CYBER RISKS for Business Professionals

A Management Guide

Rupert Kendrick

Cyber Risks for Business Professionals

A Management Guide

Cyber Risks for Business Professionals

A Management Guide

RUPERT KENDRICK

IT Governance Publishing

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

First published in the United Kingdom in 2010
by IT Governance Publishing.

ISBN 978-1-84928-093-8

FOREWORD

This book is an update of my previous publication on the subject *Managing Cyber Risks*, 2002, which addressed the subject from the perspective of law firms only. Some notable developments have occurred since then and I hope I have included those of greatest importance.

Included in this edition, for instance, are references to relevant provisions of the Companies Act 2006; Provision of Services Regulations 2009; Rome II Regulation No 864/2007; Digital Economy Act 2010; Equality Act 2010; and the Employment Practices Code 2005.

New areas covered include: wireless networks; identity and access management; Cloud Computing and IT outsourcing; corporate, IT and project governance principles; and Web 2.0 and social networking.

This edition is also widened to consider the position of business professionals, such as law firms, accountants, insurance brokers, business analysts and financial institutions, although it may be too general for more specialist sectors, such as information security experts.

PREFACE

The benefits which Internet technologies offer to business professionals also present considerable risks. The management of these risks is the focus of this book.

I have tried to distil the essential risk elements and reconstruct them into a framework that reduces complexity and creates a sense of order for their management. I have divided coverage of the subject into three sections:

- Part 1 introduces Internet risk and discusses various technology, legal and operational risks.
- Part 2 identifies some key principles for good governance, assessing risk, and risk management.
- Part 3 suggests technology, legal and operational solutions to the risks set out in Part 1 through risk management strategies identified in Part 2.

With respect to legal and compliance provisions, I have tried to ensure the law is accurate as at July 2010. Full texts of the legislation mentioned can be accessed at www.opsi.gov.uk/acts.

The book contains a *caveat* frequently issued by lawyers. Coverage of the various topics is, of necessity, generic in nature, as risks and solutions arise and apply respectively in different ways from organisation to organisation.

This book is a general guide to the origins of cyber risks and to developing suitable strategies for their management. It is no substitute for obtaining appropriate, timely and professional advice on specific cyber risk issues and their management which may arise in a specific organisation.

ABOUT THE AUTHOR

Rupert Kendrick, LL.M, was formerly a solicitor and, for many years, a partner in a medium-sized law firm. More recently he has been a director in a risk management consultancy, addressing legal IT and Internet risk issues.

In 1998 he completed a Master's programme in Legal Practice Management, studying the implications of the Internet for law firm marketing strategies, and was a member of the Law Society's Technology and Reference Committee for some years.

For the last 10 years he has pursued a career in legal publishing, as an author, editor and columnist on IT and Internet issues.

ACKNOWLEDGEMENTS

I have received helpful comment, guidance and input from a number of people, to all of whom I express my thanks. Susan Singleton of Singletons Austin Ryder, Solicitors, has shown great patience in helping me ensure that the chapter on legal compliance is comprehensive, accurate and timely.

My thanks are also due to individuals in certain organisations for offering interviews. Their selection was not scientific. I simply wanted a cross-section to show different professionals' approaches to some of the issues.

They are:

- Dennis Farm, Enterprise Information Audit Manager, Morgan Stanley;
- Emily Freeman, Executive Director, Technology Risk, Lockton International;
- Robert Jackson, Security and Infrastructure Consultant, Capgemini;
- Andrew Rose, Global IT Risk Manager, Clifford Chance;
- Richard Spooner, Head of IT Advisory, Baker Tilly.

I am also indebted to three reviewers for their time in providing helpful comments on my draft manuscript.

Finally, thanks to my wife, Sonia, for her patient support throughout this project.

CONTENTS

PART 1 – IDENTIFYING CYBER RISKS

CHAPTER 1: SETTING THE SCENE

Only a few years ago, the Internet was a relatively new phenomenon. E-mail and interactive websites offered the prospect of a radical shift from traditional business models to transactions almost exclusively conducted electronically.

To a great extent, this prospect has arrived. Wherever possible, organisations are seizing the opportunity to: market themselves through websites as opposed to conventional brochures; employ e-mail as a core business communication tool instead of traditional post; and supply goods and services electronically without the need for the physical presence of the consumer. The development and rapid expansion of businesses using the Amazon (*www.amazon.com*) model is testimony to the rapid and all-pervasive development of Internet technologies in the modern marketplace.

The importance of IT

IT of any description is now critical for the survival of almost every organisation. Without IT, few business or professional concerns could hope to survive, let alone prosper, in the modern marketplace.

IT is an essential tool for every organisation. Without IT, their administrative systems would be inadequate; business communications would be wholly impractical; marketing strategies would be slow and cumbersome; mobile business communications would be virtually ineffective in terms of time and convenience; and general business activities would not be viable.

All organisations now compete in a global market in which communication is instantaneous and competition for business is fierce. IT enables organisations to act with speed and agility. The different applications of IT enable them to engage in business activities that might otherwise be wholly impractical.

IT enables small organisations to compete with larger ones by addressing the needs of their customers proactively, efficiently, quickly and cost-effectively in a way that could not possibly be achieved otherwise.

The power and capacity of IT enables organisations to service volume markets or niche markets equally competitively. In other words, properly introduced, deployed and employed, IT enables organisations to compete in almost any market. The idea of an organisation expecting to conduct business competently and profitably without adequate IT support in the modern global marketplace is unthinkable.

The importance of the Internet

Internet technologies dramatically increase the importance of IT to every business and professional concern. Whereas traditional IT, such as accounting, may generally be regarded as 'back-office' systems, Internet technologies emerge as an offshoot of traditional IT and spawn an entirely new concept of IT systems.

Internet technologies are now dominant technologies, to the extent that any reference to IT automatically implies the inclusion of Internet technologies. What are Internet technologies? The categories of this model of IT are expanding rapidly. In the very early days, Internet technologies were limited to e-mail and the World Wide Web. Now, there is a proliferation of Web-based IT to the extent that almost all IT is Web based. Early developments included intranets and extranets, followed by Web-based telephony, known as Voice over IP (VoIP).

From these seemingly basic technologies, Web 2.0 has arisen. 'Web 1.0' technologies were largely passive technologies. For instance, websites providing brochure-type information and offering only limited opportunities for interactivity were typical of Web 1.0 technologies. They were technologies to which users responded rather than technologies which required user participation.

Web 2.0 technologies are quite the reverse. Models of Web 2.0 technologies, such as FaceBook, MySpace and Twitter, together with the rapid increase in blogging (the practice of posting weblogs) are essentially proactive Internet technologies. Here, participants exchange thoughts, ideas and personal details through electronic postings in as much or as little detail as they fancy.

With constructive content, weblogs can build into a significant body of knowledge. It is not unknown for organisations to encourage the posting of informative and relevant weblog content in order to generate interest in a website.

It might be argued that Wikipedia is a typical example of Web 2.0 technology. In this model, users post relevant and constructive information on a particular topic, citing authorities for propositions which become an authoritative body of knowledge and an information resource.

Web 2.0 users regard Internet technologies routinely as an interactive information and communications resource in which any number of participants might be involved. These technologies are not limited to what are widely regarded as 'social' networks. Professional networks, such as LinkedIn, operate for professionals to exchange opinions and network electronically to develop their business contacts and learn new ideas in their business activities.

The development of traditional IT systems and networks into a proliferation of Internet technologies which comprise a substantial knowledge resource offers opportunities for worldwide communication, enabling instant communication between any number of participants, either generally or between members of professional interest groups. This means that Internet technologies have become business tools that are equally important as the traditional IT from which they were created. Some of the principal business-value features are considered below.

Marketing

Initially, the importance of Internet technologies lay in their suitability as a marketing tool. E-mail marketing strategies enable the circulation of marketing information to a mass market of consumers in a way that is quite impossible by traditional mail.

Whenever information is required about goods and services supplied by organisations, a consumer's first reaction is to visit an organisation's website. Here there is an excellent opportunity for an organisation not only to market itself but, at the same time, to secure a purchase.

A further advantage is that the Internet enables marketing strategies undertaken through websites to be conducted globally at any time of the day or night – a strategy which is impossible in traditional marketing models.

Marketing through brochure websites has developed into interactive participation by prospective customers, who are often invited to take part in surveys and competitions and provide their views on the products and services on offer.

An extension of website marketing is the webinar – the Web version of a seminar – where prospective customers visit an organisation's website to listen, pose questions and provide feedback to an organisation offering educational information on the value and importance of its goods and services.

Business information

Sometimes as part of a marketing strategy, but not always so, organisations offer professional and trade information and guidance as part of its service to its customers. The idea behind this is not necessarily philanthropic.

The purpose of the strategy is to draw in new and existing customers through the provision of useful, relevant and timely information upon which the customer becomes increasingly reliant.

As a result, the customer relies on the organisation's site as a valuable resource and repeatedly returns to it for information and advice. This is a strategy commonly used by professional organisations supplying services to the business community.

Electronic transactions

A few years ago, electronic commerce was in a comparatively embryonic state. While electronic transactions and online businesses were emerging, generally, there was a significant element of mistrust. This arose largely from:

- the absence of the consumer from the conducting of the transaction;
- the perception of transmitting a remittance online without fully understanding how the transaction was being handled;
- general concerns over the security of the whole process.

Now, however, there is an abundance of confidence and a comparatively relaxed approach by consumers and organisations alike to transacting online. Consumers routinely make holiday reservations, bank online and make significant purchases, to name but a few transactions which are conducted online from start to finish. Beyond this, consumers now place far more trust in the information that is available online. Comparison sites of all descriptions are springing up and claim to offer interested consumers significant benefits in using their sites to shop around for bargains, particularly in the field of insurance quotations.

Most organisations recognise the importance of developing e-commerce strategies. For the organisation, benefits arise from the speed and relative simplicity of electronic transactions. For the consumer, the undoubted convenience of online transacting, for instance for the weekly supermarket shop, has now become a key factor in the increasing popularity of electronic transacting.

Business strategy

Internet technologies are now so popular that many organisations have adopted business strategies and models that are firmly embedded in, and rely entirely upon, the proper functioning of Internet technologies.

One of the earliest examples is LastMinute.com, which was formed in the early years of the 'dotcom' boom. The model of the business is based on consumers' need for last-minute solutions, for instance the need to find a gift at short notice. By logging on to the LastMinute.com website, the consumer can identify a suitable gift, pay online and have the gift delivered online almost immediately.

This type of strategy is not confined to commerce and industry. The professions also recognise the advantages of online strategies. The legal sector, in particular, has adopted online strategies in the conveyancing process.

Many law firms offer clients the opportunity to log on to a secure area of the firm's website and track the progress of their cases. As long ago as the late 1990s, solicitor Neil Davidson developed the concept of the 'virtual office', which provided law firms with a networked connection to a central office repository for the conducting of mainly IT and back-office functions.

The business strategy of almost every organisation is bound to take account of the influence of Internet technologies because their impact is all-pervasive. More important is the fact that Internet technologies can offer significant customer benefits in terms of a more cost-effective, speedy and quicker service.

Strategic alliances

The ability of Internet technologies to offer lines of electronic communication has made possible the emergence of online strategic alliances.

Again, the legal sector has developed a number of initiatives in this area. Law firms form online strategic links with estate agents and lenders in which the firm's website becomes a repository of information about the progress of a (conveyancing) transaction and enables interested parties to log on and establish the position.

In this connection, the Land Registry has developed a prototype system of electronic conveyancing. The focal point is an electronic grid which enables parties to the transaction to log on and identify the current stage of the transaction – and, incidentally, where responsibility lies for the causes of any delay!

Business models

The real impact of Internet technology is probably only just beginning. As it is, the effects have already been radical enough. Competently deployed and suitably applied, Internet technologies are able to reduce costs, increase speed and efficiency and provide a global reach.

They offer opportunities to develop novel business models and propositions because of the very nature of the technologies themselves. Examples include:

- e-mail enabling communications to be sent round the world in seconds;
- websites offering marketing and transactional opportunities worldwide;

- intranets enabling any organisation to develop, record and archive its knowledge base into a formidable repository of intellectual property;
- extranets enabling organisations to forge online links and alliances with strategic allies such as introducers and referrers, as well as providing customers with access to secure areas for the monitoring and performance of their transactions;
- Internet technologies enabling economies of scale to be achieved because they can be deployed for the volume provision of goods and services;
- Internet technologies being programmed for use in the service of specialist and niche markets and personalised services, where the technology is developed to very close specifications;
- Web 2.0 technologies offering the opportunity for a broad exchange of concepts, strategies and business development opportunities based on the facilities for information sharing that they offer.

Each of these illustrations supports the prospect of a continuing and radical change in business models throughout both commerce and the professions.

Internet risk

Released at the *Infosecurity Europe Conference and Exhibition* in April 2010, the *Information Security Breaches Survey 2010,* published by PriceWaterhouseCoopers, revealed some concerning statistics regarding corporate information security. Some of the findings recorded:

- the cost of a breach is between £27,500 and £690,000;

- the most security breaches to date;
- a threefold increase in malicious attacks compared with the previous year.

Although the use of Internet technologies has developed at a rapid pace and penetrated all areas of commerce, industry and the professions – as well as government agencies and academic institutions – in fact every area of modern life, their deployment presents significant risks with potentially catastrophic implications arising from any mismanagement. In order to understand what these risks are and how they can be managed, it is necessary to appreciate why they arise.

Internet technology features

Risks arising from the use of Internet technologies develop principally from the fact that they are disruptive technologies. The full implications of their use are not always properly understood until problems arise – in other words, when risks, which have not been assessed and managed, become crises. In their present state of development, it is fair to say that, to some extent, Internet technologies are anarchic in nature.

Internet technologies introduce new ways of conducting business and promulgating information. In almost every area of life, Internet technologies can alter traditional processes and introduce new models. For instance:

- Internet technologies are not confined within any recognisable structure or framework.
- The speed of communication and dissemination of information changes consumer and supplier relationships

and gives power to the customer, whose expectations are raised.

- Internet technologies recognise no boundaries and are essentially global in nature.
- Internet technologies have the capability of replacing intermediate services; for instance, insurance cover can be arranged directly through an insurer's website without the need for brokerages – similarly, brokerages are threatened by the emergence of comparison websites.

Effectively, what emerges is the appearance of a new engine in an old model. In the traditional model, managing consumer expectations is more straightforward. However, the speed and efficiency of Internet technologies empowers the consumer and places the onus on the supplier to respond effectively in order to retain market share.

Key features of the differences between the traditional and Internet models include the following.

- In the traditional model, change tends to be gradual and structured; in the Internet model, change tends to be sudden, unstructured and with wide-ranging effects.
- The traditional model, on the whole, is not subject to global scrutiny; the Internet model exposes every organisation to global vulnerabilities with the potential for far-reaching consequences.
- In the traditional model, strategic alliances are formed relatively close at hand with familiar organisations and agencies; in the Internet model, strategic alliances may be formed globally without any real knowledge of the partners concerned.
- In the traditional model, skills and competence are generally acquired through the development of long-

term know-how; in the Internet model, technical skills are developed and acquired rapidly, and, furthermore, they are frequently skills not recognised in the traditional model.

- In the traditional model, statutory, regulatory, codified and compliance provisions are easily identified and their application is relatively straightforward; in the Internet model, the application of similar provisions is far more challenging because Internet technologies are able to transcend boundaries.

