

Nighthawk Publishing

Publishing electronically

<http://nighthawk.firetrench.com>

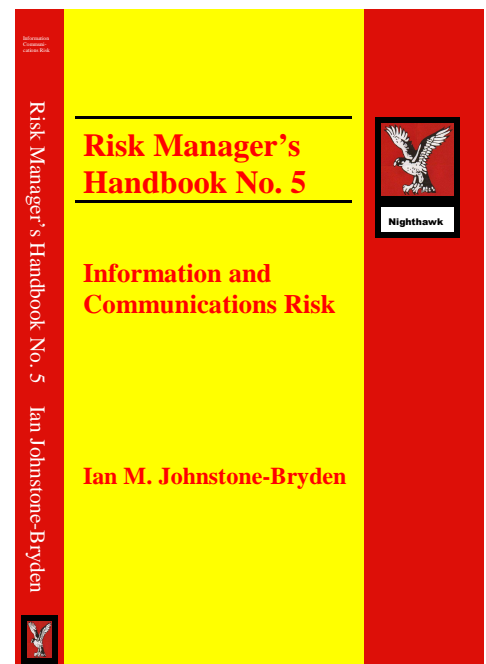


Risk Managers Handbook Number 5 -

Information and Communications
Risk

by Ian Johnstone-Bryden

eBook ISBN 1-84280-100-7
CD eBook ISBN 1-84280-101-5
On-demand ISBN 1-84280-102-3
Pages: 294
Photographs: 108
Drawings: 43
Charts: 46



Launched on June 2005

Risk Manager's Handbook Number 5

— *Information and Communications Risk* is one title in a series of handbooks that cover the many topics that make up the profession of Risk Management.

The very rapid growth in the development of electronic communications and information systems over a period of some one hundred and fifty years has brought a great many benefits. As each decade has passed, the pace of development has accelerated. By the start of the Twenty First Century, the development cycle for key components had shrunk to less than eighteen months. The result has been that users and developers have turned a blind eye to the significant risks that have been introduced along with the many major benefits.

Handbook Number 5 addresses information and communications risks but covers all types of information and communications techniques and technology that may be in use around the world, rather than covering only computer-based systems. This has been done because risk management is based on functional analysis and the analysis of those risks that apply to the functional model of the enterprise, whatever its size. Although many people might use palm computers, the humble pencil and paper is still in widespread use and is more efficient in meeting some functional requirements.

Finding a point to start from in such a large subject is always a challenge. To form a logical

framework, the division of the subject into ten elements for the BS 7799 Standard has been adopted and a further section added to address the issues of interfacing policies across an enterprise and interfacing with other essential elements outside the enterprise. BS 7799 began as a British Code of Conduct for information security, prompted by growing commercial fear of information risk. It evolved into the British Standard BS 7799 and then went on to prompt the International Standard ISO 17799. For many large enterprises, these Standards will be readily adopted to provide a narrow approach to computer-based risk. The Handbook sets out where this leaves unmitigated risks and addresses the issues of reducing risk to acceptable levels within the enterprise. It is a balanced approach based on the author's experience over some thirty years

Chapter One Risk Policy defines risk and security, providing examples of how the use of terms affects the process of controlling risk. Terms in common use are explained and related to each other within the framework of risk analysis and risk policy generation.

Chapter Two Risk Organization examines the structural requirements and methodologies necessary for successful risk management.

Chapter Three Asset Classification and Control examines the way in which assets may be successfully classified and controlled. Examples are provided both for the methods of classifying assets and controlling access to them.

Chapter Four Physical and Environmental Risk examines the impact that physical and environmental risk has on information and communications risk management.

Chapter Five Personnel Risks examines the part that people and legislation play in the expansion and reduction of risk. It shows how people contribute to the generation of risk, why their needs and behaviour must be considered, and how this may be achieved.

Chapter Six Network Management examines the role of networking in the generation of new risks. Examples are given of popular networking environments and the ways in which they combine with all communications and information elements.

Chapter Seven Access Control looks at the risk which apply to access control and the options for reducing these risks. In examining access control, the relationships between widely different approaches are reviewed and their cost relationships compared.

Chapter Eight Development and Maintenance considers the influence of development and maintenance on the management of risk. Development is reviewed in all of its forms and not just in terms of software development.

Chapter Nine Business Continuity Planning looks and the potential conflicts between the management of typical general information and communications threats and the actions necessary to ensure the continuity of business during and in the aftermath of incidents, including major incidents.

