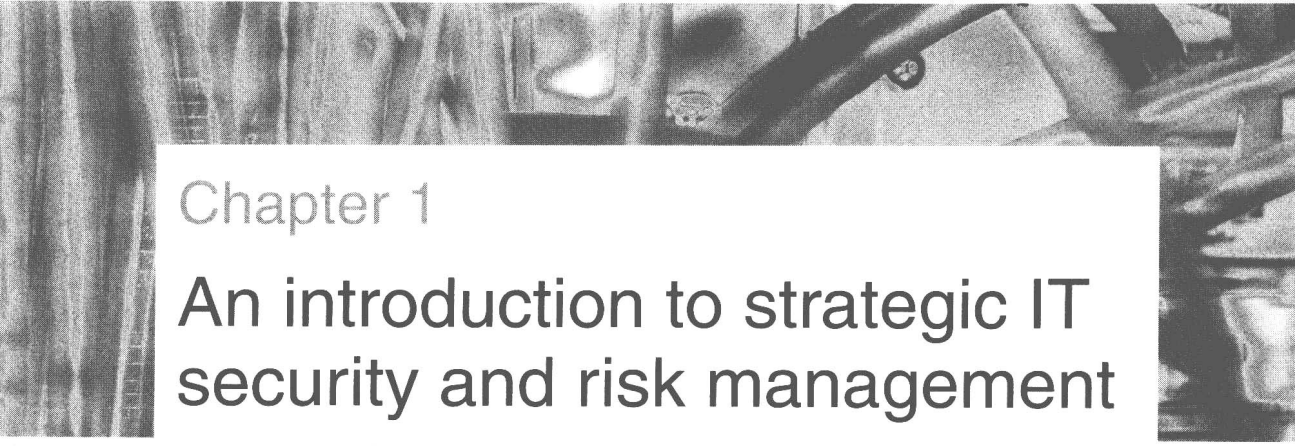
Text

Pp. 107–9: 2004 Australian Computer Crime & Security Survey, page 21, reproduced with the permission of the copyright owner, The University of Queensland trading as AusCert; **p. 70:** appears on Link: http://www.acs.org.au/about_acs/acsregs.htm#nr4, © 2003 Australian Computer Society Inc. reproduced with permission; **p. 80:** Reproduced by kind permission of The Australian Copyright Council. Appears on link http://www.copyright.org.au/publications/G056.pdf; **p. 81:** Reproduced with kind permission of The Australian Copyright Council, www.copyright.org.au; **p. 77:** Guidelines for companies about avoiding spam/Department of Communications, Information Technology and the Arts and Australian Communications Authority 2004. available at: www.acma.go.au, © Commonwealth of Australia reproduced by permission; **pp. 218–19:** Bill Goodwin, Computer Weekly.com, 22 March, 2005. Appears on link: www.computerweekly.com/Articla137434.htm#; **p. 293:** by Bill Goodwin, Computer Weekly.com, 21 September 2004. Appears on Link: www.computerweekly.com/Articles/2004/09/20/205302/Webserviceslooksettobethenextbigrisk.htm; **p. 110:** Craig Valli © 2002; **p. 71:** (ISC)_, http://www.isc2.org/cgi/content.cgi?page=31; **pp. 33–5:** Johnson & Johnson tackles security pain, by Ellen Messmer, Network World, 03/14/05; **pp. 302–4:** Web services you can bank on, by Beth Schultz, Network World, 12/27/04; **pp. 331–3:** Risks rise as factory nets go wireless, by Phill Hochmuth, Network World, 03/14/05; **pp. 207–8:** *Waikato Times*, October 21st, 2004. Appears on link: http://www.smh.com.au/articles/2004/10/21/1097951802576.htm.

Every effort has been made to trace the ownership of copyright material. Information that will enable the publisher to rectify any error or omission in subsequent editions will be welcome. In such cases, please contact the Permissions Section of John Wiley & Sons Australia, Ltd, who will arrange for the payment of the usual fee.

Brief contents

Contents



Chapter 1

An introduction to strategic IT security and risk management

Learning objectives

After studying this chapter, you should be able to:

- outline the risk management process
- explain business continuity management
- explain IT governance
- explain the importance of IT security and risk management
- discuss the role of IT in the business environment
- outline the types of risk that can threaten IT systems
- discuss the types of control that can be implemented to prevent or correct IT risk events
- explain the actions required to sustain the IT risk management strategy
- discuss the essential elements of an IT continuity plan
- explain how the business can ensure that its security and risk management strategy is followed.

Chapter overview

Modern information and communication technology has opened new opportunities for businesses in the areas of automation, interconnectivity and e-commerce as well as enabling the development of entirely new products and services. At the same time the adoption of this technology has exposed businesses to new risks — ranging from fires and floods to cyber criminals and cyber terrorists — that need to be managed. This chapter will look at the risk management process, which assesses the risks facing a business and designs steps to minimise those risks and to help the business recover should an adverse event occur. We will then look at business continuity management, which focuses on the business's plan to deal with those risks that have the potential to prevent it from achieving its key business objectives. Together, risk management and business continuity management form a complementary approach to protecting the business. An obligation under IT governance is to mitigate the IT risks facing the business. IT plays an integral part in today's businesses, and the risks affecting IT processes must be identified and managed to reduce the organisation's vulnerability. This is the core theme of this book. IT security and risk management are not ends in themselves; they are employed to support the overall business objectives.