Internet technologies, therefore, introduce fundamental changes which are quite unfamiliar in the traditional business model. Globalisation, together with the absence of a recognisable legal and compliance framework and the speed, flexibility and agility of Internet technologies provide an unprecedented change in the manner in which commercial and professional services are delivered.

Internet technologies demand transparency, openness and trust between customers, organisations, suppliers, strategic allies, introducers, stakeholders and shareholders, because Internet technologies are, by their nature, transparent. Internet technologies introduce novel concepts for providing goods and services which are not recognised in the traditional business model. Internet risk arises from these new concepts.

Internet technology risks

The principal risks arising from Internet technologies can be conveniently divided into three categories: technology risk; legal and compliance risk; and operational risk.

Technology risk

This category of risk has its origins in the technology employed in the fabric of the Internet. The most obvious example is the proliferation of computer viruses and their capacity to embarrass organisations, affect system performance and occasionally lead to system failure. This risk is most obviously managed by the deployment of up-to-date anti-virus software.

Another technology risk area is the communication of sensitive and confidential information by unencrypted e-mail. Here, an organisation may need to equip itself with adequate encryption facilities and educate personnel on their use and application.

Legal and compliance risk

This category of risk arises from failure to comply with statutory and regulatory provisions that govern the use of Internet technologies. In some ways, this is the most problematic category of risk to manage adequately.

The disruptive and radical changes that Internet technologies bring to commerce, industry and the professions were considered earlier. A key issue is that most statutory and regulatory provisions are enacted for what might be termed terrestrial concerns. They are not always easy, or practical, to apply to the ethereal and global nature of the Internet. An example of this is Cloud Computing, which is considered later.

In simple terms, most legal and compliance risks will be addressed by observance of the statutory or regulatory provisions governing the circumstances. However, in some cases, such as the application of relevant law and jurisdiction in global disputes, these provisions can be extremely complex and very difficult to apply.

Operational risk

This category of risk arises from business and professional strategies and practices that an organisation adopts in providing goods and services, the manner in which the organisation manages its employees, and the policies and procedures implemented to govern the organisation's relationship with its customers.

In practical terms, management of operational risk is addressed by the introduction of policies and protocols that govern employee conduct in using Internet technologies. Examples include policies for: the use of e-mail; the use of the World Wide Web; the management of the organisation's website; and data protection compliance.

Each of these risk areas exists for every organisation employing Internet technologies and each raises important considerations for all organisations. In order to address these risks, organisations need to assess the level of expertise at their disposal. If there are insufficient skills and competence available, the recruitment of suitable personnel may be necessary. Proper control of each of these risk areas raises significant management implications for any organisation.

These categories are not mutually exclusive and in many respects they overlap. For instance, managing information security issues might involve each of the three categories. There might be a technological solution (the introduction of a security solution), a legal compliance solution (compliance with data protection provisions), and an operational solution (training employees in the proper handling of data through appropriate acceptable use policies). A similar example of overlap might include the downloading of unacceptable material from the Internet.

It is important that the three categories are not considered in isolation and that the identification of Internet risk is mapped across all categories in order to obtain a complete management solution.

Internet risk implications

What are the implications of failing to take adequate measures to address the risks that arise from use of Internet technologies? Every organisation is different and risks affect organisations in different ways. Some of the most significant implications are listed below.

Reputational damage

The speed, cost-effectiveness and efficiency with which Internet technologies enable organisations to provide goods and services offer the opportunity for organisations to enhance their reputation significantly in a competitive marketplace.

However, in a marketing environment where excellence of performance is a key factor, any incident which damages this will have a significantly adverse effect on an organisation. In the Internet environment, reputation is hard won, but easily lost. System down time, service interruption caused by a virus, racial or sexual innuendo in an e-mail; or inaccurate or misleading information posted on a website can damage the reputation of any organisation in an instant.

Legal proceedings

In certain situations, organisations that mismanage Internet risk can find themselves subject to civil or criminal proceedings. Examples include the following:

- infringement of certain provisions of the Data Protection Act 1998 (DPA) can result in criminal proceedings which can carry heavy fines; a number of law firms have been fined for having failed to register with (notify) the Information Commissioner (ICO);
- posting sexually or racially discriminatory material on a website or inclusion of such material in an e-mail may lead to prosecution under equality legislation;
- publishing obscene material in an e-mail is a criminal offence under the Obscene Publications Act 1959 (OPA);
- monitoring employees' use of e-mail and accessing the World Wide Web may result in proceedings if the provisions which govern this are not strictly observed.

In civil proceedings, damages or an injunction may be ordered for:

- misleading material posted on a website on which a visitor to the site relied to his or her detriment;
- the posting of libellous statements on a website without lawful excuse or justification;
- the loss of confidential and sensitive data as a result of system failure;
- the posting of copyright material on a website without permission of the copyright holder;
- erroneously entering into online contracts which are not then fulfilled.

There are numerous circumstances in which an organisation can be exposed to proceedings for infringement of legal and compliance responsibilities or failure to take adequate precautions in employing Internet technologies.

Consumer relationships

Failure to manage systems and processes introduced by Internet technologies can irreparably damage consumer relationships.

A website that posts outdated and inaccurate information is a major disincentive to any potential customer visiting the site with the intention of making a transaction. It is a clear indication that an organisation lacks interest in, and respect for, actual and potential customers.

Frequent system down time resulting in delayed provision of goods and services, or frequent interruptions to online services will soon affect an organisation's customer relationships. In the context of finding new suppliers or sources of information, the Internet breeds a promiscuous and unforgiving consumer who rarely offers an organisation another chance.

The cumulative effect of these implications is a serious impact on an organisation's business strategy. Reputations carefully and painstakingly established over a long period of time are suddenly lost and may never be restored. Criminal proceedings attract unwanted publicity and damage the competitive reputation in the marketplace at a stroke.

As a result, an organisation may have to cease trading temporarily and even reconstitute its business plan. A number of organisations have been fined several hundred thousands of pounds recently for data protection breaches.

Any organisation that fails to take account of the risks inherent in Internet technologies, and then fails to adopt an adequate risk management strategy for their avoidance or containment, puts at risk nothing less than its very existence.

The importance of governance

If there is one strategy for addressing, and ultimately controlling, the anarchic features of Internet technologies, it is the application of sound governance principles.

Governance principles enable an organisation to manage the tools of its trade (for instance, IT and Internet technologies), its business activities and its personnel in such a way as to:

- provide value and return on investment for shareholders and other stakeholders;
- realise the objectives in its strategic business plan.

In respect of Internet risk, there are three categories of governance to be addressed: corporate governance, IT governance and project governance.

Corporate governance

Corporate governance principles emanate from the Board of Directors or Partners and should be applied throughout all levels of management of the organisation.

In essence, corporate governance is a business strategy based upon transparent decision making; the establishment of lines of accountability and responsibility; securing shareholder and stakeholder value; and the adoption of sound risk management strategies, including information security.

Corporate governance is a culture created by the Board and Partners to be reflected throughout the organisation.

IT governance

The unpredictable, rapid and occasionally haphazard emergence of solutions based on the application of Internet technologies calls for specific governance principles to be applied for the management of IT strategies.

IT governance is a subset of corporate governance. IT strategies need direction and management in exactly the same way as the overall strategic business plans of an organisation.

IT governance is essentially a framework within which IT is designed, deployed and managed in such a way as to ensure that its employment and application remain aligned to the organisation's business objectives.

This principle applies to all IT infrastructures, platforms and applications, of which the management and administration should also embrace the principles of corporate governance as IT governance principles are introduced.

The implementation of IT governance principles is supported by various tools and methodologies. The most notable is the international standard, BS ISO/IEC 38500:2008, which is a standard developed for directors and senior managers for the corporate governance of information technology. It provides organisations with a framework of principles for the achievement of the effective use of IT and provides a model for the Board's involvement in IT projects.

In accordance with true governance principles, the standard addresses the interests of stakeholders and provides guidance on the evaluation of corporate governance of IT.

Project governance

Project governance may be regarded as a subset of corporate governance, sitting alongside IT governance. Most business activities surrounding IT are, in effect, projects.

Project governance is a set of principles that addresses the development, management and conclusion of projects. The key constituents of project governance principles comprise clear leadership and commitment at the highest (board) levels; the procurement of adequate resources; suitable lines of accountability and responsibility; the adoption of appropriate project management and implementation methodologies; and relevant risk management strategies.

Few organisations confine themselves to only one IT project. In theory, the use, encryption, management, storage and archiving of e-mail are all sub-projects of the single project of e-mail management.

The development, maintenance and supervision of an organisation's website are three sub-projects of a single project – the organisation's web strategy.

Outsourcing some or all of an organisation's IT function is a third project that calls for the application of governance principles.

It is important to understand that all IT functions are, whether large or small, IT projects to which project governance principles must be applied. Many organisations will have numerous IT projects. These can result in a confused execution of an IT strategy. Projects may overlap or be mismanaged, or fail to provide a return on investment. As a result, ultimately, the organisation's project strategy loses direction and consequently fails.

For this reason, project governance principles embrace the creation of a framework for the management of multiple projects – programme portfolio management (PPM).

Organisations use PPM methodology to identify and define the scope of each project within a specific portfolio and continually assess it against the general corporate governance principles of risk, stakeholder value, correct lines of accountability and responsibility, transparency of decision making, risk management and continual alignment with the organisation's expressed business strategy and objectives.

Managing risk

Risk assessment and management are key components of corporate, IT and project governance principles. The application of governance principles is designed to ensure the welfare of shareholders and stakeholders, achievement of the organisation's goals and objectives, and a return on investment.

None of these objectives is achievable in the absence of a comprehensive and properly executed risk management strategy. For this reason, risk assessment and management are core requirements in the application of corporate governance principles.

Risks abound in every Internet technology project and arise at strategic IT, legal and regulatory compliance, and operational levels. Effective application of corporate, IT and project governance principles enables these risks to be confronted and managed systematically.

Strategic risks arise, for instance, from the management of a website which offers advice and guidance to visitors. Care must be taken to ensure the advice is correct and timely and regard must be paid to the fact that the website is globally accessible and that advice may not be universally appropriate.

Legal and compliance risks arise most obviously from failure to comply with the DPA, for instance failing to ensure the safety and security of confidential data.

Operational risks arise, for instance, where employees may post defamatory or otherwise unsuitable comments on one of the many social websites, or indulge in online gambling, or contribute to newsgroups without permission or authority.

Risk identification, assessment and management are the responsibility of the Board and Partners. The establishment of a risk management framework is a function to be performed at board and partnership level.

Each organisation is different but such a wide variety of risks arise from Internet technologies that a dedicated risk manager is almost certain to be required. In larger organisations, a risk management team may be required comprising, or having access to, specialists in IT, legal and compliance, and personnel management. The risk management team should be led by, and accountable to, the risk manager, who in turn should be directly responsible either to the Board or to a senior manager who is accountable to the Board on recognised line management principles.

The need for governance principles

Corporate, IT and project governance principles are designed to ensure that an organisation performs cohesively and collectively towards the achievement of its strategic goals and objectives.

But why is the application of these principles so important? What do the principles bring to the 'corporate table'? Governance principles are highly desirable, but why are they needed? There are a number of factors which, taken together, make a compelling case for the adoption of governance principles.

Control

The application of governance principles ensures the organisation, through its board or partners, is able to maintain a close control over its strategies, functions and performance standards. In turn, this leads to a greater assurance that its goals and objectives are achievable in the long run.

Direction

A board or partnership that espouses governance principles is able to exercise direction over the control that the governance principles offer. In the case of IT strategies and IT projects in particular, all too frequently, over time, an organisation's IT strategy becomes misaligned with its objectives and fails to provide anticipated returns on investment. Rigorous direction enforced in accordance with governance principles minimises this risk.

Leadership

Corporate governance principles and their implementation are the responsibility of the Board and Partners. It is they who set the culture and establish the management framework within which the organisation implements strategy and achieves defined strategic objectives.

Personnel

The assumption of control, direction and leadership by the Board and Partners, underpinned by transparent decision making, encourages a culture of accountability and responsibility throughout the organisation, which can be observed and implemented by personnel at all levels.

Motivation

Organisations, the functions of which are properly controlled and directed under robust leadership supported by its personnel, are more attuned to the need to attain and maintain acceptable standards of performance arising from mutual respect between board and partners, management and subordinate staff.

Understanding

Clear leadership and direction supported by transparent decision making help all levels of personnel to:

- understand fully the organisation's strategy and the goals it is intended to achieve;
- appreciate their roles and responsibilities;
- understand the need for teamwork and a collective approach to achieving the organisation's objectives.

The wide range of risks to which Internet technologies can give rise requires a collective approach towards, and a firm understanding of, methods of their management – both essential components of managing Internet technology risk.

CHAPTER 2: TECHNOLOGY RISKS

There are numerous consequences of mismanaging Internet risks. Missed business and professional opportunities, failure to capitalise on the potential for developing business opportunities, and an inability to compete adequately for market share are all potentially incidental consequences. Consumers and clients need confidence that organisations deploy, manage and operate Internet technologies with the skill, care and expertise that offer assurance of good practice in the conduct of their business.

Technology risks arise from the deployment, use and operation of technology systems. Typical technology risks arise from insecure messaging systems and inadequate security in the management of data; insufficient business continuity and disaster recovery systems to confront the threat of hackers and other types of intruder; and insecure electronic payment systems. They are referred to as technology risks because they arise primarily from the use of Internet technologies.

The principal technology risks arise from the handling of communications and information. In both respects, security and confidentiality are key concerns for any organisation.

Internally, concerns arise from the way in which confidential and sensitive data is managed, for instance the loss of one or more CD-ROMs containing confidential databases. Externally, similar concerns arise over the exchange of communication and data with consumers and those with whom the organisation may have formed strategic alliances, such as those introducing work or collaborating with the organisation in the provision of goods and services. Here, the principal threat is from external hostile sources interfering with communications and misappropriating confidential data.

The complaint is often heard from senior managers that security is a ‘hard sell’ to boards of directors and partners because it provides no tangible return on investment in terms of greater profitability or the attraction of more business. Commercially, this is an unacceptably short-term view. There are now two major considerations for any organisation in the global marketplace:

1 The need to assure consumers of the security and confidentiality of data in accordance with the provisions of the DPA.
2 The increasing tendency of potential consumers to require organisations to specify what security measures are in place for the secure management and confidentiality of their data before entering into a contract for the supply of goods and services.

The various technology risks will be considered in the general categories of:

- communications risk;
- information security risk;
- business continuity;
- IT outsourcing;
- social networks.

Communications risk

Although there are competing methods of communication, such as instant messaging and VoIP, e-mail remains the principal Internet communication technology.

E-mail

There are four key risks to be addressed in achieving adequate security and confidentiality in respect of e-mail communications:

- **privacy:** e-mail must be transmitted, so that only the intended recipient can read it;
- **integrity:** e-mail must be sent with the confidence of both sender and recipient that there is no opportunity for interference with, or alteration to, its content;
- **authenticity:** e-mail must be sent with the confidence that the recipient can be certain of the person by whom it was sent;
- **reliability:** e-mail must be sufficiently reliable for the recipient to be able to act upon it with confidence that the sender cannot repudiate it at a future date.

These communication risks apply to both internal and external e-mail.

However, e-mail also carries additional risks that go beyond confidentiality and security between sender and recipient:

- **Attachments** may include malware in the form of viruses, such as Netsky. When the attachment is opened, the virus infects the user's computer and proliferates by automatically despatching itself to addresses in the user's e-mail address book.
- **'Phishing'** is a term assigned to e-mail which purports to originate from a source that is well recognised by the user, or from a source that is of high repute, and on which the user acts to his or her detriment. Most frequently, users are persuaded to click on a link to a bogus website resembling a financial institution and to

enter personal (security) details which are collected by the website hosts and used to obtain access to the user's account.