Chapter Ten Compliance reviews the essential work of measuring compliance of processes, tools and procedures to achieve implementation and enforcement of risk policies. This review addresses both mandatory and optional management against a published Standard or Criteria, and informal specifications established by the enterprise to meet its specific needs.

Chapter Eleven Interfaces examines the ways in which risk analysis and policy production can be broken into manageable chunks without leaving dangerous gaps. Risk management is frequently undertaken only because of a specific incident or an increased awareness of a particular risk. Even when an enterprise intends to achieve holistic risk management, the work must start somewhere and cannot be completed simultaneously for all risks. Interfaces provide the means to work on risk modules and progressively link them together in holistic management of risks.

Author's Note

The Author's Note is often the least read part of any book. In this case I would recommend that the reader takes time to glance through my note because it provides qualification of the way in which this handbook has been produced. Understanding the qualifications will make it much easier for the reader to relate the examples and advice to his or her practical requirements.

The Risk Manager's Handbook Number 5 - Information Systems & Communications provides a complete view, across an enterprise, of the techniques and technologies for the management of information and communications risks. This book is the complete handbook, each chapter having also been published as a part work.

There have been several challenges in producing this work. Deciding where to start was the first challenge. Handbook Number 5 specifically addresses risks relating to information and communication systems. One approach would have been to rigorously confine the handbook to electronic information systems and communications.

The decision was made to use BS 7799 as a broad framework and to consider all information systems and communications systems. Inevitably, this means that this handbook has to consider risks that are not exclusively related to information and communications systems, such as physical security and environmental considerations. This inevitably means that these relational risks are not reviewed in their full detail, but only as they apply to information systems and communications. However, it is most important for any risk manager to understand that there are always many different ways of reducing risk and every risk may be reduced from acknowledgement, with no further steps to reduce that risk, to total reduction or avoidance. Every enterprise has so many unique considerations, the majority of risks will be reduced in different ways and to different levels by any two enterprises that outwardly look very similar to each other.

It is not unusual, as a consultant, to visit a client and review risk potential and existing risk reduction methods, only to find that significant sums of money have been spent in an attempt to reduce risks, but where some risks did not merit reduction, and other risks required a very much stronger approach. Most commonly, this turns out to be due to someone buying a fashionable and much promoted product, as a complete solution, without stopping to think what the problem was that required a solution. Often, some information risks are much better addressed by not allowing the information anywhere near a computer, or an effective solution may be achieved at much lower cost by fitting some new locks, or ensuring that personnel use existing locks.

As the Risk Manager's Handbook Series develops, there will be other handbooks that deal in much greater depth with some of those risks that apply to information and communications, but also apply to other parts of enterprise operation. This is the only way to produce handbooks that cover subjects in adequate detail, without becoming too heavy to lift in hard-copy format. I am looking forward to writing some of these and to reading others written by colleagues. Risk management is such an enormous subject that we all continue to learn and to develop methods that best suit our individual situations.

Handbook Number 5 assumes that the risk manager, addressing information and communications risk, will be as much an information practitioner as a risk professional. This is a

consequence of the way in which awareness of information risk has risen through fears of attack from the Internet into corporate computer systems. The IT staff seemed like the logical people to saddle with the risk management task and the common assumption has been that they need no training for this new duty. That so many have done so well is frequently more a testament to their personal qualities than to the support they received from superiors, colleagues, vendors and regulators.

One set of information risks that are not comprehensively dealt with in this handbook are those created by propaganda. The reason for this is that the solutions are essentially political. The enormous growth of information through the new electronic techniques of the last fifty years has provided mass manipulators with new opportunities to trick large numbers of people. The growth, particularly in North America and in the United Kingdom, of single interest lobby groups and *spin doctors* has led to democratic processes, which have evolved over hundreds of years, being replaced by lobby management and propaganda.

Every organisation and every individual is adversely affected by this dangerous process which may in due course be regarded as just another form of corruption to be driven from society. That process will either come from political evolution, or by revolution, but it will be beyond the direct scope of any risk manager. It does however directly impact all organisations and individuals. Whether or not change will come peacefully by democratic political means, or violently through revolution, will depend largely on the way in which administrations seek to force acceptance on a population. If frustration and rage are allowed to build there will be civil disorder. Therefore, a risk manager has to live with the situation as it now is and prepare for the possibility of violent change.

One of the most interesting and chilling aspects of the development of mass manipulation is that the manipulators begin to fool themselves and become isolated from reality. The speed with which they can begin to control the masses and the speed with which they fool themselves is increasing through the generations, and the ability to deceive themselves brings about their ultimate destruction.