Using a risk management framework, we will examine the IT risks, focusing particularly on the business context of IT, the types of risk that can threaten IT systems, the steps businesses can take to reduce their risks and the things that need to be done to maintain an IT security and risk management strategy. We will then look at the essential elements of an IT continuity plan.

Strategies and plans are useful only if they are implemented and adhered to. We will look at ways in which the business should go about ensuring that its IT security and risk management strategy is properly used. Finally, we will outline the key IT security issues that will be discussed throughout the rest of this book.

Risk management

Risk management is an ongoing process designed to assess the likelihood of an adverse event occurring, implement measures to reduce the risk that such an event will occur and ensure the organisation can respond in such a way as to minimise the consequences of the event (ANAO 2000). A risk is any event that has the potential to prevent the business achieving its objectives. In Australia and New Zealand, Australian Standard/New Zealand Standard 4360 'Risk Management' provides a framework to identify, analyse, assess, treat and monitor risks. HB 231 'Information security risk management guidelines' provides guidance specific to information security risk management.

An appropriate risk management process involves the following steps (AS/NZS 4360; HB 231; ANAO 2000):

- *Establish the organisational and risk management context.* This step defines the business objectives and the key business processes and resources that support those objectives.
- *Identify, analyse and evaluate significant business risks.* This step involves several actions:
  - It seeks first to *identify* the risks a business might face. Risks can be external or internal. External risks include: political, legal and administrative changes; economic and market changes; natural events and disasters; and technological factors, such as infrastructure failures or hacking. Internal risks can be strategic or operational in nature (ANAO 2000).
  - The risk *analysis* assesses the likelihood of each identified event occurring and the consequences given the current controls in place. It determines which risks are acceptable and which are not, on the basis of their effect on the business's outputs, resources, reputation, legal compliance and continuity.
  - The risk *evaluation* ranks the risks to establish the relative priority of managing each risk.
- *Design and implement preventive and corrective controls.* Responses to risks include accepting the risk, controlling the risk and transferring the risk. The controls could be aimed at stopping the risk from occurring (called preventive controls) or at minimising the consequences should the preventive controls fail and the event occurs (corrective controls). This step designs these controls and puts them in place. The business continuity plan, described on pp. 27–9, is one of the corrective controls.
- *Monitor and review the risks and controls.* Risk management is an iterative process. The business must regularly review the strategic and operational risks it faces and test and modify the controls to ensure that they effectively deal with changes to the risks.

Risk management requires the investment of resources (time, money and effort) to prepare the organisation for unforeseen circumstances. There will always be a trade-off between the resources invested against the risks faced and the probability that they will eventuate. Some risks threaten the continuity of the business's operations. Risks of this scale must be effectively managed. Hence business continuity management (discussed below) is an integral part of the risk management process. It prepares the business for when the preventive controls — implemented as part of the risk management process — have failed.

Business continuity management

Business strategies are based on the presumption that the business will continue to operate into the future. Any event that disrupts the continuation of business operations has significant consequences for the business and directly affects its ability to accomplish its objectives and those of its stakeholders. It can cost

revenue, reputation, investor confidence and customer loyalty. Business continuity requires that the resources supporting the essential business activities are always available. Clearly, then, **business continuity management (BCM)** is a broad concept that covers the entire business and so it must encompass information technology. The concept of BCM is receiving increasing attention from the business world. BCM is part of risk management. In theory BCM:

- identifies those risks that have the potential to interrupt the normal course of business operations
- implements preventive controls to prevent the occurrence of such risks
- develops corrective controls for coping should the preventive controls fail and the risk eventuates (ANAO 2000).

The overlap with risk management is obvious, but whereas risk management is concerned with all of the potential risks that face a business and their likelihood of occurring, business continuity management is concerned just with those events that have the potential to interrupt the achievement of the business's objectives. The likelihood of their occurring is only relevant in determining the cost–benefit trade-off of controls. It prepares for all risks to business continuity, regardless of the likelihood of their eventuating. Any other approach leaves the business vulnerable should the unlikely occur (even if very unlikely). The scope of business continuity extends beyond the enterprise: it also considers external risks arising from political, economic and natural changes in the business environment, making use of such business tools as a SWOT (strengths, weaknesses, opportunities, threats) analysis.

The business continuity management process involves (ANAO 2000; Savage 2002):

- *Initiation.* This step establishes the objectives, personnel and responsibilities, budget and schedule. It recognises that the business is not in complete control of its environment and will in all likelihood one day face a threat to its continuity (Smith 2003).
- *Identification of key business processes.* This step identifies what resources and activities are essential to support the strategic, operational and support processes that produce the outputs that fulfil the key business objectives. It also ranks each business process according to its importance in achieving the business objectives.
- *Business impact analysis.* This step determines the impact on the business should a business process be disrupted. It establishes the maximum tolerable downtime for each business process and hence the priority for recovering those processes should an adverse event occur. Jordan and Musson (2003) report that 46 per cent of Australian government organisations believe they need to recover their critical services in less than eight hours in order to ensure that their business objectives are not threatened. A further 15 per cent believe they need to resume operations within 24 hours.