- **Social engineering** is a term to denote the response of a recipient of an e-mail inviting the recipient to react to an e-mail for his or her benefit. Frequently, the user is persuaded to release user names and passwords or, in other cases, to part with money in response to a request to contribute to a 'good cause'. In other situations, the result can be that the user downloads a virus.
- **Storage and archiving of e-mail** is subject to various legal and compliance provisions and is also required for the purposes of electronic discovery of legal documents in legal proceedings.

The risks of using e-mail arise from both the use of the technology and the failure of personnel to be properly trained and educated in the risks.

Instant messaging

Instant messaging (IM) comprises text-based electronic communications sent in real time, as opposed to e-mail which is not necessarily sent contemporaneously. Its most useful function is to communicate short messages to large numbers of personnel, for example urgent departmental instructions.

Data flow is generally internal and may, therefore, not be protected by firewalls, filters and URL (website) blockers. Risks from the use of instant messaging technology arise in a number of situations such as:

- the distribution of pornographic or copyright material;

- vulnerability from the free-flow unencrypted data which may be exposed to hackers, interception of communications and network insecurity;
- the infiltration of viruses and similar malware;
- the assumption of false identities through the uncontrolled use of screen names;
- the emergence of 'spim', the equivalent of e-mail spam, which can in turn lead to 'phishing' attacks and social engineering exploits;
- lack of knowledge within organisations as to who is using internal messaging systems;
- failure to maintain formal records of IM communications for the purposes of relevant legal and compliance provisions.

Voice over Internet Protocol

This is a network telephony protocol used for the transfer of voice data over the Internet. Rather than using a dedicated telephone network, voice calls are sent over existing digital networks using the Internet.

Skype (www.skype.com) is an example of telephony technology which enables users to make calls using Internet technology. Calls to other users are generally free, unless made to landline or mobile telephones.

As a result, many organisations are now using converged communication networks for voice and data, commonly referred to as unified communications. Some of the benefits include free calls between departmental offices; lower maintenance costs for the use of one network; and flexibility for remotely located personnel.

Potential risks from the use of VoIP communications may arise in a number of situations:

- since VoIP involves the use of the Internet, the same potential vulnerabilities arise as in the case of e-mail and IM;
- potential vulnerabilities arise in respect of hackers, denial-of-service attackers and eavesdroppers;
- VoIP calls can be decoded and calls can be intercepted and redirected;
- 'phishing' attacks can emerge, where an intruder poses as an institution or other trusted body and obtains confidential data;
- spam over Internet telephony can arise, otherwise referred to as 'spit', in the same way as applies to e-mail.

Networks

In any organisation, communications are contained within a network. Networks link all personnel internally and may also link external agencies, such as other stakeholders, suppliers, introducers and strategic allies.

Most importantly, it is now common for networked communications to be extended to include consumers and clients. The most common mechanism for this is the secure extranet. This enables consumers and clients to interact with the organisation over business in hand and to track and supervise how the transaction is conducted.

Networks are protected by firewalls, which are dedicated computers governing the entry and departure of data from the organisation's network. In other words, a firewall is software configured to prevent the entry of unwanted communications, and which can also prevent the sending of certain material.

However, in recent years, the proliferation of mobile devices, such as laptop computers, mobile phones, iPods and the Blackberry as well as removable storage devices, such as the CD-ROM and memory sticks means that increasing amounts of data are now passing beyond the corporate network and, therefore, beyond the control and management of the corporate firewall. This trend for data to be removed beyond the traditional network is called deperimeterisation. The volume of mobile communications makes deperimeterisation a business necessity.

Business is now conducted globally and mobile workforces operate all over the world, connected to the organisation's network through mobile devices. Data no longer remains under the protection of the corporate firewall; it is stored in numerous portable devices owned and managed by a wide variety of personnel, each of whom is connected to the network.

An example of the vulnerability of organisations in this respect is the recent loss of a CD-ROM which contained data relating to approximately 25 million individuals who were in receipt of child allowance.

A more frequent example is that of laptop computers being left in taxis or otherwise mislaid, without any form of data encryption being applied to the hard drive.

Portable storage media present a particular danger. A disgruntled employee with access to the corporate network can download and save valuable corporate data on a memory stick in a matter of seconds and pass the contents to a competitor. Such storage devices are also capable of being used to spread viruses, which can enter the network and cause significant periods of down time.

The risks from the deperimeterised environment raise some difficult issues, such as:

- the need to develop policies to ensure remotely working personnel protect the organisation's data;
- the need to identify and apply technologies that will secure the different types of mobile communications and storage devices;
- the prevention of loss of data;
- the need for additional security procedures for the performance of the organisation and its personnel;
- the need to develop a security infrastructure beyond the network at proportionate cost.

Firewalls offer adequate protection within a closed and defined network, but cannot be applied to individual types of mobile device. Encryption of data is a partial solution, but there is nothing to stop the owner of, say, a company laptop computer from transferring an unencrypted version of the data to another computer or memory stick.

Hackers are a threat to any network. Their prime objective is to obtain access to a corporate network through breaching security. Some hackers are 'professionals' while others are bored or disaffected employees or even youths.

Wireless networks pose considerable risks to organisations whose employees use this technology. Increasingly, wireless-enabled mobile technology is employed with users having little understanding of the security implications. Critical for adequate network protection are the security settings on routers. Default settings from the manufacturer are not necessarily sufficient. The highest level security protocol, WPA2, should be applied.

Hacking is an offence under the Computer Misuse Act 1990. Section 1 makes it an offence to access computer material without authority; Section 2 makes it an offence to access material intending to commit further offences; and Section 3 makes it an offence to modify data, for instance by the introduction of a computer virus.

This Act was amended by the Police and Justice Act 2006: Section 35 extends the definition of accessing a computer without authority; Section 36 extends the scope of committing acts with intent to impair the operation of a computer; and Section 37 addresses the making, supplying or obtaining articles for computer misuse offences.

Typical hacking activities might include:

- defacement of a website;
- obtaining access to and stealing information;
- corrupting data;
- the illicit use of credit cards in corporate payment systems.

Information security risk

Data is a highly valued corporate asset. The numerous types of Internet technology mean that data is stored in a wide range of sources within in an organisation. Examples are hard drives, memory sticks, mobile devices, intranets and extranets, and storage area networks.

Not only must an organisation protect its data from external intruders and hackers, it must also ensure that personnel are trained and educated in appropriate data-handling procedures, usually through acceptable-use policies.

The wide range of data sources and storage devices combined with the need to impose and manage internal and external technological and operational controls make a consistent approach to data management a significant problem for any organisation.

Apart from data leakage and the direct theft of data by external parties, such as hackers, there are other issues that arise in which the organisation does not necessarily suffer a loss of data but, instead, data is in some way compromised.

Websites

Website ‘scraping’ can be a potential risk to valuable data, if performed illegally or without authority. This involves the extraction, collation, harvesting and retention of data from websites; a practice which may potentially be in breach of the terms of use of many websites.

Websites and their data are also at risk of Structured Query Language (SQL) attacks, involving the injection of infected code that exploits vulnerability in the sites’ incorrect or inadequate programming or scripting language. This presents the opportunity for hackers to gain access to sensitive data and even to hijack databases.

Passwords

Both externally and internally, individuals can manipulate and change passwords and their settings to gain access and entry to network systems. A determined intruder can always employ software to identify passwords.

Even today, passwords remain a highly popular method of verifying identity. Yet individuals can be remarkably casual over protecting passwords, and where passwords are created for access to numerous sources, they are frequently lost or forgotten. Passwords create a number of problems:

- they offer only limited proof of identity;
- they have no legal validity;
- they cannot be verified;
- they are difficult to remember;
- they need continual updating.

As an example of a casual approach to passwords, some users write them on Post-it® Notes, which can then be found stuck to the computer monitor!

Viruses

Viruses are one of the most common and serious threats to data integrity and security. A Google™ search reveals several hundred different types of known computer virus and more continue to emerge. A computer virus is difficult to define, but fundamentally it is a computer program which:

- infects a computer;
- might remain dormant;
- remains dormant until triggered by a host computer;
- causes a computer or network system to fail;
- damages or distorts data; or
- infiltrates other computers on a network.

A virus may be activated on booting up a computer, or by opening an infected attachment, or even visiting an infected website. The most common virus types are:

- a malicious virus, which is spread by opening infected e-mail attachments or documents;
- a Trojan Horse, where malicious code is concealed beneath an apparently harmless program;
- a worm, which develops and insinuates itself throughout a network.

Most virus attacks are general in nature, but an emerging threat is the targeted Trojan. This delivers a malicious attack to a specific recipient or group of recipients, most commonly involved with organisations handling high-value data. Furthermore, these attacks are frequently directed at those holding positions of the highest seniority.

One recent, highly damaging virus is now circulating, the Conficker virus, which attacks operating systems. Having infected one computer, it then proceeds to infect other networked computers, connecting them in such a way that the 'network' of infected computers falls under the control of the virus writers. Some sources suggest that the virus has spread worldwide and it is now considered by many to be one of the most widespread virus infections in computer history.

Miscellaneous

There are a number of other types of computer infiltration:

- **Botnets:** this is an abbreviation of 'robot networks', whereby a hacker infiltrates one computer and is able to control it remotely. The infected computer is referred to as a 'zombie' and forms part of a network of robot computers. Often, the computer user is quite unaware of the infection.

- **Cookies:** these are small programs 'collected' by a computer on visiting a website. They record the computer's visit, so that it is recognised on any subsequent visit, and track details of the user's interests. They are essentially a commercial device to enable the website host to market its goods and services more effectively to site visitors. The problem with cookies is that confidential details are released, which are then stored by the website host without the user's knowledge or consent.
- **Spam:** this is unsolicited commercial e-mail and is effectively the electronic equivalent of the junk mail delivered by the traditional postal service. Most spam is sent from infected computers and, despite its name, can yield significant profits for senders. Spam creates a number of problems:
  - significant quantities of spam e-mail can bring down an e-mail system, sometimes referred to as a 'denial-of-service' attack;
  - it can take a considerable amount of time for users to filter spam from genuine e-mail;
  - spam can infect receiving computers with viruses and similar programs.

Some users are now being exposed to spam through social networking sites on which they reveal their identities and contact details, and then become targets for spam e-mail:

- **'Pharming':** essentially involves an attack on an organisation's website which results in visitors being directed to a bogus website operated by the attacker. This is usually perpetrated by exploiting vulnerability on an organisation's web server.

- **'Phishing':** is an increasingly common form of attack by which the perpetrator invites the user to provide personal or organisational details through manipulative activities, such as verification of online banking security details as part of an auditing exercise. This is commonly expressed to be 'social engineering'. Once confidential information is divulged, the perpetrator exploits this accordingly.
- **Drive-by attacks:** involve the user downloading material from the Internet which subsequently is found to contain malware of some description. This may occur when downloading legitimate software which is later found to be infected, or may arise when the user is duped into downloading spyware or other infected code without their knowledge, such as by answering an advertisement.
- **Spyware:** is a program that is 'collected' by a computer without the user's knowledge when visiting certain websites – or when the user complies with a request to download apparently harmless software. Spyware tracks users' activities without their knowledge. Linked to this is the practice of 'keylogging', where software is downloaded to a user's computer which enables the user's keystrokes to be tracked and used to obtain confidential details of, for instance, passwords and credit cards.
- **Website vulnerabilities:** can arise in a number of ways, including the presence of malicious code; leakage of confidential data; insufficiently protective architecture; and inadequately deployed defensive measures.

Online payment systems

Electronic service delivery is now a routine process but nonetheless still carries serious risks. Consumers now make online purchases in the expectation that the systems and networks employed will retain credit-card data safely and securely.

Two principal risk areas arise in online transactions:

- the confidentiality of the identity of the consumer who is conducting the transaction;
- the potential for criminals to gain access to the merchant's system and obtain details of consumers' credit cards.

In all such transactions, there must be some assurance that the identity of the consumer is accurately verified and that the transaction is conducted securely and confidentially.

In late 2006 and early 2007, considerable publicity surrounded the infiltration of the systems of a major retailer in which intruders accessed systems which processed and stored consumer information collected in the use of credit cards, debit cards and related transactions.

The payment card industry (PCI) has developed a set of standards with which providers of payment services are expected to comply and these are considered later.

Business continuity risk

The seriousness of the risk to an organisation's business continuity arising from Internet technology 'failure' is frequently underestimated.

Many organisations either have no viable business continuity plan in place, or have a plan which remains untested, or have a plan which has been tested and found to be inadequate yet where the inadequacies remain to be addressed.

Business continuity and disaster recovery plans are frequently not a priority on an information security budget because their incidence is a relative rarity. However, Internet technologies introduce an environment in which consumers expect service 24 hours a day, 7 days a week, 365 days a year. System failure which results, for instance, in the suspension of an organisation's website can considerably damage the reputation and credibility of an organisation in the eyes of consumers.

The scenario is exacerbated where an organisation relies on a network of strategic allies for the supply of its goods or services. Imagine the reputational damage to a firm offering professional services through a network involving lenders, surveyors, estate agents and local authorities in which transactions are brought to a halt through the absence of a business continuity plan.

Examples of the principal threats to business continuity have already been considered. They include:

- the entry of hackers into the corporate network;
- the infiltration of viruses;
- the receipt of spam e-mail in such quantities that the organisation's system is unable to cope.

Another agent for damaging business continuity is the denial-of-service attack. In this situation, a hacker infiltrates corporate systems and overloads the system in such a way as to interrupt their normal operation. Most frequently, the targets are websites and servers as these are essential technologies for almost all organisations.

One of the most popular methods of inflicting a denial-of-service attack is by a launch from each computer in a network of robot computers, so that the organisation sustains multiple attacks. This is termed a distributed denial-of-service attack (often referred to as a DDoS).

Cybercrime

A significant threat to information security is that of cybercrime. This is criminal activity most commonly designed to secure financial reward through criminal exploitation of Internet technologies. ‘Hacking’ into the website of a large organisation and misappropriating critical and confidential data is a common form of cybercrime.

Typical examples of this type of crime involve the distribution of malware, the spreading of virus-infected code, or attacks which threaten the ability of an organisation to operate – sometimes referred to as a ‘denial-of-service’ attack and often perpetrated through the distribution of vast quantities of spam e-mail.

The motivation for cybercrime, however, is not confined to purely commercial motives. Financial gain can be obtained through other means, such as the distribution of obscene or pornographic material; drug trafficking; fraudulent activities such as altering, deleting or manipulating data; abusing software and operating a variety of ‘scams’; and even terrorism.

Cyberwarfare

In extreme, if rather unlikely, circumstances, an organisation may find its information security compromised in cyberwarfare activities. Espionage, website hacking, data theft, denial-of-service attacks and infrastructure attacks are common examples of such activities. Emily Freeman, Executive Director, Technology Risks, Lockton International, says:

> The emergence of 'cyberwar' in the context of attacks on organisations' critical infrastructures; the increase of espionage (whether by individuals, entities or countries); and the vulnerability of critical infrastructure systems are some of the key current concerns of corporate clients. Cyber risk insurers are very concerned about the worldwide exposure to disclosure or theft of high-value data, especially non-public financial or medical information.

The damage to an organisation as a result of either cybercrime or cyberwarfare attacks, even if rare, should not be underestimated. Loss of confidential data, damage to reputation and professional integrity, and breaches of professional obligations are all potential risks to business professionals.