A handbook of risk can only address the aspects of these politically-based risks as they directly affect the enterprise, and review the way in which their effects can be mitigated, or understood, in terms of information risk management. BS7799/ISO17799 were of course based on a belief that commerce needed a solution to the growing risks that were consequential to new business communications systems that also offered considerable benefits. In many respects, BS7799 was a Standard too far. In attempting to produce a replicable Standard, BS7799 ignores some of the basic rules of risk management, particularly the rule that risk management is infinitely variable. As a risk manager developing skills over thirty years ago, I did not have much help in the form of established frameworks and Standards. At that time, risk avoidance was king under the name of *security*. Risk management was something vaguely disreputable practised by insurance companies and book makers, and just starting to be employed by the more dubious attorneys. As a result, I began with a huge enthusiasm for Standards. Experience over the years has tempered my enthusiasm. This is not because I no longer believe that Standards are good. Far from it, in an increasingly complex world of fast moving technologies, I believe that the ability to explain what something does and how it interfaces with other things is vital.

Standards grew with the Industrial Revolution. A craftsman produces each item in isolation and every product of his skills is slightly different from those before and those yet to be made. Industrialization only works if it can produce vast numbers of identical products, and to produce those products to the closest tolerances because over-engineering costs money. That makes it essential to have a system of specification that allows a product to be measured accurately and in detail. Over the last three hundred years we have produced more and more Standards. However, there are several ways of producing a Standard and several

ways of using it. An engineer making a steam boiler needs to know exactly what stress a nut and bolt combination will endure before failing, but he does not necessarily need to know how the nut and bolt were produced, or what type of alloy has been used in their production. He may however need to know if the metal is resistant to rust and what that resistance is, or what type of coating has to be employed to reduce the rate of oxidation. He would also like to know the anticipated life of the nut and bolt so that he can produce a preventive maintenance manual for his steam boiler.

In this simple example, the engineer could be satisfied by a statement from a supplier that the nut and bolt had been tested to withstand a given pressure for a number of hours before failing, and that the material used in their manufacture is an alloy that conforms to a particular published standard which may state corrosion resistance. If he does not have this information he must guess, and that inevitably means using much thicker stronger components to provide a large safety margin. Even then, some of his boilers will explode and that may result in even thicker, heavier, more costly materials to reduce risk.

The difficulty in producing meaningful Standards for information and communications systems is that although Standards can be specified for particular components, there are an almost infinite number of permutations in which components are assembled and employed to serve any individual enterprise. This has bedevilled computer security from the first computers. Over the years it has become more difficult because the functionality and versatility of computer-based products has dramatically increased.

For me, this has modified my enthusiasm for Standards but it has not stopped me using those existing Standards when I felt that they offered specific benefit. Unfortunately, this selective approach to the employment of Standards runs against the principles behind standardization and measurement. I am no longer convinced that the information and communications industries will ever be able to use Standards as effectively and painlessly as older engineering disciplines unless the whole approach to product development changes significantly. I doubt that this level of change will prove possible because the economics of the electronics industries demand short life products, rapid development cycles for hardware, and even shorter cycles for software which never manages to remove all known errors.

There will be exceptions but these will generally be beyond the reach of most enterprises, either because the technology is restricted to special government departments, or too costly, or take too long to implement. Where it is within reach, it may provide the basis for effective information risk management at high levels of effectiveness. Generally, this type of product will have been developed from a specification in a formal method, have been independently evaluated to the functional specification, and been certified as complying with both the mathematical model and a published information security criteria. Each component will have achieved this level of measurement and certification, and each system built from these components will be specified, evaluated, and certified in the same way.

Where this form of high assurance is practical, there will be a need for accreditation of the system, its operators, and its users. That accreditation is broadly similar in concept to BS7799, but is practical because of the level of assurance available for every part of the complete system and its human interfaces.

The reader may therefore feel that I think BS7799 to be a worthless specification. I do not, but I am very sceptical of the way in which the Standard is misused. In its favour, it is a published Standard and it is widely recognized, particularly in its ISO 17799 incarnation. It also provides a framework and starting points. Against it, enterprises could accredit to the Standard but not interface with similarly accredited enterprises. This creates the very real risk that two enterprises working together might fail to understand the points at which they dangerously interface, introducing major levels of information risk and multiple consequential risks.

