

Nighthawk Publishing

Publishing electronically

<http://nighthawk.firetrench.com>

How To Manage Risk

- Working Successfully with Risk

by Ian Johnstone-Bryden

| | |
|--------------|--------------------|
| eBook | ISBN 1-84280-004-3 |
| CD eBook | ISBN 1-84280-013-2 |
| On-demand | ISBN 1-84280-091-4 |
| Pages: | 294 |
| Photographs: | 103 |
| Drawings: | 19 |
| Charts: | 16 |

Launched on May 2005



How to Manage Risk examines the subjects of risk analysis, risk reduction, and risk management as a comprehensive subject across an enterprise. The principles apply equally to all sizes and types of enterprise. Most organizations still deal with aspects of risk piecemeal, with very few enterprises charging one individual with the ultimate responsibility for managing risk across the enterprise, resulting in unmoderated risk and/or unnecessary and costly duplication of effort.

The author wrote the first book to describe holistic risk management, "Managing Risk", published by Avebury in 1995. This work has been much quoted in subsequent work by other authors, used as a text book in University courses and as a corporate library volume. **How To Manage Risk** is an updated and expanded review and explanation of holistic risk management, based on the original pioneering book.

Risk management is an enabling process that provides access to information, assets and processes to ensure that objectives can be achieved at an acceptable risk. This contrasts with Risk avoidance or security which is a process of denial and constraint, frequently preventing necessary access yet failing to adequately counter all potential risks, usually creating a false sense of security. Effective risk management provides the most economic method of achieving objectives without facing unacceptable risk.

How to Manage Risk examines the subjects of risk analysis, risk reduction, and risk management as a comprehensive subject across an enterprise. The principles apply equally to all sizes and types of enterprise. Most organizations still deal with aspects of risk piecemeal, with very few enterprises charging one individual with the ultimate responsibility for managing risk across the enterprise, resulting in unmoderated risk and/or unnecessary and costly duplication of effort.

Human nature is optimistic. We prefer to think that risk only affects other people. It can be difficult to decide the probability and impact of any particular risk, encouraging the strong temptation not to invest precious funds in countermeasures that we hope will never be needed. When we do take risk seriously, it is often just after we have suffered from fire, theft, or accident, and by then it may be too late to act.

Historically, enterprises have attempted to address areas of risk in isolation. Today, even the smallest enterprises automate processes, making it impossible to reliably divide operations. Quality management relates to health and safety issues, fire protection can conflict with crime protection, every activity involves personnel, and we increasingly rely on complex computer networks. Effective risk management must span all of these areas.

How to Manage Risk shows how risks can be identified and reduced economically and effectively, before serious damage occurs.

How to Manage Risk is available in several forms. The complete book is available electronically by email, secure ftp, ISDN, and, on CD, delivered by post. It is also available in printed paper form and has been published as set of Part Work volumes, each volume being a chapter in the complete works.

How to Manage Risk is presented in the context handbook form. In place of a traditional index, there is a detailed table of contents where each sub-heading addresses an area of risk and each chapter addresses one of the primary compartments of risk management in an enterprise. For those readers working on a computer, the PDF format used for the electronic versions of this book includes the ability to search in a way that suits the reader — a considerable advance on using a printed index.

Chapter One 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.

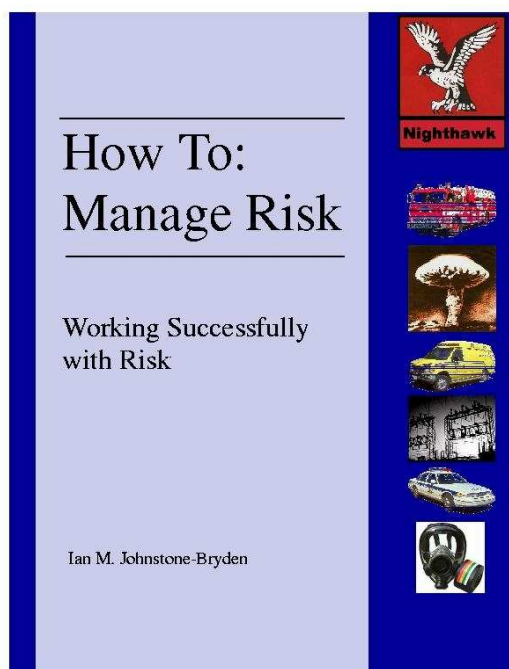
Chapter Two examines the use of enterprise and risk policies in successful risk management. Methodologies are examined, establishing the need for dynamic policies to test threats and solutions.