IT outsourcing risks

Cloud Computing, also referred to as 'software as a service' (SaaS), is an emerging model of computing in which an organisation's software requirements are outsourced to a specialist supplier who provides these services over the Internet – hence reference to the 'Cloud'.

It is effectively a subscriber-based hosting service, universally available and scalable for single (single-tenanted, dedicated or private Cloud) or multiple (multi-tenanted or public Cloud) organisations. It is provided as an on-demand facility in the same way as traditional utility services.

Cloud services are frequently provided from farms of virtualised servers, each holding vast amounts of data belonging to organisations using the service.

There are some obvious attractions for outsourcing the management of information security technology to an experienced supplier. The organisation may benefit from the economies of scale that a specialist supplier of security services can bring as against the total cost of ownership and management of a full-scale dedicated in-house information security department. A supplier may be able to provide security upgrades faster, less expensively and more regularly, and provide a swifter and more comprehensive response to incidents and generally manage the organisation's security technology strategy more efficiently and effectively.

As with all emerging Internet technologies, Cloud Computing presents a number of risks which have yet to be addressed satisfactorily:

- **Service interruption:** this is the risk of the supplier being unable to maintain its service to the organisation which, in turn, affects the organisation's service to its end-users.
- **Availability of data:** an organisation must be guaranteed access to its data at all times; any interruption or periods of sustained down time will prevent this.
- **Virus infection:** while under the management of the supplier, the organisation is exposed to the risk of data

contamination, especially in the case of multi-tenanted servers with the potential for cross-contamination.

- **Deperimeterisation:** in the Cloud model, the supplier operates outside the organisation's corporate firewall and the organisation's data suffers a corresponding reduction in levels of protection.
- **Criminal activity:** the storage of large quantities of data in server farms is potentially a considerable attraction for cybercriminals, who may be able to bypass identity management procedures.
- **Data management:** the remote storage of data has a number of implications for an organisation, such as:
  - loss of control;
  - securing access to the data, for instance for the purpose of legal proceedings;
  - securing the safe return of data at the end of the outsourcing contract;
  - ensuring the supplier adopts safe and compliant data management procedures;
  - the risk of data leakage;
  - the safety of data should the supplier become insolvent;
  - ensuring the security and confidentiality of data.
- **Jurisdiction:** a Cloud supplier may be based in a foreign country, raising jurisdictional and applicable law issues.
- **Certification:** the absence of any reliable standards of certification of the performance of Cloud suppliers.

Dennis Farm, Enterprise Infrastructure Audit Manager at Morgan Stanley, comments:

> A current problem is the potential for hacking into networks and systems by external parties. With the current tendency for network perimeters to extend significantly through the use of

mobile technologies and remotely situated personnel, it is almost impossible to remain incident-free in this respect.

It is clear from the range and type of issues listed that Cloud Computing presents some significant risks for organisations choosing to adopt this model for managing its technology. As with all Internet technologies, development of new solutions presents potentially attractive business possibilities which are accompanied by new risks to which there are no obvious solutions.

Social networking risks

Social networking is now commonly referred to as Web 2.0 technology. Whereas Web 1.0 technologies tended to involve business models that 'pushed' goods, services and information to prospective consumers, Web 2.0 technologies are based upon collaboration and information sharing.

Social networking has resulted in the emergence of a number of dedicated websites, most notably MySpace, FaceBook and Twitter. These sites invite visitors to share information, thoughts and ideas about themselves and issues of interest. Typical activities and facilities include:

- posting blogs;
- file sharing, information sharing and the exchange of videos and photographs;
- shared resources for user information and exchange;
- wikis – in the form of data and information resources;
- online communities for networking opportunities.

Social networking remains primarily at a 'social' level at present, but is surely likely to develop into a culture that embraces the commercial environment, where consumers who are accustomed to informal online information sharing and collaboration will expect commercial enterprises to adopt a similar approach.

Dennis Farm comments:

> Probably the most significant emerging risk is that posed by social media and networks. The development of wiki leaks, in particular, means that organisations' sensitive data can be posted on the Internet for all to see. One reason for this is the perception of young people, most of whom use social media routinely. They tend not to distinguish between personal and corporate, or commercial, information and often post derogatory remarks or allegations concerning employers.

As will be seen later, social networking presents a number of legal compliance and operational risks. As far as technology is concerned, the risks are no less critical.

The obvious risks surrounding this free exchange of information are:

- the opportunity for viruses to infiltrate systems and networks as communications are exchanged;
- the potential for insecure data to be transferred with the risk of loss, contamination or corruption;
- the assumption of false identities without any proper system of identity-checking procedures.

However, as social networking sites develop into communities with no regulation or supervision, it is unlikely to be long before other risks emerge. These could include:

- the transmission of bugs and general malware, leading to the creation of botnets;
- the cracking and reuse of passwords;

- the harvesting of e-mail addresses;
- data and information harvesting;
- spam e-mail marketing;
- the downloading of illegal software;
- wasted bandwidth.

Andrew Rose, Global IT Risk Manager at Clifford Chance, says:

> Once data is posted on the Internet, it is extremely difficult to ensure it is deleted and not replicated or promulgated without permission. Social media, such as blogs and informal networked communities, make this a particular problem.

This sentiment is echoed by Robert Jackson, Security and Infrastructure Consultant at Capgemini:

> Abuse of social networks can severely impact on the profitability of an organisation. It is very difficult to detect, for instance, defamatory content and commerce and industry has yet to get to grips with it.

At first glance, social networking sites may not appear to present a significant risk to business enterprises. However, in the absence of any sound policies governing access to such sites, organisations are likely to find personnel visiting them in business hours in the same way as they might send personal e-mail in the workplace. In such circumstances, any organisation may be exposed to many of the risks identified previously.

CHAPTER 3: LEGAL COMPLIANCE RISKS

Legal compliance risks arise from failure to comply with legislative, regulatory and codified (for example, professional and business codes of practice) provisions governing the supply of particular goods and services. Typical instances include infringement of: applicable laws and codes in foreign jurisdictions; domestic and foreign advertising regulations and codes of practice; provisions governing the handling of personal data; provisions relating to the protection of consumers; and general legal provisions, such as defamation or harassment. They are referred to as legal compliance risks because they arise primarily from infringement of the law.

Legal and compliance issues arise from the use of Internet technologies in the same way that they arise in the conduct of traditional commercial, business and professional activities. For instance, advertisements on websites must conform to regulations and advertising codes in the same way as advertisements which appear in publications or other media.

Legal and compliance issues range across a broad sweep of activities. For the purposes of this analysis, the following categories are identified:

- website management – addressing risks arising from the operation of an organisation's website;
- consumers and services – addressing risks arising from the use of Internet technologies to supply goods and services;

- jurisdiction and applicable law – addressing risks arising from the conduct of business in global markets;
- Internet abuse – arising from misuse of Internet technologies;
- monitoring and surveillance – addressing risks that arise for both employers and employees from the monitoring and surveillance of personnel in the workplace;
- Web 2.0 and social networking – addressing risks arising from abuse of this activity;
- Cloud Computing – addressing risks that arise from organisations using services hosted by suppliers over the Internet.

Website management

Two types of risk arise in the context of an organisation's management of its website: first, from the use of a domain name; and second, from the information posted on the website.

Domain names

Domain names (website addresses) uniquely identify an organisation's presence on the World Wide Web and should be instantly identifiable to consumers, stakeholders, suppliers and introducers alike. They represent a significant element of an organisation's goodwill.

Care should be taken to register a domain name precisely with a domain name registration agent. Even slight variations may cause confusion with other domain names of similar appearance or sound, potentially giving rise to proceedings over any infringement.

Once registered, the organisation must ensure it is renewed periodically and that changes are recorded appropriately.

In the past, the practice of 'cybersquatting' has arisen. This involves an organisation registering the brand name of another organisation as a domain name and then attempting to sell the domain name to the brand owner.

One of the earliest cases on this issue was *Marks & Spencer Plc v. One in a Million Ltd.: (1999) 1 WLR 903*; on appeal, *(1999) FSR 1 CA*. Its implications are discussed later. Other similar cases involving illegal or improper use of domain names, with slight variations, have arisen since.

The risk posed by this type of situation is the potential to significantly affect an organisation's trading name and goodwill. Risks also arise from failing to search thoroughly against a proposed domain name and failure to renew a registered domain name.

Website information

The quality of website content is a vital factor in drawing the attention of consumers to the site and, therefore, attracting new business. A website should promote the good name of the organisation; proactively offer information; and generate interest in the organisation's services. Ultimately, it should aim to become a valuable resource to which consumers and clients return repeatedly.

Most importantly, information and advice posted on any website must be timely, up to date and accurate because there must be a reasonable expectation that a visitor to the site may act upon it.

Various risks arise from the content of a website. A misleading or inaccurate statement may give rise to an action for deceit or proceedings under the Misrepresentation Act 1976 if a visitor acts upon the statement and suffers loss. Out-of-date, poor-quality or inadequate information may give rise to an action for negligence.

In the same way, if an organisation links its website to that of another organisation, an action might arise against both organisations in respect of inaccurate information if the claimant can prove loss.

Many websites contain disclaimers. These can be binding as long as they are brought early to the visitor's attention, but they are subject to a legal test of reasonableness and may be rejected by the courts.

One further issue is frequently overlooked in terms of website content. An important compliance issue is the need for websites to be accessible to the visually impaired under the provisions of equality legislation. Failure to comply may result in proceedings. Many organisations fail to reach minimum standards in this respect.

Website advertisements

Organisations both fund their marketing strategies and derive considerable income from website advertising.

However, Internet advertising creates a number of potential risks. Chief among these is the fact that online advertisements are globally accessible. While 'terrestrial' advertisements are governed by the law of the country in which they appear, global advertisements will appear in numerous countries and may, therefore, be subject to jurisdictions worldwide, so increasing the risk of contravening laws, regulations and professional or commercial codes of practice where advertising content is received.

Earlier, in the context of website information, the risk of liability arising from content on a linked site was considered. The same risk potentially arises in respect of advertising content too.

Domestically, criminal proceedings may also arise. Both the Trades Description Act 1968 and the Consumer Protection Act 1987 create offences for misleading statements of certain types.

Website copyright infringement

Copyright gives the owner or originator of material the legal right to prevent others from copying the material without permission.

Two risks arise in the context of information posted on websites:

- the unauthorised reproduction by another of material posted on the organisation's website;
- the posting of content on the organisation's website without permission of the creator and/or the website host.

UK copyright law is governed by the Copyright Designs and Patents Act 1988 and includes material posted on a website. Risks, therefore, arise from the reproduction of material on the organisation’s website; inadequate notice to website visitors regarding the organisation’s policy on the copyright of posted material; and failure to appropriately instruct personnel responsible for management of the copyright of website content.

Related to copyright infringement is the emerging practice of downloading copyright material in the form of (most commonly, music) files and distributing these illegally – known as illegal file-sharing. This is now governed by the Digital Economy Act 2010 (*see Chapter 9*).

Website compliance

The correct management of a website includes ensuring that it is operated in compliance with relevant statutory and regulatory provisions. This includes compliance with provisions governing the supply of information regarding the provision of services through websites.

Examples of these compliance procedures include the: Companies Act 2006 and the Provision of Services Regulations 2009, regarding the supply of information about an organisation offering services, both of which are considered in Chapter 9.

In addition, there is a duty on website owners to ensure that adequate provision is made for visually impaired users of a website. This was governed by the Disability Discrimination Act 1995, which is consolidated in the Equality Act 2010, also considered further in Chapter 9.

Consumers and services

Data management

Organisations handle vast quantities of confidential electronic data and are exposed to considerable risk because of the instantaneous, mercurial and pervasive manner in which information and data can be dispersed through Internet channels.

Internet technologies make personal data easy to distribute, transfer, retain and store. At the same time, errors in operating Internet technologies can result in loss, distortion, corruption or erroneous transfer of data. Improper management of data arises in the following forms:

- improper or unlawful processing;
- improper use of data;
- storage of inaccurate data;
- loss or damage to data;
- unauthorised transfer of data.

Internet technologies enable information to be easily transferred. International transfer of data has never been easier, but it is governed by strict provisions. All organisations should be familiar with the increasing amount of complex legislation surrounding data handling as well as various codes of practice and guidance issued by the ICO.

Breach of confidential information

Information which is widely available is no longer confidential – there is no control over those who have access to it. Internet technologies are inherently insecure and careful thought is required over their suitability for communicating private information.

The obligation to treat information confidentially can arise in a number of ways, for example:

- professional obligations through codes of practice and professional regulations; for example, in this respect solicitors are governed by the Solicitors' Code of Conduct 2007;
- the insertion of a confidentiality clause in a contract;
- the use of a non-disclosure agreement (NDA) in tendering documents;
- employer–employee relationships, where obligations of confidentiality are frequently imposed.

Breaches of confidentiality can easily arise through the use of Internet technologies. Casual use of e-mail can result in a confidential e-mail being sent to the wrong recipient(s). Unauthorised individuals may access confidential data which is not adequately protected. The trend towards information sharing and collaboration, as exemplified by Web 2.0 and social networking, offers numerous opportunities for data leakage.

Data leakage and breaches of confidentiality can result in criminal and civil proceedings, and reputational damage.

Negligent online advice

At law, a duty of care arises when providing advice to someone who may reasonably be expected to rely on it. E-mail, websites and extranets are Internet technologies which are all employed for the provision of information and advice. Employees may frequently have occasion to offer advice through these channels.

The risks surrounding the content of websites were considered earlier. The speed and informality of e-mail can result in information and advice being provided with insufficient consideration – and, in the case of employees behaving in this way, there follows the risk of an organisation being exposed to legal proceedings.

In complex transactions using extranet technologies, where teams of personnel with differing levels of expertise are engaged, there is a real danger of inexperienced personnel inadvertently giving incorrect advice and information.

In a similar way, informal communications through social networking sites can result in casually offered information and advice on which reliance is placed.

Online contracts

Yet another risk arising from the speed and informality of e-mail is the ability to form online contracts inadvertently. Inexperienced employees are especially vulnerable in this respect and run the risk of exceeding their authority and accidentally concluding a contract on behalf of an employer.

If the employee has ostensible or apparent authority to enter into a contract on behalf of an employer, the contract may be binding and the employer may be liable under the terms of the contract, regardless of whether the employee had actual authority.

Transactions

Risks can arise in the conduct of transactions and are a good illustration of how the traditional model of business activity sits uneasily with the Internet model.

It is perhaps best illustrated within the legal profession in which 'high-street' practices, in particular, offer traditional legal services, such as the preparation of wills and the administration of probate estates. Internet technologies now enable these services to be provided at a distance.

The question arises as to the conduct of these transactions. Are there any codes or regulations or consumer protection measures that apply to 'distance' contracts for goods and services? If so, what level of compliance is required and what risk management steps should be taken?

Jurisdiction and applicable laws

It is almost impossible to apply terrestrial laws reliably to an environment governed by Internet technologies. This problem is significantly compounded when considered in an international context, where individual countries jealously guard their jurisdictions.

As e-mail and website content can be read in virtually any country, there arises the potential for considerable confusion in providing services over the Internet because, in theory at least, each country receiving content may wish to claim exclusive jurisdictional control in the event of a dispute.

Given this confusion, the most likely method of resolution is to obtain some form of international agreement. Some organisations provide frameworks to govern certain aspects of the Internet. The World Intellectual Property Organisation (WIPO) and the Internet Corporation for Assigned Names and Numbers (ICANN), which administers the issue of domain names, are two examples of bodies supervising administrative issues 'consensually'. However, strictly speaking, there is no overarching authority.

