

Managing Information Risk

A Director's Guide

Stewart Mitchell

Managing Information Risk

A Director's Guide

Managing Information Risk

A Director's Guide

STEWART MITCHELL



IT Governance Publishing

Documents



Document Sharing Hub

Copyright IT Governance Ltd

Provided by IHS Markit under license with IT Governance Ltd. See=/, User=,

No reproduction or networking permitted without license from IHS.

Full document details: ITG 2009

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EH
United Kingdom

www.itgovernance.co.uk

© Stewart Mitchell 2009

The author has asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2009
by IT Governance Publishing.

ISBN 978-1-84928-019-8



Documents

Document Sharing Hub

PREFACE

Information risk is endemic in any modern organisation. From the potential for losing sensitive information to a full-system crash that incapacitates the company, the consequences can be disastrous.

Yet more than half of all companies have no formal risk management practices in place, meaning they are unable to be sure their systems are secure, reliable or resilient.

This pocket guide addresses the scope of risks involved in a modern IT system, and outlines strategies for working through the process of putting risk management at the heart of your corporate culture.

Given that no two companies are the same, this pocket guide should not be taken as a step-by-step guide, but should provide decision makers with a solid overview of the factors they need to consider and a framework for implementing a regime that suits their needs.

It provides a checklist of steps that companies need to take to safeguard against various threats, highlights potential vulnerabilities and lists methodologies for mitigating against the risks.

This pocket guide draws on previous works by senior security advisory bodies – in particular the US National Institute of Standards and Technology, which has produced numerous landmark ‘Special Publications’ on the subject,

Information Security Council

Preface

and various UK government guidelines drawn up in the wake of high-profile data breaches.

UK governmental and industry white papers were also consulted during research, including interviews with security analysts and board-level risk management practitioners.

Copyright IT Governance Ltd

ABOUT THE AUTHOR

Stewart Mitchell has been an IT journalist for more than 10 years, working across a number of publications including *The Sunday Times* and specialist magazines such as *PC Pro*, *Computer Shopper* and *PC Advisor*. He has run his own internet-based business for the last four years and regularly meets with IT business leaders.

Recent work has focused on the work of security professionals and the challenges they face in an ever-evolving digital world.

Stewart's other best-selling pocket guides for IT Governance include *Managing IT in a Downturn* and *How to Survive a Data Breach*.

Copyright IT Governance Ltd
Provided by IHS Markit under license with IT Governance Ltd
No reproduction or networking permitted without license from IHS

CONTENTS

Introduction	10
Chapter 1: Managing Risk.....	13
Reduce/Mitigate/Control	14
Transferring risk	15
Avoid	16
Accept.....	17
Chapter 2: Information Risk Policy	19
Chapter 3: The Risks.....	21
Accidental disclosure	21
Theft of hardware or data.....	22
Acts of nature.....	22
Alteration of software	22
Redundant media	23
System configuration error	23
Suppliers and partners.....	23
Critical information is wrongly destroyed	24
Poor data input.....	24
Critical information is lost	24
Wasted assets	24
Failure to make information available	25
Chapter 4: Risk Management Framework.....	26
Chapter 5: Risk Assessment.....	30
System characterisation	30
Identify threats	31
Identify vulnerabilities.....	33
Control analysis	34
Likelihood determination.....	34
Impact analysis	35
Risk determination.....	36
Control recommendations.....	36
Documentation.....	37

Chapter 6: Risk Mitigation Strategy 38
 Seven-stage plan 39
Chapter 7: Controls 42
Chapter 8: Interacting with Partners and Suppliers 44
Chapter 9: Standards 47
Appendix 1: Checklist for Directors.....49
Appendix 2: Establishing an Information Risk Tsar 52
Further Reading 53
ITG Resources.....55

INTRODUCTION

Information is critical to every large enterprise, yet its mission-critical importance is all too often overlooked – until something goes wrong.

Information risk management is a method of assessing information threats, which can be anything from a burst pipe flooding your server room to someone leaving a laptop on the train, and taking actions to minimise the chances of risks becoming reality.

The reasons for managing information risk are many. Properly implemented security controls sparked by a risk assessment could save huge financial or reputational fallout.

A 2008 cybercrime report by McAfee suggests that globally businesses lose \$1 trillion a year in lost intellectual property and expenditures for repairing the damage. And cybercrime is just one small link in the information risk chain.

Poor organisational practices also risk information leakage, often by organisations failing to apply or adhere to strict practices on how information is treated.

According to the Privacy Rights Clearinghouse, the number of records containing sensitive personal information that were involved in security breaches in the US in the three years prior to December 2008 was 250 million. And in 2008 in the UK alone, there were 29 million instances where people's personal information was disclosed.

Introduction

While it's important to guard information closely, making information available to the right people is an equally important role in the risk management process because inaccessible or (worse) inaccurate data is useless to the organisation.

While you can protect your organisation's systems internally, many threats are beyond your control. What happens when there is a natural or terrorist incident that affects power supplies or when snow on the line means your IT support team can't reboot the e-mail servers after a glitch? Continuity planning can mitigate against such problems, but before an organisation spends potentially millions on a disaster recovery programme its director must be sure that the risk, and the likelihood of a vulnerability being realised, are worth the expense. Does the clear-up operation cost more or less than the impact of the information risk that comes to fruition?

Of course, risk management can only go so far – at certain points the cost of securing marginal value systems or data outweigh the benefits of preventing risks, but even then risk management can reduce the costs of putting things right after the incident.