There is one further disadvantage with many Standards, such as BS7799, that have wide scope. They are essentially bureaucratic. As such they are potentially most effective in a bureaucratic organization, such as a major corporation, or a government department. They are potentially least effective when used by smaller entrepreneurial organizations. This has the unfortunate effect of placing smaller enterprises at a severe trading disadvantage where they need to trade with large bureaucratic enterprises. It can also close several markets to them, unless they adopt a Standard that is not only ineffective, but actually imposes undesirable operational overheads.

This brings us to the growing threat of over legislation. All politicians down the ages seem to suffer an uncontrolled urge to legislate, whether legislation is required or not. When this urge is combined with modern mass manipulation and Orwellian domination by a ruling elite, is a very dangerous mixture. Legislative groups are increasingly unable to digest all of the legislation placed before them. They find the wealth of technical detail and complexity too great and rely ever more heavily on deceitful Management

Summaries. This results in masses of defective legislation which requires armies of administrators to review and interpret. Large bureaucratic enterprises find difficulty and greatly increased cost, but smaller enterprises can be crippled by the weight of legislation. Most areas of most enterprises suffer, but none more so than the risk management team.

Ian Johnstone-Bryden

Extract from Table of Contents

Author's note	51
Acknowledgements	55
Introduction	57
1. Risk Policy	61
1.0 Policy Scope	61
1.1.0 Bureaucratic flaws	62
1.1.1 Management flaws	62
1.1.2 Definition of terms	62
1.1.3 Beyond BS 7799	63
1.2.0 Achievement by objective	64
1.2.1 Lack of objective	64
1.2.2 Developing objectives	64
1.2.3 Focus on objectives	64

	1.2.4	The planning culture	65
	1.2.5	The <i>firefighting</i> approach	65
	1.2.6	Defining the objective policy	66
	1.2.7	Adequate qualification of objectives	66
	1.2.8	Evolutionary factors	66
	1.2.9	Market forces	66
	1.2.10	The profit objective	67
	1.2.11	The true objective	68
1.3.0		The overhead factor	68
	1.3.1	The period of forecasting	69
	1.3.2	Effects of actions	69
	1.3.3	Funding sources	70
	1.3.4	Funding options	70
	1.3.5	Management control	70
	1.3.6	Informed funding	71
	1.3.7	Statistical error	71
1.4.0		Fundamental risk	72
	1.4.1	Risk of downsizing	72
	1.4.2	Increasing risk	73
	1.4.3	Necessary reaction	73
	1.4.4	Percentage efficiency	74
	1.4.5	Market forces	74
	1.4.6	Corporate Governance	74
	1.5.0	The temporary policy	75
1.6.0		The starting point	75
	1.6.1	Departmental factors	75
	1.6.2.	Departmental example	75
	1.6.2.a	Accepted standards	76
	1.6.2.b	Reduced productivity	77
	1.6.2.c	Perceived restrictions	77
	1.6.2.d	Understanding issues	77
	1.6.2.e	Hidden Risks	77
1.7.0		Life of counter measures	78
	1.7.1	Differentiating life cycles	78
	1.7.2	Depreciation factors	78
	1.7.3	Common excuses	78
1.8.0		Direction of effort	79
	1.8.1	Achievable objectives	79
	1.8.2	Testing and enforcement	79
	1.8.3	Dynamic forces	79
	1.8.4	Accountability	79
1.9.0		Positive culture	80

1.10.0	Software Risks	80
	1.10.1 Retaining risk	80
	1.10.2 Risk carriers	80
1.11.0	Starting Risk Analysis	80
	1.11.1 Analysis stages	80
	1.11.2 Threat sources	81
1.12.0	Gathering information	81
	1.12.1 Initial lists	81
	1.12.1a High probability	81
	1.12.1b Very low probability	82
	1.12.1c Zero probability	82
	1.12.2 Analysis limitations	83
	1.12.3 Risk identification	83
1.13.0	Methodologies	83
	1.13.1 Top level methodologies	83
	1.13.2 Human interaction	83
	1.13.3 Supporting methodologies	83
	1.13.4 Secure Enterprise Environment	84
	1.13.5 Time management	84
	1.13.6 Information security	84
	1.13.7 Statistical analysis	84
	1.13.7a Qualified statistics	84
	1.13.7b Variables	84
	1.13.7c Destructive testing	84
	1.13.7d Shared culpability	85
	1.13.7e Statistical variations	85
	1.13.8 Fault tree analysis	85
1.14.0	Collecting data	87
	1.14.1 Form design	87
	1.14.2 Interviews	87
	1.14.3 Trust and confidence	87
	1.14.4 Data reliability	87
	1.14.5 Culture conflicts	88
	1.14.6 Conflict resolution	88
	1.14.7 Progress reviews	88
1.15.0	Analysing collected data	89
	1.15.1 Simple local studies	89
	1.15.2 Typical events chains	89
	1.15.3 Alternative approaches	89
	1.15.4 Common assumptions	90
	1.15.5 Compromises	90
	1.15.6 Available statistics	90
1.16.0	Conclusions	91