Internet abuse

Defamation

The law of defamation applies equally to electronic communications in the same way as it does to any other 'traditional' paper-based communication. Defamation on the Internet is sometimes referred to as 'cyberlibel'.

Defamation is an untrue statement, published to a third party, that damages the reputation of a person, or persons or a corporate entity. Therefore, electronic defamation might occur through publication in an e-mail, on a website, on a bulletin board or newsgroup, or in a discussion group. Social networking sites are now an increasing source of Internet defamation, largely because of their informal nature.

There must be publication to a third party, but Internet technologies change traditional concepts and views of publication. For instance, screening of e-mails might give rise to publication. As liability can attach to publishers of a libel, an organisation might attract liability for statements made by employees acting within, or ostensibly within, the scope of their employment, or even through third-party statements appearing on its website.

When sending an e-mail, it is easy to slip into informality. In both internal and external e-mail, employees can overlook the legal validity of e-mail and make comments that would clearly be defamatory in a letter or fax.

Pornography

Internet technologies enable obscene material to be accessed and distributed in various ways and can facilitate obscene behaviour in the workplace. Typical examples are the publishing and distribution of indecent or obscene material via e-mail, or the display of indecent material downloaded from a website. E-mail is an example of the use of a public communications system on which it is a criminal offence to send an offensive, indecent of obscene message.

A development of this is the specific offence of possessing an indecent photograph or pseudo-photograph of a child, and there have been various high-profile cases, almost all involving the downloading or distribution of such material from the Internet

Harassment

Harassment is conduct of a nature which the victim finds unacceptable, unreasonable or offensive. It can include both verbal and physical behaviour and a single act can be sufficient. Sexual harassment might, for example, include direct harassment by e-mail or indirect conduct, such as downloading or distributing sexually explicit material.

In both instances, the most obvious source of offending is likely to arise through the careless or irresponsible use of e-mail. The informality of e-mail lends itself to the use of inappropriate and improper language and expression.

Offensive material copied from a website might also constitute commission of the offence in either case. A board of directors (in the form of a company) or partners in a firm might find themselves liable for an employee's conduct in this area, if it was within their control.

Once again, social networking sites are a potential source of this behaviour because of the informal nature of communications and the ready sharing of information and opinions.

Monitoring and surveillance

A number of statutory and regulatory provisions have been introduced to govern the status of secure communications passing over the Internet. These provisions attempt to balance the right to intercept secure communications for certain purposes, for example, the interests of national security, against the rights of individuals conferred by the European Convention on Human Rights.

Included in these provisions are rights for employers, in certain circumstances, to monitor employees in the workplace, including their use of e-mail and the Internet. The risks arising from the use of Internet technologies in the workplace are considered in the next chapter. However, these operational issues also give rise to legal obligations with which employers must comply.

These statutory provisions are examined in Chapter 9, but they introduce particular questions for consideration. First, there is the possibility that secure communications with clients and others may be the subject of an application for surrender and disclosure to the authorities, with implications for the confidentiality of professional and business relationships.

Second, while employers may have the right to monitor the use of Internet technologies in the workplace, there are limited grounds upon which they are entitled to do so. Taking action outside exemptions contained in the legislation will expose the employer to the risk of criminal prosecution.

Social networking

Potentially serious legal and compliance issues also arise from the casual use of social networking sites. Employers who use social networking sites as a source for recruiting people may be vulnerable to accusations of discrimination.

An employer may attempt to, or actually, obtain information and data about a potential employee's sexual or religious orientation through such sites. As well as offending against existing legislation, this also contravenes the Employment Practices Data Protection Code (*see Chapter 9*).

The exchange of confidential data by employees, within and beyond the organisation risks a breach of the DPA; and in certain circumstances, the employer and/or employee might be liable to criminal proceedings.

Furthermore, overfamiliarity between potential or even actual employees through the use of social networking sites can give rise to problems for both employer and employee. Much publicity has arisen from the practice of employees publishing derogatory remarks about their employers on such sites.

Recently, an employee was dismissed for publishing offensive remarks about her employer on such a site and in another case, some members of a transport service were dismissed for insulting remarks about passengers posted on a social networking site.

The development of social networking has given rise to the emergence of illegal file-sharing. This activity most frequently involves the downloading and distribution of music files, avoiding the required payment. Sometimes pornographic material is also involved. While this is an operational issue because it involves employees' behaviour, it is also illegal because it may infringe the Copyright Designs and Patents Act 1988 and the Digital Economy Act 2010, both considered in more detail in Chapter 9.

IT outsourcing risks

As well as technology risks, Cloud Computing also gives rise to a number of legal and compliance risks. These risks arise mainly from organisations failing to understand the scope and relevance of legal and regulatory provisions, including codes of practice and industry standards.

Probably the most prominent legal and compliance risks revolve around compliance with the DPA. Many of the issues involving compliance with this legislation run in tandem with the technology risks associated with Cloud Computing.

An organisation does not divest itself of responsibility or liability under the DPA by simply outsourcing the processing of its data to a supplier of such services. Responsibility and liability remain with the organisation at all times for the duration of the Cloud Computing project.

IT risks arising from the safe and proper handling and management of the organisation's data by a supplier also involve compliance issues under the DPA. Non-compliance with the DPA can result in the organisation facing criminal proceedings under the DPA, or civil proceedings for negligence taken out by a consumer for loss or damage to its data, as well as considerable reputational damage.

Penalties for non-compliance with the DPA have recently increased and the ICO has expressed an intention to give examples of serious non-compliance a significantly higher profile.

Therefore, situations involving loss or damage to data are not only serious risks to an organisation in the context of IT, they are also serious compliance issues because such situations will almost certainly have involved a failure, directly by the supplier and vicariously by the organisation, to take adequate steps to protect the security of the data concerned – a breach of one of the eight principles of the DPA.

Similar exposure to liability might arise in respect of the potential for contamination by viruses and other malware of data stored in close proximity to the data of other organisations in farms of virtualised servers.

The collection of vast amounts of data in remote servers, sometimes globally dispersed, raises another compliance issue. The DPA provides that data shall not be transferred beyond the EEC, unless there is clear and available evidence of adequate provisions for its safe and proper management in the recipient country.

CHAPTER 4: OPERATIONAL RISKS

Operational risks arise from failure to manage employees' use of Internet technologies adequately. Typical instances include: abuse of e-mail facilities through unauthorised use in the workplace; accessing and downloading inappropriate material from websites; failing to accept delegated responsibility for managing the organisation's website; and inadequate delivery of the organisation's electronic services. They are referred to as operational risks because they arise from some failure of the operational functions of the organisation, principally the failure to manage employees, so that they recognise and accept their responsibilities when using Internet technologies.

Operational risks arise from business practice. They concern employees' professional and business practice and conduct in the ordinary course of their work and their use of Internet technologies. Some risks arise from activities of employees which might simply be resolved as an internal disciplinary matter but which equally might expose the organisation to civil or criminal liability. The previous section identified the key legal compliance risks of which organisations need to be aware.

It is important to remember that categories of cyber risk overlap and a risk can fall into one or more categories. This applies particularly in respect of legal compliance risks, categorised as 'Internet abuse' in the previous section. While there are compliance issues for the organisation, and there may be proprietary technological solutions for their management, there are also operational risks arising from the conduct of the organisation's employees. Internet technologies offer considerable opportunity for employees to act without supervision. It is the issue of supervision that gives rise to potential employee misconduct.

There are various operational issues for organisations to consider and they are considered in the categories of:

- employee use of e-mail;
- employee use of the Internet;
- website management;
- delivery of electronic services;
- miscellaneous risks.

Employee use of e-mail

There is considerable scope for employees to use e-mail for their personal convenience. It is impractical to supervise e-mail in the way that traditional correspondence can be monitored, and in the absence of supervision, there are endless opportunities for employees to abuse e-mail. There have been a number of highly publicised cases – some involving law firms – where the improper use of e-mail resulted in professional embarrassment.

This problem also extends to the use of e-mail for business purposes. Here, the risks arise less from e-mail abuse, but rather from inappropriate behaviour arising from lack of management control. This absence of management can expose an organisation to risk in a number of ways. The inadvertent formation of online contracts, breaches of confidence through e-mail and the sending of spam e-mail have already been mentioned.

However, other risks are present. Receiving instructions by e-mail can be dangerous if received from a client by an unsupervised member of staff insufficiently skilled in providing the required services, or who fails to make the appropriate identity checks. Professional undertakings can be given by e-mail, binding the organisation to legal obligations. In law firms, other issues concern the use of e-mail for the issue, service and settlement of court proceedings. Lack of supervision and management in this area exposes a law firm to all manner of risks.

Security is another risk area. Employees can receive e-mail containing viruses, potentially exposing the organisation to liability for negligence. Viruses can be received which employees fail to detect because they fail to apply virus-checking procedures. E-mail can be sent to clients containing highly confidential issues and, through forgetfulness or laziness, employees may fail to employ security procedures.

E-mail notices can be a problem. To what extent should employees attach notices to e-mail? Should there be notices containing disclaimers warning against breach of copyright in respect of the content of the e-mail, warning of the possibilities of viruses, or reminding the recipient of the confidentiality of the e-mail and giving directions in the event of receipt by someone other than the person intended by the sender?

These are typical, but by no means exclusive, examples of the risks that can arise through employees using e-mail and the failure to implement adequate management and supervisory procedures.

Employee use of the Internet

Similar problems arise in respect of employees' use of the Internet. Without the assistance of technology, it is impossible physically to check websites that are visited. While technology now enables the monitoring of websites visited by employees, this raises the issues of monitoring and surveillance mentioned earlier.

How is an organisation to ensure that employees do not abuse the Internet in business hours by visiting inappropriate websites and viewing, downloading and distributing unsuitable material in the workplace? Other issues arise from personal use of the Internet in business hours.

Some sites have discussion groups, presenting opportunities for employees to take part during business hours and to post comments that might embarrass the organisation in some way. The Web 2.0 social networking environment simply adds to the potential risks in this area. Employees have ample opportunity to browse websites and lose valuable time, as well as making online purchases for personal purposes.

Here, the risks arise from employees who deliberately abuse the facilities that the Internet offers. They do so if they are able to, and when there is no management or control mechanism to enforce appropriate behaviour.

Website management

Proper management of the organisation's website is the responsibility of the Board and Partners, together with senior management, for its strategic success; and of personnel for its efficient operation and effective performance. Brochure sites present no significant risk because they generally contain static information of the sort that may be found in a traditional brochure.

However, websites offering advice and information present various opportunities for problems to arise. Many of these are discussed as legal compliance issues and they show how cyber risks span across the three categories. For instance, website content must be accurate and up to date, and advertisements must conform to regulations and codes. Employees must be aware of their responsibilities in this area. The organisation may choose to post disclaimers in respect of certain information on the site, or with regard to links with other sites. It is the responsibility of employees to ensure these disclaimers are accurate and relate to those sections of the website for which the organisation wishes to avoid exposing itself to liability.

In posting material on a website, employees must be aware of copyright issues and ensure that copyright notices are posted to protect information and advice that the organisation values. On the other hand, if, as a marketing strategy, the organisation is content for certain material to be copied, employees charged with managing the site should ensure that a notice to that effect appears on the site.

If the site collects personal data from visitors, there should be a notice on the website explaining how the data is to be used. In the same way as for other website notices, employees should understand their responsibilities and the criminal and civil risks to the organisation if these notices are not properly posted and updated to reflect the organisation's electronic services.

The risks to an organisation's website will lie in failure to comply with legal requirements, and also in the attitude and behaviour of employees charged with its management. They, therefore, become operational issues for the organisation.

Delivery of electronic services

The risks arising from the delivery of electronic services are similar to those arising from use of the organisation's website, but involve additional concerns because as well as providing advice and information, the organisation is undertaking certain activities.

Risks surrounding the formation of online contracts were discussed earlier. Concerns also arise where the organisation provides services with the support of a site to which it is linked. An example might be that of a financial services provider linked to the website of a lender, investment company or broker. Employees must understand how and to what extent liability might arise in connection with advice and information from linked sites.

Most organisations offering electronic services introduce systems for electronic payment. The technology issues to which payment systems give rise were discussed earlier. There are also operational issues. Employees involved in their use and responsible for their management must understand the implications. The system must be secure, with checking procedures to prevent fraudulent use.

These operational features require monitoring, so that as the organisation develops its service provision, the risks that arise are controlled and managed. This involves supervising and managing personnel associated with the activities and, therefore, becomes an operational issue.

Miscellaneous

The potential range of operational risk is significant because it arises from the conduct of employees and other personnel, such as independent contractors. This is often unpredictable – what may be an operational risk for one organisation may be irrelevant to another.

In addition to the categories above, particular risks arise from the behaviour of employees in a number of areas:

- **Phishing and social engineering:** employees may take the risk of responding to inappropriate e-mail, resulting in breaches of confidentiality or infiltration of malware.
- **Instant messaging and VoIP communications:** carelessness can result in the infiltration of malware.
- **Passwords:** carelessness can result in unauthorised individuals gaining access to corporate systems and networks.
- **Negligent management of data:** careless handling of data can result in breaches of confidential information, loss of data, reputational damage, and civil or criminal proceedings.
- **Negligent management of mobile technologies:** loss of mobile devices, such as a Blackberry, mobile phone or laptop computer, can result in breaches of confidential information, loss of data, reputational damage, and civil or even criminal proceedings.
- **Negligent management of storage devices:** loss of CD-ROMs or USB drives can result in breaches of confidential information, loss of data, reputational damage, and civil, or even criminal, proceedings.

- **Illegal file-sharing:** involving evasion of payment for copyright material, downloaded and distributed without permission, may result in legal proceedings.

The wide-ranging categories of Internet risk pose significant risk management problems. Frameworks for managing these risks are discussed in Part 2.

PART 2 – RISK MANAGEMENT STRATEGIES

CHAPTER 5: THE NEED FOR GOVERNANCE

In many respects, the identification of cyber risks is a relatively straightforward task. Almost all Internet risks spring from one or more of three sources:

- variable reliability and application of technology;
- uncertainty surrounding legal and regulatory compliance issues;
- problematic behaviour of personnel in employing and operating Internet technologies.

These types of concern tend not to arise so critically in traditional business and professional environments where procedures are well established, codes and protocols govern business and professional conduct, and models and channels for providing goods and services are conventional.

Internet technologies are disruptive. They introduce new models for the provision of goods and services based on a global platform and in an environment where communications are instantaneous, paper records are subsumed in digital content, and speed, efficiency and cost-effectiveness are paramount.

In such a challenging environment, risks abound and are not always easy to identify. In fact, the risks are so numerous, it is virtually impossible to assemble a comprehensive catalogue of Internet risks, not least because they differ from organisation to organisation – and what may be a risk for one concern may present no problem to another.

Strategy

The real challenge in addressing Internet risk lies in developing a strategy complemented by an appropriate framework for identifying, categorising and assessing it, and deploying responsibility and accountability for its containment and management.

The decision of an organisation to employ Internet technologies to achieve its goals, like any other strategy, is a decision for boards of directors, or partners in the case of a partnership. It is the task of boards and partners to set the strategy of an organisation.

Internet technologies and IT are now vital for the effective performance of any business or professional organisation. Without these technologies, organisations will almost certainly be unable to compete effectively in their respective markets and probably will be unable to survive.