Chapter Three examines the process of risk analysis, necessary to the production of enterprise and risk policies. The methods of evaluating risks are discussed and compared with common enterprise practice.

Chapter Five examines risks that affect enterprise sites and describes methods of reducing and managing risk within the area of a site.

Chapter Four 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 Five examines the risks that affect an enterprise site up to but not including any buildings that may occupy the site. In some enterprises site boundary controls may be adequate and building security may not be a requirement.



Chapter Six continues the examination of a site, considering the special and different requirements of buildings within a site. Risk reduction methods are described, in relation to area site protection.

Chapter Seven reviews the challenges presented by facilities shared with other enterprises and with the general public. Examples are provided of the different technology and approaches and the need to balance protection with the operational requirements of enterprises.

Chapter Eight follows the examination of risk management at fixed installations, by reviewing the different needs of mobile facilities. It examines the reasons for mobility and the new technologies which are changing the patterns of mobility and resultant risks.

Chapter Nine examines the way in which the use of information is introducing social and economic change with major changes to risks. It identifies why information systems are making enterprise wide risk management not only desirable, but essential, through their bridging of traditional divisions in the work place.

Chapter Ten examines the ways in which information risks may be successfully managed. The dramatic growth of computer-based systems and international networks is examined in its relationship with risk development. The national and international security criteria are examined against the background of the commercial development of computer and communications equipment.

Chapter Eleven discusses some of the changes that have already been introduced by the Information Revolution, some which are about to be introduced, and how these will affect risk management. In particular, the social and economic possibilities are explored. It concludes that there will be revolutionary change, that a number of possible courses are open, and that this change will have a strong impact on the way in which risk develops and may be managed.

Author's Note

When I began writing *Managing Risk* in 1992, the world was very different from the world ten years later, and yet so much has not changed at all. Many of the risks that face us today have faced the human race for millennia. Many of the risks we see as modern risks are really only minor variations on very old risks. Perception of risk changes greatly from one period to another. Most of the trends established in 1992 have continued to develop in a reasonably predictable manner.

A key perspective is *information*. The development of electronic information systems has introduced great benefit and additional risk. One area of expanded risk is created because modern systems collect together information elements of the enterprise that are not individually sensitive but can be very sensitive when they come together in one medium. Another area of risk is that the very rapid growth of information systems has created a new group of practitioners who do not always integrate well with other long established elements of enterprises, particularly in managing risks.

Perhaps the greatest challenge of electronic information systems is that they now open windows into every part of most corporations, side stepping risk control systems that have previously been effective in keeping unauthorised people out of the enterprise. Today, there is a growing pre-occupation with *information security* but, sadly, much of this effort is not producing safer information systems, rather it is producing yet more bureaucracy without adequately addressing risk. The pathetic efforts of some facile governments is contributing a raft of legislation that does nothing to reduce risk but much to increase it, particularly in terms of civil liberty. A classic example is the extraordinary British legislation that requires Internet Service Providers to record their clients' mail and keep it on file for seven years, to be handed over to the British Government, or its agents, on demand. If a government passed legislation to require postal services to open all mail passing through their sorting offices, copy the contents, keep those copies for seven years, and hand over any copy whenever requested, there would be, rightly, a massive public outcry.

It continues as a paradox that the engine of the British Victorian Industrial Revolution, the limited liability corporation, continues to be the model that most enterprises are based on, even though the commercial, industrial and governmental realities in 2001 are very different from those of 1801 when the model started to form, becoming commonplace by the 1860s.

The last decade has been most interesting in that several of the technology concepts that I included in the original book were not available as commercial products and several were no more than theoretical concepts. Ten years on, much of this technology has been developed into standard products. In particular, video recording of CCTV cameras is routinely done using digital storage in computer servers, wireless connection is practical for many risk management systems, and the computer is routinely employed to link many different detection and communications devices together in an integrated and intelligent control system.

Against this rapid development of technology options, the computer base continues to be very unsuitable for effective risk management unless large risks are accepted. When computers were first used, they were employed in situations where physical security could be easily applied. When they increased in popularity it was mainly in accounting, scientific and engineering applications where computer downtime was not an issue because the computer was so much faster than manual processes, even allowing for breakdowns. As the computer has become ubiquitous, the pressure has been to reduce its cost and increase its functionality to assist marketing personnel to create new and bigger markets. Unfortunately, that has meant that many early errors are still tolerated and many new errors have been introduced, reducing the risk management potential of the systems.