Illustrations

<i>Figure 1</i>	<i>Top Down View</i>	<i>63</i>
<i>Figure 2</i>	<i>Policy Documents</i>	<i>67</i>
<i>Figure 3</i>	<i>Enterprise Cycles</i>	<i>68</i>
<i>Figure 4</i>	<i>C.I.A.</i>	<i>69</i>
<i>Figure 5</i>	<i>Data Removal</i>	<i>71</i>
<i>Figure 6</i>	<i>Document Jackets</i>	<i>72</i>
<i>Figure 7</i>	<i>Integrated Systems</i>	<i>76</i>
<i>Figure 8</i>	<i>Fault Trees</i>	<i>82</i>
<i>Figure 9</i>	<i>Company Failure</i>	<i>86</i>
<i>Figure 10</i>	<i>Strategic Programmes</i>	<i>91</i>

2.	Risk Organization	93
2.0	Preparation	93
2.1.0	The information revolution	93
2.1.1	Enterprise factors	94
2.1.2	Job creation	95
2.1.3	Accountability and authority	95
2.1.4	Progressive approach	95
2.1.5	Scope and relationships	95
2.1.6	Basis for expansion	97
2.2.0	The task of risk management	97
2.2.1.	Origin of workgroups	97
2.2.2	The corporate structure	97

Extracts from text

1. Risk Policy

ORGANISATION has developed an enterprise-wide risk policy to ensure that corporate objectives are achieved at acceptable risk. In developing a comprehensive risk policy, ORGANISATION is taking positive steps to reduce risk to acceptable levels in the interests of staff, stock holders, customers, and all those with whom we transact business.

In addressing risks, it is easy to think of security, which is a process of denial, but ORGANISATION has chosen to adopt a true risk policy to empower personnel in the safe achievement of objectives. This document explains the approach to risk management, and why reliable risk management is a team activity depending on the support and contribution of every employee.

As risks are ever changing, the ORGANISATION Risk Policy has been designed to respond to changing requirements. A series of documents will be produced, covering specific elements of the risk management processes, procedures and equipment. These documents will change when new requirements and risks demand it. Each employee will receive appropriate documentation and training. As far as is practical, the means of risk reduction will be invisible and automated, assisting every employee to carry out assigned duties safely.

1.2.6 Defining the objective policy.

The real difficulty is in deciding what a policy actually is. It seems so obvious that there appears little point in asking the question. Unfortunately, some of the greatest risks in any enterprise stem from the thoughtless use of words. Many different types of document are referred to as policy documents. They can be anything from a short mission statement, to a shelf full of bound volumes. They can even be verbal directives and common acceptance or activities.

Each chapter of Handbook Number 5 starts with a policy statement related to the topics covered. This could be used as a high level policy statement, only requiring modification to adapt to a particular enterprise culture. At that level, the policy is technology-free. The point at which specific technology and procedural references should appear is several levels lower down. That means that the high level policy statement may remain unchanged for many years, although detailed policies further down the stack may have very short working lives.

A common situation is for policy documents to fulfil a political rather than a practical role. A disadvantage of starting

risk management with information and communications is that there may be inadequate definition of objectives available to the risk analysts and a reluctance on the part of Senior Management to agree any review of objectives which they see as *mission creep* beyond the scope of the risk analysis.

1.2.7 Adequate qualification of objectives.

On foundation of an enterprise there is usually a commonly accepted objective. A health care authority is established to provide health care. A corporation manufacturing animal feed clearly has the objective of manufacturing and selling feed products for animals.

The information risk policy must be based on a clear set of objectives that reflect the corporate operational objectives and relate information security to the achievement of those objectives.

1.2.8 Evolutionary factors.

It will usually be neither practical nor desirable to attempt any *future proofing*. A risk policy must deal with today's threats, but be capable of amendment to address changing threats. The basic responsibility for managing this change is the part of the policy that relates to enforcement, which

3.0 Nature of assets.

The Classification and Control of Assets is an essential part of all operations, or should be. Most enterprises have a remarkably casual attitude to this important subject. Some assets will be recorded and controlled in detail, but others will be taken for granted. Information itself is an asset, and yet most organisations would be hard pressed to list all information available to them, much less classify and control that information.