Organisations rely on IT for:

- supporting supply and demand functions;
- streamlining business processes;
- developing and maintaining a global presence;
- supporting niche business and professional services;
- performing competitively in markets that involve instant and global communications;
- administering the operations of their personnel.

Given the critical importance of IT to any organisation, it is imperative that IT and Internet strategies are managed and administered competently and effectively. Internet and IT strategies that are misaligned with business goals and objectives; managed without forethought and planning; inadequately resourced with up-to-date IT; and assigned low priority at board level will almost certainly cause an organisation to underperform in terms of its competitors, to the extent that eventually it will fail in its chosen marketplace.

Critical to the efficient management and successful implementation of the strategy of any organisation is the need for the effective adoption of good governance principles. Essentially, governance represents the control of and regulation of an organisation that is reflected by good order and competent management.

For the purposes of considering Internet risk in the context of governance principles, there are three areas of governance to be addressed: corporate governance, IT governance and project governance.

Corporate governance

At either board or partnership level, corporate governance is defined by certain well-recognised categories of management conduct:

- clearly defined roles of line-management responsibility and accountability throughout the organisation;
- transparent decision making at all levels throughout the organisation;
- the taking into account of the interests of shareholders and other stakeholders, such as employees, suppliers, creditors and business referral sources;
- addressing risk issues confronting the organisation, including legal and regulatory compliance and information security.

The range and categories of Internet risk discussed in the previous chapters are quite clearly strategic risks. Even those risks that are categorised as arising in an operational context have significant strategic implications.

In the context of IT risks, failure to encrypt e-mail may result in breaches of confidential data, which may in turn affect the organisation's reputation.

In the context of legal and compliance risks, failure to comply with the DPA may result in the prosecution and conviction of an organisation and its employees.

In the context of operational risk, the circulation of obscene material on an employer's e-mail system may also result in prosecution of an organisation and its employees.

Each of these three examples offers the potential for an organisation's reputation to be significantly damaged in a global market.

Managing Internet risk, therefore, clearly involves making strategic decisions at board or partner level. In any organisation, the responsibility for identification, development and execution of a strategy lies with the Board or Partnership. It is at that level that the nature, scope and oversight of the implementation of a strategy are decided.

Internet risks can be highly complex. They frequently require an understanding and knowledge of complicated IT and obscure legal and regulatory provisions. The consequences for any mismanagement can be significant and may affect the very existence of the organisation.

The primary statutory framework governing corporate bodies is the Companies Act 2006, which consolidates and adds to previous legislation. Sections 171–177 govern directors' duties and may be summarised as:

- acting within their powers;
- promoting the success of the company;
- exercising reasonable judgement;
- exercising reasonable care and diligence;
- avoiding conflict of interest;
- declining benefits from third parties;
- declaring any interest in transactions and arrangements.

The primary non-statutory framework governing corporate bodies is the Combined Code on Corporate Governance 2008, which provides a framework within which directors are able to develop and improve an organisation's performance by addressing the interests of shareholders and which refers to the governance criteria discussed earlier.

Companies listed on the Alternative Investment Market (AIM) in the UK are subject to Corporate Governance Guidelines for AIM Companies 2007, published by the Quoted Companies Alliance and designed to help organisations develop frameworks that accommodate corporate governance principles.

IT governance

The principles of IT governance are a subset of corporate governance principles. They introduce a framework of leadership, structure, business processes, standards and compliance requirements designed to ensure that an IT strategy supports, and remains aligned with, an organisation's objectives.

IT governance frameworks are supported by various tools in the form of methodologies, standards and compliance legislation. It is often mistakenly believed that these 'supports' are IT governance. They are not. They are the tools by, and with, which IT governance principles are implemented.

IT governance is a framework that defines the management infrastructure, organisational procedures and compliance requirements, including lines of responsibility, accountability and transparency, and decision-making processes at the various levels of the organisation, all of which operate in the context of IT achieving an organisation's business objectives.

Although IT governance may be implemented at operational level, its substance and direction, or oversight, are a matter for the Board or Partners. Directing strategy is a board and partnership function for ensuring that an IT strategy remains aligned with organisational goals and is likewise a strategic issue.

Why should an organisation adopt IT governance principles? There are a number of important reasons:

- the need to support corporate governance principles;
- the need for a management framework to protect confidential data;
- the need for a framework to manage IT risk – of which the range and categories of Internet risk are typical examples;
- the need to develop a competitive edge by effective execution of the Board's or Partners' strategy.

IT governance frameworks

Alan Calder[1] suggests that designing an IT governance framework involves eight key decision areas:

1 IT governance principles and decision-making hierarchy.
2 An information strategy derived from the business strategy.
3 IT risk management in the context of the organisation's overall risk management framework.
4 Software applications – how business applications are developed, authorised, acquired and managed.
5 Information and communications technology (ICT) architecture (integration and standardisation) to meet the requirements of the information and applications strategy.
6 ICT infrastructure/technology – how IT services are specified, developed, authorised, acquired and managed – what services should be outsourced, why and to whom.
7 ICT investment and project governance – given the IT strategy, which IT initiatives (including outsourcing initiatives) should be implemented and how they should be managed.
8 Information compliance and security – the criteria for securing information and achieving legal/regulatory compliance.

In the case of a company, Calder suggests this comprises:

- a board steering committee comprising key board members and executives, including the chief executive officer, the chief finance officer and the chief compliance officer – and the functions of which would

[1] *IT Governance Guidelines for Directors*, Calder A, IT Governance (2005).

be oversight of the organisation's whole IT operations, with project governance (of which Internet risk management is a typical example) singled out as a particularly important area for board oversight and monitoring;

- an executive committee comprising appropriate business managers, including a chief information officer to ensure cost-effective implementation of the Board's strategy – and the functions of which would be to exercise powers of delegation to appropriate levels;
- a technology committee comprising IT personnel and business managers with appropriate theoretical and practical skills.

Various views are advanced for the formation and composition of a governance framework. Much depends on the nature of the organisation's IT infrastructure and function, current IT projects and the availability of suitable personnel. A single model framework is unlikely to be sufficiently comprehensive to suit all organisations.

Some general principles that emerge as issues to be addressed within IT governance frameworks include:

- IT and business strategies;
- risk and compliance strategies;
- implementation and performance strategies;
- monitoring, reporting and auditing processes;
- value delivery;
- resource allocation.

The frameworks generally advocated for implementation consist of:

- a board of directors (or partners) to identify, set and drive the strategy;
- a management board to ensure implementation and compliance;
- a technology board to bring expertise where required;
- an operational board to address implementation;
- a project team to progress and manage projects;
- a programme management team to manage the organisation's portfolio of current IT projects.

These frameworks can be applied equally to partnerships. Most medium-sized and large partnerships in many ways now resemble large corporate bodies and delegate the operational direction of strategic partnership decisions to partnership committees.

Partnerships of any size usually assign specific management functions to specific partners and it is common for there to be a managing partner, a risk partner and a finance partner although, curiously, 'information security' partners are rare.

Nonetheless, with thought and planning, there is no reason why the IT governance issues and framework composition described above cannot be implemented by partnerships, with the support of consultancy expertise where required.

Project failure

The management of Internet risk is a vital project to which the principles of IT governance should be applied. The risks identified in the previous chapters permeate through the IT, legal and compliance, and operational functions of every organisation. Effective management of these risks is vital to the survival of most organisations, if not commercially then certainly professionally.

Various reasons are commonly advanced for the failure of IT projects. They are:

- uncoordinated and misaligned processes;
- poor relationships between personnel and teams managing and implementing the project;
- inadequate skills and experience;
- inadequate resources.

In the same way as some organisations, particularly professional bodies, express little enthusiasm for IT, there is also a frequent misunderstanding of IT governance principles.

The management of Internet risk is subject to project failure in just the same way as any other IT project and the implementation of an IT governance framework should be a priority. However, a governance framework is unlikely to succeed without appropriate tools – standards and methodologies – to support its implementation.

Governance framework tools

Certain standards and methodologies have been developed to address the need for a systematic and methodical approach to developing an IT governance framework and the application of IT governance principles. In the context of Internet risk, they establish principles by which an organisation develops, implements, manages, controls, monitors, audits and reviews an Internet risk project.

COBIT

COBIT (Control Objectives for Information and related Technology) is a standard for best practice and is essentially an IT governance control framework to maximise investment in IT and provide controls.

COBIT's fundamental premise is that the framework helps to ensure that IT strategies and projects remain aligned with business requirements. It helps to achieve this by suggesting management controls and resources and combining them into an identifiable model for application to strategies and projects. Further details of this methodology can be found at *www.isaca.org/cobit*.

BS ISO/IEC 38500:2008

An IT governance framework, such as that described above, can be complemented by certification of the organisation under BS ISO/IEC 38500:2008, the international standard for corporate governance of information technology.

The standard offers guidance to directors of organisations on the most effective use of IT and is designed to give confidence to stakeholders of all descriptions in an organisation's application of corporate governance principles in IT.

One of the key benefits is the ability to manage risk more effectively because the standard provides a framework within which to help directors and senior management to address legal and ethical responsibilities.

The standard applies to the governance of management processes (and decisions) relating to the information and communication services used by an organisation. These processes could be controlled by IT specialists within the organisation or external service providers, or by business units within the organisation.

The purpose of this standard is to promote effective, efficient and acceptable use of IT in all organisations by:

- assuring stakeholders that, if the standard is followed, they can have confidence in the organisation's corporate governance of IT;
- informing and guiding directors in governing the use of IT in their organisation;
- providing a basis for objective evaluation of the corporate governance of IT.

The standard provides guidance to senior managers; members of groups monitoring the resources within the organisation; external business or technical specialists, such as legal or accounting; specialists, retail associations or professional bodies; vendors of hardware, software, communications and other IT products; internal and external service providers (including consultants); and IT auditors.[2] The standard identifies six principles requiring:

- assumption of responsibility for IT;
- recognition of the strategic importance of IT;
- the rational acquisition of IT;
- the capable performance of IT;
- IT's compliance with legislation;
- appropriate IT policies.

[2] Permission to reproduce from the BSI website is granted by BSI (*see footnote on page 155*).

How might the six principles contained in the standard be applied to managing Internet risk? It must be remembered that the governance role of the Board or Partners is to set the strategy, establish and oversee lines of responsibility and accountability, ensure transparency, have regard to stakeholder interests and adopt an appropriate risk management strategy to include compliance and information security. Below are suggested some general applications for each principle.

Responsibility: the Board or Partners must recognise the importance of Internet technologies in providing the organisation's services and that managing the risks associated with Internet technologies is an essential element of this responsibility.

Strategy: the Board or Partners determine and set the organisation's Internet strategy in terms of the IT to be employed, the resources to be made available for its implementation and the resources in terms of finance and personnel to be directed at implementing a risk management strategy.

Acquisition: the Board or Partners must base their decisions on a clear analysis of the advantages and disadvantages, together with the risks and associated costs.

In this context, the Board and Partners should consider, for example:

- the business case, including the risks of using Internet technologies for providing services;
- the operational case, including the risks of using Internet technologies;
- the IT implications and the need to devote additional IT resources to manage Internet risks;

- the financial implications of an Internet risk management strategy, particularly the cost of deploying new IT and possibly recruiting new personnel.

Performance: the Board or Partners must decide how the use of Internet technologies and the management of risks associated with them will provide the required services and, at the same time, satisfy the needs of shareholders and stakeholders. Examples of particular considerations might be:

- the suitability of the organisation's existing Internet technology for the provision of its present and future services;
- the skills and capabilities of the organisation's current personnel for maintaining and improving service levels;
- the need for, and the cost of, additional resources for developing and maintaining an Internet technology risk management strategy;
- the extent to which the development and implementation of such a strategy will impact on the overall performance of the organisation;
- the need for a management structure or framework dedicated to the management of Internet risk and compliance.

Conformance: the Board or Partners must assess the implications of using Internet technologies for the provision of services in the context of legal and regulatory compliance.

For example, the Board or Partners should examine:

- the implications of compliance with the DPA;

- the implications of compliance with the provisions governing employee use of e-mail and accessing the World Wide Web in the workplace;
- the implications of complying with industry, trade or professional codes of practice.

It is the responsibility of the Board or Partners to establish the full extent of the organisation's exposure to liability for non-compliance. The Board or Partners should, therefore, promulgate policies and procedures addressing compliance issues among all personnel at all levels.

Human behaviour: it is widely recognised that in the context of information security, the great majority of incidents (some commentators have suggested as many as 70%) arise from human error. It is the responsibility of the Board or Partners to ensure that personnel are trained to understand their responsibilities.

This is a key principle of corporate governance which begins with the Board's or Partners' responsibility to establish clearly defined lines of accountability and responsibility throughout the organisation.

The Board or Partners should promulgate suitable policies and procedures to be observed, for instance, in respect of the use of e-mail, the handling of confidential data, or engaging in social networking sites.

COSO

COSO (*www.coso.org*) is a committee of sponsoring organisations, created in 1985 from a number of influential finance, auditing and accounting organisations with the objectives of identifying key causes of fraudulent financial reporting and making recommendations for its prevention through internal controls. The COSO framework is set out in the report: *Control – Integrated Framework 1992*.

Internal controls are measures introduced by a board of directors or partnership designed to provide confidence in an organisation's operations, financial reporting and legal and regulatory compliance.

Internal controls are described simply as processes (not documents) that provide reasonable assurance that the organisation's projects are aligned with its business goals.

COSO has been linked with Section 404 of the Sarbanes–Oxley Act 2002, requiring management to reveal any financial weaknesses that may raise questions over an organisation's assurance of the adequacy of its financial controls, where vulnerabilities have been disclosed.

It is important to understand that certification and implementation of methodologies are not IT governance, although they may be evidence of this. IT governance is the framework of leadership, organisational infrastructure and business processes. Standards and methodologies are tools employed in implementing an IT governance framework.

The principles of corporate governance are extended by the concept of IT governance and its various tools and methodologies which establish a framework for the implementation of any IT strategies introduced by the Directors or Partners.

Project governance

The management of Internet risk is a project in the same way that any other activity of an organisation is a project.

More precisely, the management of Internet risk is a series of connected projects.

For instance, the implementation of organisation-wide encryption of e-mail, perhaps internally, and externally with preferred clients or strategic allies, is a project. Development of a website through which financial transactions can be concluded is another project. A third project might be organisation-wide deployment of a business continuity and disaster recovery plan.

Internet risk management involves a series of individual projects which may or may not be related. However, if Internet risk is to be managed effectively, the series of projects undertaken by an organisation should amount to a co-ordinated, organised and logical set of projects. This is often referred to as programme portfolio management.

Definition

It is difficult to find a comprehensive, universally accepted definition of the word 'project'. Essentially, a project is a task to which are usually attached specific time limits and objectives and which is usually performed by a team with the appropriate skills for achieving its objectives.

In the case of Internet risk, whatever the nature of the individual project, there will almost certainly be:

- time criticality;
- the need for a team;
- the need for skills, for example in the areas of IT and legal and compliance issues.

Governance

Like corporate governance and IT governance, project governance is a framework for the delivery and achievement of a project's objectives through application of the governance principles of transparency, responsibility, accountability, compliance and risk management.

Implementation involves securing and managing the required resources, adapting to change, and monitoring and auditing performance. In the governance hierarchy, project governance sits below corporate governance, alongside IT governance, and above project management.

Objectives

The objectives of a project governance framework are to:

- keep the project aligned with the strategic objectives of the organisation for its duration;
- provide a continual auditing of resources against cost;
- deploy resources, so that the project provides maximum value and benefit to the organisation;
- provide a formal and structured approach to risk management;
- apply recognised best practice project management methodologies.