Another disappointment through the last decade is that risk is frequently introduced by communication and the limits of natural language. This results from inconsistent use of words and terms, misunderstanding of words used, and offence caused by use of particular words and terms. The wider the audience, the greater the potential for risk.

In 1992 that was understandable because risk management was a new concept outside the insurance markets. During the last ten years, it has become increasingly popular to talk about risk management but, far too often, when people talk about *risk management* they have just replaced the word *security* and not the meaning.

The amazing speed with which electronic communications functionality has developed during the last decade has introduced another set of risks. The volume of information is swamping enterprises and leading to emails not being read properly, or at all, and a mass of misunderstood and inaccurate information. Information integrity is now a growing issue. An author therefore has to attempt to write with integrity and clarity. I hope I have achieved that in this book.

In writing a book, which covers the full range of risk management, a number of niches are covered, such as crime prevention, health and safety, and quality control. Each niche has generated its own jargon and one of the worst areas is in Information Technology. To further complicate matters, a term used freely in one niche area may also be used with equal freedom in another niche, but to mean something very different. As far as possible, jargon terms have been avoided throughout this text. Where it has been necessary to use a particular specialised word, its meaning has been described at least at the first point of use.

One particular area of risk today is the use of words that imply gender. The structure of the English language gives a writer limited choice in this matter, and maximum potential to offend some readers. The writer either has to select one gender, or to produce a confusing and unnecessarily long document where every point contains an explanation of equality. This book uses the male pronoun in the interests of economy, and has standardised on the male gender throughout the text, only in the interests of continuity. The writer has not intended to favour one gender above the other, and asks the reader to treat all uses of gender as full equality without preference.

Jan Johnstone-Bryden

Example of the Table of Contents

Chapter 1 Definition of risk and security

| | |
|---|----|
| 1.0 Security — by definition | 57 |
| 1.1 Security — the consequences | 57 |
| 1.2 Security — the relative effectiveness | 58 |
| 1.3 Security — operational effectiveness | 58 |
| 1.4 Ownership — origin of risks | 58 |
| 1.5 Reasons for failure | 58 |
| 1.6 True Cost | 59 |
| 1.7 Competitive advantage | 60 |
| 1.8 Excuses, not Reasons | 60 |
| 1.9 Risk Analysis | 60 |

| | |
|-----------------------------------|----|
| 1.10 Security Criteria | 60 |
| 1.11 Assurance | 61 |
| 1.12 Integrity | 61 |
| 1.13 Availability | 61 |
| 1.14 Security — which works | 61 |
| 1.15 Risk Management | 62 |
| 1.16 Risk Avoidance | 62 |
| 1.17 Authorized Users | 62 |
| 1.18 Data Subjects | 62 |
| 1.19 Need-to-know | 63 |
| 1.20 All Risks | 63 |
| 1.21 Access Privilege | 63 |
| 1.22 Risk Reduction | 64 |
| 1.23 Acceptable Reduction of Risk | 64 |
| 1.24 Risk Policies | 64 |
| 1.25 Enterprise Policies | 64 |
| 1.26 Achievement by Objective | 64 |
| 1.27 Tasking | 65 |
| 1.28 Processes | 65 |
| 1.29 Tools | 65 |
| 1.30 Resources | 65 |
| 1.31 Scope | 65 |
| 1.32 Overheads | 66 |
| 1.33 Probability | 66 |
| 1.34 Impact | 66 |
| 1.35 Risk Analysis | 66 |
| 1.36 Natural Language | 66 |
| 1.37 Structured Methods | 66 |
| 1.38 Expert Systems | 66 |
| 1.39 Artificial Intelligence | 66 |
| 1.40 Formal Methods | 67 |
| 1.41 Methodology | 67 |
| 1.42 Inadequate analysis | 67 |
| 1.43 Enforcement | 67 |
| 1.44 Authority | 68 |
| 1.45 Conclusions | 68 |

Illustrations

| | | |
|-----------------|---------------------------|-----------|
| <i>Figure 1</i> | <i>Armour</i> | <i>57</i> |
| <i>Figure 2</i> | <i>Identification</i> | <i>58</i> |
| <i>Figure 3</i> | <i>Training</i> | <i>59</i> |
| <i>Figure 4</i> | <i>ITSEM</i> | <i>60</i> |
| <i>Figure 5</i> | <i>Equipment</i> | <i>61</i> |
| <i>Figure 6</i> | <i>Castles</i> | <i>62</i> |
| <i>Figure 7</i> | <i>Medical Facilities</i> | <i>63</i> |

Example Text

3.4 Terrorism

A similar situation may result from urban terrorism. The objectives of the terrorist are to win publicity and frighten the population into acceding to some unreasonable demands, which cannot be achieved through democratic debate and agreement.