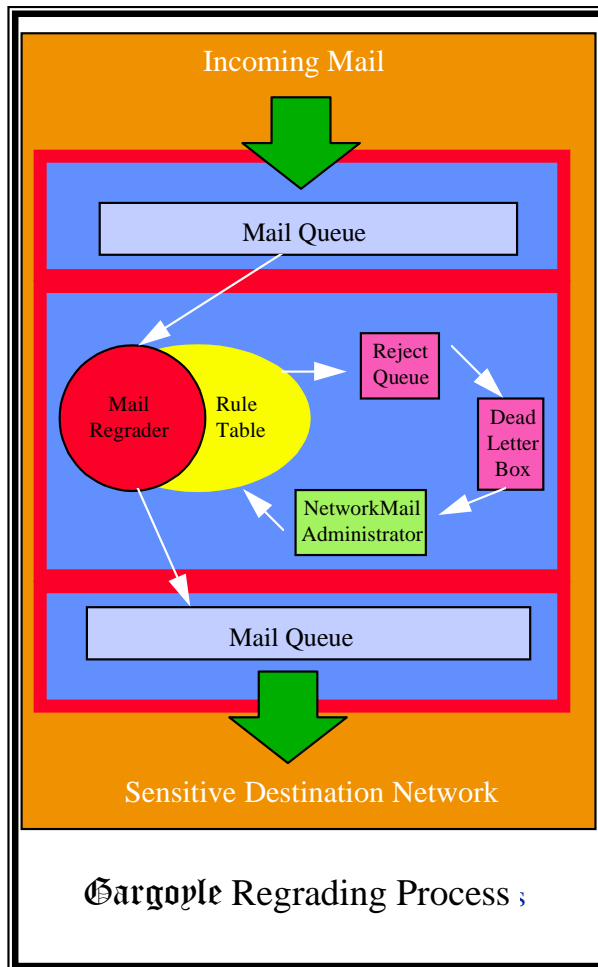
3.1.0 Methods of classification.

There are several ways of classifying any asset. The most common method is to record the acquisition of an asset and classify it either by its purpose, or by who con-

trols it. Therefore, personal computers may be recorded as being the responsibility of the Information Systems Department, or under the user department. In some cases they may be recorded under a specific end-user. That usually depends on how budgets are allocated and assets procured.

Essentially it is a finance driven process because the recording of the asset is intended to enable financial auditors to check that adequate financial control is being exercised by the enterprise. This is not adequate for risk management purposes and tends to exclude any asset that is acquired without the exchange of money.

It is not uncommon in some enterprises to engage in fraud because of the slack approach followed by their auditors.



The Gargoyle Trusted Gateway provides the means to operate multi-level security. This is a basic feature of Trusted Operating Systems above B1 level Certification and inherent to the concept of the Compartmented Mode Workstation that was developed originally for the US Defence Intelligence Agency to enable intelligence analysts to access data at several levels of classification. This specialist intelligence requirement also maps to commercial enterprises where the ability to grade information speeds access to all levels of sensitivity without compromising a risk management policy. It also potentially reduces cost by avoiding or reducing the protection of low sensitivity data and data that is already in the public domain. In addition, there are a number of other benefits that derive from the fact that employees only access data that is applicable to their job function, providing them with fast access to information they need and preserving the integrity of data. More surprisingly, this type of Trusted system reduces hardware and operating costs because one machine replaces several common firewalls.

Trusted Gateways Figure 81

How to order

Risk Managers Handbook Number 5 - *Information & Communications Risk*

You can order **RMHB5—Information & Communications Risks** an electronic file to be delivered to you by email. There is no charge for email delivery. Just select the complete edition and pay by PayPal for the Right To Read license.

Or you can order **RMHB5—Information & Communications Risks** to be delivered by post on a CD as a complete edition. The pricing includes license, CD media, and DVD box with colour printed cover insert. Post and Packing options are displayed.

Or, if you wish to order **RMHB5—Information & Communications Risks** as one title in your own selection of titles from the Nighthawk Publishing On-line Catalogue, you can save money by using the Custom CD Option

Or you can order **RMHB5—Information & Communications Risks** on paper as an on-demand printing. The on-demand print option provides full colour on white paper in a ring leaf binder with full colour cover inserts.