Recent Ponemon Institute research found that remedial action after data breaches cost \$189 per capita in companies that had employed information risk management practices, while the 56% of companies that had no risk management had to spend \$224 on each lost file.

Successful information risk management should enable an organisation to accomplish its mission by better securing systems, enabling

Documents

Introduction

management to make well-informed risk management decisions to justify the IT budget expenditure and by assisting management in authorising the IT systems.

CHAPTER 1: MANAGING RISK

The key to managing risk is understanding that whatever the security controls your organisation puts in place some level of risk is inevitable. The following chapters help identify, evaluate and quantify the risks, but at all stages of the risk assessment and control framework, managers need to be considering just what level of risk is acceptable for any given threat. Given the potential costs of an IT systems security breach, assessing ‘risk tolerance’ is a board-level consideration.

After each threat and risk is assessed and the cost-benefits of mitigating a risk have been established, directors need to decide how to treat residual risk. The key question directors need to ask themselves is: ‘Should we mitigate, transfer, avoid or accept these risks?’

This mantra should be used as a motto throughout the risk management process, and some risks might need to be reassessed several times before directors are confident that all that can be achieved has been undertaken.

UK government guidance document *Infosec Standard No 2* stresses the importance of directors being able to show due consideration of how risks are managed.

‘There must be an accountable management process for the formal acceptance of which risks

1: Managing Risk

are to be mitigated, avoided, transferred or accepted,' the document says. 'This process should include the acceptance of all the costs implied by those choices, and justification and formal agreement of any deviation from corporate policy, together with acceptance of any potential business impacts resulting from such deviation.'

Indeed internal controls are central to any risk management project or programme. *Internal Control: Revised Guidance for Directors on the Combined Code* (Oct 2005) (the 'Turnbull Guidance') says that directors should ensure there is an internal control system to 'facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud' (clause 19) and that the internal control system should include 'information and communications processes' (clause 20). This pocket guide helps directors meet this obligation.

Reduce/Mitigate/Control

The first consideration for most risks identified is how to reduce the risk through a series of controls and fail safes. These options are detailed in later chapters, but rely on countering threats through astute application of control mechanisms. Vulnerabilities can be countered through improved security measures, such as better control of physical access to data centres or better network security, for example; or by simply applying security patches to vulnerable systems.

Documents

1: Managing Risk

In an ideal world, directors can ensure enough controls and security measures are put in place to minimise a threat to the point it becomes acceptable, if not entirely palatable. Management may have to go through the risk assessment process several times before reaching the point where risk is acceptable, depending on the nature and seriousness of the risk.

Transferring risk

Transferring the risk involves persuading or paying someone else to take the risk on your behalf. Usually, transfer measures are most relevant to financial risks that can be measured, and take one of two forms – either insurance or contractual obligations with a third party supplier.

In the same way that we pay for car insurance to cover the risk of having to pay thousands in medical and repair costs in the event of a crash, IT system failure risk can be passed on to third parties. Insurance shifts the responsibility to an insurance company, which will provide financial coverage for losses incurred from circumstances such as fire, legal proceedings, vandalism or theft.

Possible insurable risks include:

- Damage to systems equipment.
- Damage to a contractor's property on your premises.
- Equipment replacement.
- Identifiable and measurable business interruption.
- Legal liability for physical injury to employees and contractors.

1: Managing Risk

Insuring against the risks may well be cheaper than trying to fix the problem in-house, but directors should also consider that insurance that is affordable now may become unacceptably expensive if several claims are made.

The UK government's *Infosec Standard No 2* states that: 'Where risk transfer is used as a risk treatment, an organisation should consider planning in preparation for the possibility that the third party may later fail them in some way. After a number of insurance claims, for example, an insurance company may increase premiums to an unacceptable level or refuse to renew a policy'.

In many cases, non-insurable problems can be counteracted by strong contractual obligations that transfer the risk to suppliers of equipment and services.

How this is done depends on the risk. Complete system failure risk can, for example, be transferred by paying a third party company to run a redundant mirror system which comes online the second the internal system fails. Not only is the risk reduced, but strong service level agreements and contractual obligations should mean costs incurred as a result of the failure could be met by the third party company.

Performance bonds and warranties can ensure that any increased costs incurred as a result of failed projects are passed on to the supplier.

Avoid

The most complete method for managing risk is to avoid it altogether. This can be hugely effective

1: Managing Risk

against some risks but unrealistic for others. Take, for instance, the danger of company secrets being hacked into over the Internet. Keeping such confidential files on a non-networked computer in a locked room with a monitored key can pretty much guarantee the safety of the data therein. The risk is avoided, but at a cost of not having the information available. Locking down the e-mail system in the same way is impossible without rendering it completely useless.

Similarly, the risks associated with a software product can be avoided by simply switching to another brand of software, or removing the element of the business that relies on the software altogether.

Accept

Some risks are so unlikely to come to fruition, are impossibly expensive to mitigate, or so benign in terms of damage, that directors simply accept them. Residual risk is seen after all the measures and controls have been considered, and documentation must highlight why and how these risks are considered acceptable.

According to UK government guidance, it is essential that the business fully understands the residual risks, so that it may make an informed decision on the acceptance of the asset. The accreditation process must document residual risks clearly and record their acceptance. Residual risks may also need to be fed into other corporate risk considerations, such as business continuity, disaster recovery, and forensic readiness plans.

1: Managing Risk

Directors should also consider who is responsible for accepting the risk – is it the IT security staff that can authorise the acceptance, or should it be a board-level decision?

Document ID: ITG 2009