Features

Project governance features are based on the same principles as corporate governance and IT governance: responsibility, accountability and transparency, and in many respects project governance features mirror them.

The key features of a project governance framework are:

- leadership and commitment from the Board or Partners;
- a clear management, executive, operational and administrative committee structure for approval, monitoring and audit processes, including if necessary a specific risk management committee;
- within the committee infrastructure, the assignment of clear line-management responsibility and accountability at all levels with defined timescales and goals;
- within, above and below the committee infrastructure, the establishment of clear communication channels;
- specified objectives communicated to all stakeholders, including customers and clients;
- defined project procedures and processes aligned with measurable business objectives and IT infrastructures designed for realising a return on investment;
- adoption of recognised project management methodologies;
- dedication of adequate and relevant resources;
- provision for independent monitoring and reporting.

Because the potential for project failure is so significant, every project should possess certain characteristics such as:

- effective sponsorship;
- clear objectives;
- skilled and competent team members;
- recognised methodologies;
- lines of responsibility and accountability;
- awareness of stakeholder interest;
- analysis of the organisation's existing portfolio of projects.

Project governance tools

Project governance methodology is the process of applying governance principles to the management of a project in order to maximise the chance of the project fulfilling its business objective. Methodologies support project governance; they are not, in themselves a governance framework. They are aids to implementing project governance principles.

PRINCE2

The most widely applied project methodology is PRINCE (Projects in Controlled Environments *www.prince2.com*). The most recent version, PRINCE2, was published in June 2009.[3] It is a process-based standard used widely by the UK government for providing best practice guidance on project management.

It introduces seven key themes of project management that focus on the business case, the organisation, planning, project risk, progress monitoring, quality control, and issues and changes.

The processes that support these themes are starting projects, directing projects, initiating projects, controlling stages, managing stage boundaries and closing projects.

The methodology addresses the importance of the business environment and identifies and considers the essential roles required for managing a project, supported by process-based checklists.

[3] See, for instance, *Managing and Successfully Directing Projects with PRINCE2 TM*, Murray A, Outperform, © TSO 2009, © PRINCE2 2009, Overview Brochure.

PRINCE2 can be adopted for all types of project, large or small, although a small project may not justify adoption of each aspect, in which event the organisation can implement only the relevant features of the methodology.

BS 6079:2002

BS 6079:2002[4] is the current standard of certification for project management and provides guidance for various personnel on the techniques of planning, managing and implementing projects. BS 6079-1:2002 provides guidance on compliance with the standard. Work has begun on an international standard, ISO21500.

PPM

PPM is the integrated management of a portfolio of projects designed to deliver strategic business benefit.

PPM organises projects so as to enable an organisation to ensure it adopts a mix of projects which is consistent with business objectives. This ensures the organisation's overall project strategy and selection is tailored to its needs and remains aligned with corporate obligations.

The benefits of PPM are significant. Effective PPM offers flexibility in terms of an organisation's response to market forces. A wider range of solutions becomes available and can be more appropriately assessed. PPM enables an organisation to weigh up and compare issues such as risk, cost, investment and commitment of resources, and to

[4] Permission to reproduce from the BSI website is granted by BSI (*see footnote on page 155*).

prioritise them appropriately across a range of selected projects.

PPM is organised and conducted by a programme management office (PMO), which provides guidance in respect of, for instance, the suitability of projects for inclusion in a portfolio, risk profiles, availability of personnel and resources.

An organisation embarking on a comprehensive Internet risk management project should consider the introduction of a PPM process in order to maintain control of the varied, sometimes complex, and sometimes interconnected mix of risks to which Internet technologies give rise.

Val IT 2.0

Val IT 2.0 is a governance framework and is concerned with the management of an organisation's portfolio of investment in projects so as to ensure an adequate return on investment for the organisation.

In essence, the principles of Val IT 2.0 address the need to manage investments in IT in a prescribed way, defining them in categories, tracking their performance, ensuring that stakeholder interests are recognised and assigning lines of accountability during the life of the investment.

In the case of Internet risk, an example of a useful application of this methodology might be the introduction of an e-mail encryption strategy. This technology remains relatively underdeveloped and is not widely used. An organisation might employ the methodology to decide whether or not embarking on such a course might, or might not provide an adequate return on investment in the long run.

Val IT is explained in a series of white papers published by the IT Governance Institute (*www.itgi.org*), which set out the various management practices to be adopted in the areas of value governance, portfolio management and investment management. Ultimately, the Board of Directors or Partners are responsible and accountable to stakeholders in the organisation to ensure that business investments and resources deliver adequate business value.

Risk

A key component for the effective and successful application of corporate, IT and project governance principles is a methodical and comprehensive assessment and management of risk. No matter how conscientiously governance principles are applied, unless the Board or Partners conduct an analysis of the risks attendant upon an Internet technology strategy, there is not only considerable scope for strategic and operational project failure but, worse, the potential for civil or even criminal proceedings.

A key development in the management of Internet risk is the code of practice, BS 31100:2008, for risk management, which provides recommendations for the framework, process and implementation of a risk management strategy.

The principles of risk assessment are addressed in the next chapter and principles for the management of Internet risk are addressed in Chapter 7.

CHAPTER 6: ASSESSING RISK

Effectively managing cyber risks requires an understanding of how to assess the impact of risk. A strategy for the management of a risk should correspond with the nature and degree of the risk to be addressed. Risk assessment tries to identify and anticipate possible events. Effective risk assessment offers an organisation the opportunity to take greater control of its internal and external environment. Instead of reacting to events, the organisation with an effective risk assessment and management strategy can plan and direct its actions with greater confidence that it will not be undermined by unforeseen events.

Risk assessment involves certain processes. The first is to identify the risks associated with a particular activity or strategy. Technological, legal compliance and operational risks were identified in earlier chapters. The next process is to assess and evaluate the potential impact of a particular risk on the organisation. This chapter is concerned with that process. The third process involves implementing appropriate steps to either eliminate the risk or reduce it to an acceptable level, namely risk management, which is considered in Chapter 7.

Fundamentally, risk assessment is no different from any other form of assessment, involving the same processes of planning, and evaluation. Business professionals, such as lawyers, accountants, surveyors and financial advisers are always involved in this process when acting upon clients' instructions. By their nature and training, professionals are naturally cautious and, therefore, risk averse. In their own businesses, the traditional concept of risk assessment is predominantly associated with strategies for the avoidance of professional errors and omissions.

A management strategy cannot always eliminate risk and sometimes the strategy must be limited to reducing risk, so that the consequences are manageable. This is especially so in respect of Internet technologies where, for example, placing advertising material on a website, which is accessible globally, risks infringing regulations in foreign countries and exposes organisation to risks of a global nature.

Risk concepts

Broadly, risk may be regarded as any matter that might jeopardise a business's accomplishment of its objectives. There are different types of risk. Strategic risks concern the overall direction of an organisation and frequently arise from its position in the wider business environment. In terms of Internet technologies, the decision to deploy a website will be a strategic decision – it concerns the future competitive position of the organisation.

Operational risks involve the functioning of an organisation. If a website is deployed, thought must be given to appropriate content. Management of the content is an operational issue. If inaccurate content is posted, the ability of the organisation to offer its services could be prejudiced.

Cyber risks introduce a confusing blend of strategic and operational risks. Collecting data through a website for the purposes of marketing an organisation more effectively to clients and visitors is a strategic decision because it is concerned with gaining competitive advantage in the marketplace. However, the proper handling of any data collected is an operational issue involving the internal compliance functions of the organisation. If data is handled incorrectly, risk of prosecution or an action for damages arises and the business operation might be prejudiced. In this instance, there are, therefore, strategic and operational risks arising from a single issue, the collection of data.

There are different types of risk. Pure risks can result only in losses. Speculative risks involve potential benefits and disadvantages. Some risks have clearly foreseeable consequences. Others have only possible consequences. The risks with clearly foreseeable consequences are easier to manage. They can be avoided altogether or strategies can be devised for management of the consequences.

Speculative risks with possible, variable, or ill-defined consequences present greater difficulty. For the most part, this type of risk arises in the use of Internet technologies, partly because the technologies are developing rapidly and partly because the extent of their use is potentially global.

For example, what might be the consequences of collecting personal data through a website? The consequences might be an increase in volume of business as consumer relationships develop, or a prosecution for infringing the provisions of the DPA. In assessing and managing cyber risks, frequently the only strategy is to take and accept some risk, reduced as far as possible by careful planning in the hope that the business strategy succeeds.

Risk is not always obvious and can emerge quite unexpectedly. It does not necessarily appear as an identifiable threat. This is especially true of external risk where organisations are dependent upon an environment wholly outside their control. Risk might arise from failing to recognise the need to adopt a relevant strategy in a changing market – particularly relevant in the case of Internet technologies. Failure to employ adequate security measures may be regarded by clients and strategic allies as poor service and result in loss of competitive advantage and business opportunity. Internal risk can arise just as unexpectedly in the form of the unpredictable behaviour of staff. Risk appears in a variety of guises. It is impossible to confine its incidence to particular events or situations.

Risks can impact at all levels and will differ according to the size and nature of the organisation. Small organisations are more likely to be at risk from events threatening their future survival. Larger organisations may be at risk from factors arising from their sheer size and the intricacy of their organisational processes. In order to understand whether and, if so, how an organisation faces risk in respect of a particular activity, it is helpful to ask certain questions:

- What is the worst that could happen?
- How likely is it to happen?
- Are procedures in place to stop it happening?

Risk can also be confused with a number of other situations which are not truly risks. These might arise in two instances. First, the perception of risk can, and often does, differ from individual to individual. For a business manager, an information technology project represents a major opportunity. For the information systems project manager, however, it may involve major risks. Risk assessment determines the difference between the real and the perceived risk. Therefore, there is a need to create a commonly understood perception of risk.

Second, potential confusion lies in the analysis of problems as opposed to risk. Every organisation faces problems.

Risks are potential problems. In trying to understand what is a risk and, therefore, requires analysis, and what is a problem masquerading as a perceived risk, perhaps requiring a different approach, the manager or the individual charged with the assessment needs to be clear that it is the impact of a future set of circumstances that is to be addressed.

Risk will affect an organisation adversely in two ways: either impacting upon the day-to-day performance of the organisation's function; or, more seriously, impacting upon business continuity. An example of a risk affecting the efficiency of the organisation is the failure to plan and adequately manage Internet technology systems to ensure quality of performance. Examples of risks threatening business continuity are virus intrusion, 'hacking' activities, or 'denial-of-service' incidents preventing the organisation from providing an electronic service.

Approaching risk assessment

The first step in assessing risk is to identify any risk that might arise from a particular strategy as accurately as possible. This is familiar territory for professionals accustomed to identifying risk on behalf of their clients; distinguishing one or more courses of action open to a client and suggesting the advantages and disadvantages of each, then offering advice on the most appropriate course of action.

The same principles can be applied in the case of cyber risks. Consider the strategy that the organisation wishes to pursue, such as allowing limited client access to check the progress of instructions online, and then list the potential risks – the most obvious being that a third party may inadvertently gain access to this confidential information. Every organisation will identify different risks because every organisation is different. In many cases, risks will be specific to the particular activity proposed and the manner in which the firm proposes to undertake it.

Once a risk is identified, its impact will need to be assessed. This process involves identifying the business assets and assessing the impact on the organisation if the perceived risk should materialise.

In terms of cyber risks, 'business assets' are the organisation's reputation and the goodwill of its clients. Risks will be any consequences of the proposed activity that has an adverse impact on the business assets, for instance the interception of insecure confidential e-mail. The impact will be the immediate and future loss, including any action taken by the client as a result.

There are different methods for performing a risk assessment. It might be calculated in terms of a mathematical formula as an estimation of the likelihood of a risk materialising. Another approach might be to conduct an analysis of its likelihood based on decisions in the light of particular circumstances. A third approach might be to take a calculated risk based upon convenience or practicality.

Some examples might help to explain this suggestion. In respect of the first approach, for an assessment of whether there might be any real risk of staff using Internet technologies to harass fellow employees in a small organisation with trusted and long-serving personnel, a simple mathematical formula, such as a score of 1–10 might be applied.

In the second approach, a decision-based assessment may be required regarding, say, the risk of infringement of foreign advertising codes in placing advertising material on a website. The decision might be taken to proceed provided a statement on the site makes it clear that the advertisement is directed at United Kingdom viewers of the website only.

In the third approach, a calculated risk might be required to incur the expense of security technology that would allow clients to access the organisation's systems, in the hope that this would generate an improved client relationship and enhance the organisation's reputation, although at the same time exposing the firm to the potential danger of unwanted access by unauthorised third parties.

Risk assessment also involves other features. For example, there will always be a human element in assessing risk, in the decision-making process and even in the risk itself. Most of the operational risks considered earlier concern the conduct of staff in the workplace.

It is important to adopt the right approach to personnel. Management that is seen by subordinates as divisive or indecisive is unlikely to gain their support and commitment and is, therefore, far more likely to be exposed to risk than an efficient committed team.

In the same way, a management team that lacks adequate technical and business expertise is unlikely to show adequate ability in assessing the risks arising from a project involving skills beyond its capabilities. An individual whose experience of information technology is severely limited can hardly be expected to be at the forefront of the implementation of an IT security strategy.

A poorly performing management team is unlikely to gain the competitive advantage that a properly thought out risk assessment strategy can offer. In these situations, the danger is that an irresolute or incompetent approach to the project will result in the organisation continuing to remain exposed to risk.

Objectives and benefits

The objective of risk assessment is to balance the potential benefits against the potential risks of a proposed course of action, enabling a decision to be made on whether the action is justified. Properly assessing risk helps to provide time, information and a degree of control that will assist in more effective decision making.

The assessment needs to be as accurate as possible in order to develop a framework to manage it most effectively. A risk strategy aims to accept risk and manage it in a way that is acceptable to the organisation.

A risk assessment will have particular objectives. First, there is the need to assess all aspects of the risk, so that it can be minimised.

Second, it provides the ability to investigate whether the risk can be managed by transferring the responsibility for its management, for instance by outsourcing some or all of the organisation's IT function.

A third objective is to assess the degree of a particular risk with a view to its elimination. A risk that is eliminated does not require any subsequent management.

Other more direct benefits include:

- improved understanding of risks and their impact;

- more appropriate business response strategies;
- more accurate risk/cost calculations;
- identification of business opportunities;
- development of an organisation-wide approach to risks;
- enabling an organisation to develop 'know-how' in risk management;
- identification of a wide range of internal and external risks, which may be categorised for future reference.

In order to understand how these benefits might apply in terms of Internet technologies, a useful exercise is to apply them to a specific strategy, for example a proposal to provide encrypted e-mail facilities for a large commercial client for the completion of a complex project. Mapping the benefits listed above across the proposed strategy, the following benefits emerge:

- Discussion of the strategy with the client will clarify requirements and expectations and improve the quality of the service.
- Consultation will take place with the client on the steps required to implement the strategy, to agree any contingency plans and to explain any exceptional costs that may be incurred.
- The consultation process encourages both parties to develop procedures for handling e-mail that will minimise exposure to risk and maximise the efficiency with which e-mail is employed.
- A feature which was once a threat becomes an opportunity for collaboration and, therefore, a business opportunity.

- As confidence is generated, other ideas emerge for the use of secure communications technology on other projects, or in other ways.
- Valuable information is obtained about the client's potential requirements so developing the organisation's knowledge base.
- Mutual discussion ensures that all aspects of the risk assessment are considered for future occasions.