To achieve these objectives, the terrorist attacks targets that are least able to defend themselves. There is no complete defence against threats of this type because the small numbers of terrorists have a wide choice of potential targets.

Giving in to the terrorists' demands is also unlikely to remove the threat because, as one demand is conceded, additional demands will be put forward. Experience shows that terrorists become addicted to their life style and the only effective counter is to starve them of publicity and increase the risks to them.

This presents a dilemma for a democratic open government. It is unable to effectively prohibit publicity of terrorist outrages, and the news media has shown itself to be incapable of self-regulation. In fact, the news media appears to need disasters as much as the terrorist is driven to cause them. The public are naturally reluctant to travel to an area where they risk being shot or blown up. The terrorist is therefore winning.

If this situation continues, the risk increases because the terrorist is encouraged to continue and to expand his campaign. He will also win if a government is driven to introducing oppressive measures, because another objective is to destabilize the government by making it unpopular.

A democratic government is left with limited choices. A significant increase in spending on policing measures, to reduce the terrorist threat, will take money from other areas of government spending, or result in increased taxation.

Neither situation is welcome, or desirable, but all governments take some action of this nature. This results from subjective and emotional judgement in response to public concern generated by emotional, and often inaccurate, news reporting. A greater proportion of resources may be devoted in a vain attempt to halt terrorist bombings in cities, than is devoted to reducing death and injury caused by motor accidents and fire. A terrorist bomb exploding in a city, or being found and defused in time, will be a major item on national news. A fatal road accident, or injury in the home, is unlikely to achieve the same level of news coverage. Probably, any coverage will be restricted to a few lines in a low circulation local newspaper. However, the risk to the individual from road and domestic incidents will be considerably greater than those resulting from terrorist actions. The financial impact of any terror attack may be relatively small but the psychological impact will be very high.

3.5 News Media Impact

The impact of the news media on risk analysis is frequently to distort the process. If risk analysis depends on news, and responds only to that, it will be both a superficial and a reactive process. Inevitably, news is only available after the event has begun. If the event does not directly affect the enterprise, it may provide information which should be included in the analysis process. If it does directly affect the enterprise, it may be too late to consider because it may already have inflicted fatal damage.

3.6 Policing

The public also have a part to play in actively defeating threats such as terrorism. No police force is able to dedicate the resources necessary for the prevention of terrorism. The news media have more resources to advertise the terrorist than police agencies command for all policing duties. Therefore, a police force needs all the help it can get. Unfortunately, police forces have some communications difficulties with the public.

The British policeman was internationally famous for his good natured common sense, courtesy and reliability, to the extent that a book by a Jewish refugee from Nazi Germany was titled "And the Policeman Smiled", because the refugee had never before experienced a policeman who was there to cheerfully serve rather than to grimly control. British police should therefore have the best prospect of reliable communication with the public. At the other extreme, some police forces revel in the projected image of storm troopers, and may expect a less enthusiastic relationship with the public.

How to order

How to Manage Risk

Go to the Nighthawk eBookshop at <http://nighthawk.firetrench.com>

You can order *How to Manage Risk* as an electronic file to be delivered to you by email. There is no charge for email delivery. Just select the complete edition or select Parts from the Part Work option and pay by PayPal for the Right To Read licenses.

Or you can order *How to Manage Risk* to be delivered by post on a CD as a complete edition or as one or more parts from the Part Works option. Each of the Parts listed is a chapter from the complete edition, with full Table of Contents and preliminary pages, copied to its own CD. The pricing includes license, CD media, and box with printed cover insert. The CD is supplied in a DVD box case with full colour insert. Post and Packing options are displayed.

Or, if you wish to order several Parts of *How to Manage Risk* to select your own selection of titles from the Nighthawk Publishing On-line eBookshop. You can save money by using the Custom CD Option.

Or you can order *How to Manage Risk* 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 inserts.