This analysis shows that if approached on the basis of collaboration and dialogue, in addition to a proper assessment of risk, a valuable marketing opportunity presents itself as well as the ability to enhance the reputation and goodwill of the practice.

The risk assessment

Effective risk assessment requires sufficient information to be available to enable an informed assessment to be made for successfully managing the risk. There must be an effective mechanism for collecting information. There are three useful approaches that can be adopted, which may be employed exclusively or in conjunction with each other, according to preferences and the needs of the organisation.

Collecting information

One approach is to interview key personnel to identify the particular issues that might arise. These personnel will be those most closely concerned with eventual management and control of the risk in question. Returning to the example of collecting personal data from a website for marketing purposes, there may need to be consultation with those responsible for ensuring compliance with the DPA and individuals in the firm's IT department responsible for ensuring that any data received is securely stored in the organisation's system.

A second strategy is to circulate questionnaires directed to key personnel. This can be valuable where the organisation wishes to establish whether there are common concerns over particular risk issues.

Third, workshops or focus groups for key personnel can also be employed to receive and develop ideas for managing identified risks.

Once adequate information is received, it can be recorded in a standard format, which includes a measurement of the greatest risks. It is important to ensure that information is obtained from appropriate sources. Risks which may be regarded as strategic – for instance, those arising from marketing activities through the firm's website – will require information from those responsible for strategic issues. These will usually be at senior management (board or partnership) level, even though implementation may be at a lower level. Risks that are essentially technology based in nature, for instance the threat of virus infiltration and the need to deploy anti-virus software, will require information from those with technological knowledge.

Consideration should also be given to the quality of information collected. It is important to obtain a full perspective of the risk when seeking information. Some individuals' perspectives will be more valuable than others. Often, the most valuable information is obtained from junior or support staff charged with implementing the policies of senior management.

The risk control plan

A logical approach to recording the findings of a risk assessment is to develop a risk control plan, which will specify responsibility and accountability and the nature and impact of the measures and controls to be applied. It is a mechanism for identifying and rating, or evaluating, the risk and then deciding upon suitable preventative or corrective action.

Once the risk assessment is complete, formulation of a risk control plan should not be difficult. Information identifying the risk and the circumstances of its incidence will have been obtained and can be recorded A checklist can be used, although this will need periodic review to take account of new risks arising from new services provided by the organisation.

The next step is to 'rate' or evaluate the significance or importance of the risk – how likely is it to happen? Rating risk means deciding the likely consequence to all aspects of the organisation. This will involve profiling each risk and its interrelationship with any other functions of organisation. Obviously, the greater the threat posed by the risk, the greater should be the priority accorded to it in terms of resources.

The final step is to determine the organisation's response to the risk – how can the risk be controlled, reduced or eliminated? Determining appropriate action involves deciding what measures need to be adopted to respond appropriately to the identified risks, having regard to their gravity and priority. The overall objective is, as far as possible, to place the business in the position it occupied before the consequences of the risk were realised.

Therefore, the response should include the minimum requirement for essential operations to continue.

In practical terms, the organisation should develop a risk assessment plan showing categories of information needed for an informed assessment. Typical issues to be recorded are:

- type of risk;
- origin of the risk;
- criticality of the risk;
- necessary controls;
- responsibility for management;
- measure(s) to address the risk;
- any time frame;
- actions initiated.

This can easily be documented in the form of a simple spreadsheet. In the vertical column to the left might be listed the categories of risk. Across the top of the grid might be listed the various stages of management.

A risk control plan should be accessible to all concerned with its implementation. Personnel at all levels should be aware of the existence and location of the risk control plan. Detailed knowledge of its contents may not be essential, but personnel should have a broad idea of its content and the circumstances in which reference should be made to it. If the risk control plan is not too complex, there is no reason why it should not be incorporated into the business plan of the organisation.

The risk register

An alternative approach to recording the findings of a risk assessment is a risk register – a template to include all the necessary details relating to the risk and the contingencies surrounding it.

For instance, there should be information about the company, location, department, type of risk and even a number allocated to the risk. There should be a description of the risk, its root causes, its status, the likelihood of eventuality and its consequence. The response should be recorded and if elimination is impossible, there should be details of any residual risk.

Some IT solutions are now emerging which enable organisations to computerise risk assessment and risk management techniques. Risk Reasoning Ltd. has developed two modules: RiskAid and RiskAid Enterprise (*see www.riskreasoning.co.uk*).

Risk assessment techniques – ISO/IEC 31010: 2009

In addition to the risk management standards referred to in the previous chapter, a further complementary standard, ISO/IEC 31010:2009, has recently been published.

This addresses risk assessment concepts, processes and the techniques through to such issues as the likely consequences, the probability of their occurrence and any risk mitigation factors.

BS 31100:2008 addresses risk management frameworks, processes and implementation and is considered in the next chapter.

It is almost impossible to protect an organisation from exposure to every risk that might arise in the ordinary course of business. Invariably, the best that can be done is to assess the likely risks and devise a strategy of controls which balance their cost with their intended effect.

An effective procedure for assessing risks enables an organisation to take a proactive approach to the operation of its business. It can identify priorities and direct resources where they are most needed.

The foresight that effective risk assessment provides enables an organisation to know the time and commitment needed to address particular issues instead of simply responding to crises. Accurate risk assessment calls for correspondingly effective management.

CHAPTER 7: RISK MANAGEMENT STRATEGIES

The importance of risk management in the commercial sector was recognised in the Turnbull Report produced by the Institute of Chartered Accountants (*www.icaew.co.uk*), the recommendations of which became mandatory in December 2000. Broadly, the provisions state that:

- Risk management is the responsibility of the whole Board of Directors.
- Organisations should have a system of controls to protect shareholder and company assets.
- The controls should be reviewed at least annually.
- Risks should be regularly assessed and include risk management and financial, operational and compliance risks.

The key principles of corporate, IT and project governance were explored in Chapter 5. Effective risk management is a vital and fundamental component for the implementation of governance principles.

This chapter offers some practical suggestions for the creation, development and implementation of a risk management framework for the management of Internet risk within a professional services organisation. Once the risk management framework has been established, the organisation should strive to maximise its effectiveness through the application of governance principles.

The key elements involved in assessing and prioritising risk were examined in Chapter 6. There must also be in place an effective strategy for risk control and management; that is, its elimination or reduction to manageable levels. Risk management involves having clear procedures in place throughout an organisation in order to reduce failure or error.

Risk management strategies must be owned at a senior level within an organisation, so that established procedures and processes are observed, implemented and enforced. This is fundamental to the successful management of risk.

Earlier chapters identified the three areas of technological, legal compliance and operational risk. Since these risks span all areas of an organisation, a wide range of personnel become involved, offering different skills and assuming different responsibilities for implementing solutions. A framework is required within which the functions and responsibilities of different personnel are defined and understood throughout the organisation. This chapter explores the key features of risk management and a framework for the management of cyber risks.

Senior management

Certain characteristics are required of management if a strategy is to be implemented to optimum effect.

There must be leadership at senior level from those with skills and capabilities in Internet technologies. The commitment of the Board or Partners to the implementation of any strategic development is crucial and it is in the interests of the organisation to ensure senior level support for the strategy and its implementation.

Cyber risks introduce new types of risk requiring new management strategies that affect the whole organisation. Management of the strategy may require the recruitment of skilled staff, the retraining of existing staff, or the assignment of new responsibilities. The changes may be significant. If they are to be driven through, a committed approach from senior management is essential.

Effective communications are essential for the proper function of the organisation. Simple, direct, jargon-free, relevant communication, with a focus upon both content and recipient, is the most effective way of delivering an effective strategy.

The strategy may concern staff at all levels, so care must be taken to ensure that communicating the strategy is inclusive. Information should be accurate and timely. Communicating means establishing a dialogue, receiving feedback and making staff feel involved in the process.

Motivation is most easily achieved by treating people differently, listening to their concerns and offering encouragement on subjects that cause stress and difficulty. It is part of the process of communicating effectively. Staff perceiving that their concerns are recognised will more readily participate in changes that affect them.

Risk management principles

The adoption of five key principles is essential when approaching risk management.

The first requirement is a disciplined approach to decision making. There must be a comprehensive understanding of the scope, function and limitation of the strategy to be pursued.

Second, there is a need for a culture of awareness that risk both is present and cannot be ignored. Senior management creates an organisation's culture and, therefore, bears responsibility for the development of an awareness culture in an enterprise.

Third, there is a need to develop skills in weighing risk against potential opportunity. Encryption technology may involve considerable resources in terms of staff training and the cost of technology. However, if properly managed, the strategy will more than pay for itself if corporate clients are attracted through a perception that the organisation is sensitive to consumer concerns over security and adopts a modern approach to its use of information technology.

Fourth, there is need for an understanding of the wider implications of managing the strategy – an appreciation that the risk may be spread, or that implementation might involve a mix of approaches. This is particularly appropriate for Internet risks, where the risks arise from a variety of areas and where management solutions may be needed for these different risk areas simultaneously.

Fifth, there is a need to appreciate the changing environment, and that the organisation should be in a position to handle changes as they occur. New technology solutions emerge with great frequency. Each solution may have management implications in terms of new functions required of personnel and possibly the emergence of new legal compliance risks.

Objectives

The organisation's objective is to be responsive both in its approach to problems and to the imposition of internal or external changes. In this way, it will develop a flexibility that will enable it to manage risk and take advantage of business opportunities. The ultimate objective of any management strategy is to improve performance and to develop opportunities. Take as an example an organisation's website. Examples of risk management objectives might be to:

- promote the name and reputation of the organisation and protect them from damage;
- display up-to-date information for consumers, and avoid misinformation;
- maximise cost-efficiency by, for instance, minimising wasteful telephone resources;
- increase electronic take-up of the organisation's services by ensuring a user-friendly site.

Examples of risk management objectives in respect of the use of e-mail might be to:

- improve the speed and quality of communications by avoiding poor e-mail protocol;
- encourage information sharing;
- facilitate communications by avoiding unsupervised e-mail activity;
- ensure confidentiality by managing encryption services.

Benefits

Risk management offers different benefits at different levels. Careful supervision and management of information on a website supports a strategy of developing a one-to-one relationship with commercial consumers. Ensuring a disciplined approach to the use of internal and external e-mail will increase efficiency. Adopting a controlled approach to use of the Internet will avoid wastage of employees' time and eliminate possible criminal liability.

The Internet is always available – advice and services may be required at all times. Consumers have expectations in this respect and organisations are expected to respond as part of their marketing strategy. Appropriately devised and carefully implemented strategies enable an enhanced service of this nature to be provided.

Taking a general view, a comprehensive strategy implemented conscientiously and with the commitment of top management enables an organisation to take confident control of its operations and facilitates a proactive approach in the development of its services and clients.

Cyber risk management framework

A cyber risk management framework should be integrated into the framework for the overall management of the organisation. It is important to avoid a cyber risk management strategy being 'hijacked' by developing its own identity and pursuing its own agenda, otherwise there is a danger of lack of commitment from those not involved in its implementation and of indifference towards its effectiveness.

Directly beneath and accountable to the Directors or Partners should be a risk manager, together with any team in support. At the same level might be:

- in-house experts who liaise with the risk manager, but might also offer expert advice independently to the Directors or Partners;

- internal auditors, for the most part working in conjunction with the risk manager, but also offering audit advice to the Directors or Partners;
- external sources, such as external consultants and external auditors.

Directors or Partners are then able to take a wider view of the strategy as a whole. Managers manage the risk. In-house experts provide specialist assistance. Auditors provide independent and objective assessments. While there may be some interaction between the various parties, the structure of accountability means that the Directors or Partners are at the centre of the strategy, with an overview.

The management of cyber risks can be mapped across this model. The framework of resources and accountability remains. However, the sources of information for the risk manager will flow from line managers in a number of areas. The risk manager will require advice and information from line managers experienced in technology, legal compliance and operational issues. The risk manager may also need to call upon specialist internal or external assistance. For any assessments the risk manager makes, there will be accountability to the Directors or Partners and perhaps to the auditors.

Risk manager

The risk manager has two functions. The first is to advise the organisation about the risks involved in any particular strategy. The second is to take or assume ownership of the risks. These responsibilities include:

- ensuring that responsibility for managing is clearly established, communicated, delegated and accepted;
- ensuring internal controls are adequate;
- establishing appropriate information systems;
- reviewing strategic developments.

What are likely to be the requirements of a risk manager? First, as Internet technologies involve a real understanding of information technology, the risk manager must have some grounding in this area if the risks are to be properly assessed and evaluated. There are also legal and operational risks. The risk manager, therefore, requires some awareness of legal and human resource management skills. The risk manager should also have some administrative capability to ensure that risk management strategies are implemented effectively.

The risk manager must be able to take an overview, identifying strategies and objectives across areas in which cyber risks arise, selecting the most suitable options. The risk manager is the focal point for identifying and managing risks as they arise and will consult line managers and exchange information with internal and external experts, as well as receiving the Directors' or Partners' views and concerns.

A new skills certification has been launched for risk management professionals – the Certification in Risk and Information Systems Control – commonly referred to as CRISK. This has been developed for IT and business professionals engaged at a personal level in risk mitigation by ISACA (*www.isaca.org*), the Information Systems Audit and Control Association.

Project manager

The project manager will direct the team alongside the risk manager on the implementation of the strategies approved by the risk manager.

A project is a task intended to be undertaken in specific time limits and with specific individuals and is usually the responsibility of a team. Internet risk management is not only a project in itself, but also comprises a series of sub-projects, such as the introduction of encryption technology and procedures, and the monitoring of employees' use of e-mail.

From a governance perspective, certain features are critical to the success of a project:

- continuous alignment with objectives;
- regular monitoring and auditing;
- adequacy of resources;
- a structured approach to risk management.

Where required, the application of project management methodologies and tools such as PRINCE2 and Val IT 2.0, both discussed in Chapter 5, might be adopted.

In leading the project, the project manager should have in mind the need for:

- executive leadership;
- senior-level approval and commitment;
- clear strategies, objectives, allocations of responsibility and accountability, planning and budgetary considerations and resources;
- monitoring and verifiable measurement procedures as the project progresses.

Alan Calder has addressed this aspect of project management at some length in *IT Governance Today: A Practitioner's Guide,* IT Governance Ltd. (2005).

Cyber risk team

Emily Freeman of Lockton International offers some helpful markers in identifying the key issues facing a cyber risk management team:

> The key issue for proper management of Internet risk is that there is a cross-functional structure of cyber risk management, and that risk management is not structured in individual silos.
>
> Typical areas that should be represented within the risk committee or team structure include the following:
>
> - internal audit/compliance;
> - risk management;
> - IT security;
> - legal;
> - business units/operations;
> - procurement.
>
> The risk management strategy should be supported at board/senior executive level and managed and implemented by various individual managers by function, and a standing risk committee with clear lines of responsibility and accountability.

Skills

Managing cyber risks calls for skill and capability in a variety of specialist areas, such as risk management, information security, legal and regulatory issues, personnel management and administrative functions.

Other skills may also be required, depending upon the size of the organisation, the way it employs Internet technologies and the electronic services it provides. With such a wide variety of disciplines, the logical approach is to create a cyber risk team of suitably skilled and qualified individuals equipped to address and manage the needs of the organisation.

The most appropriate leader of the team is the risk manager. The risk manager must be capable of articulating the advice of the team to the Directors or Partners and acting as a conduit.

Team members should have interpersonal skills to handle feedback in respect of the new issues being addressed. Teamwork requires conformity to a common purpose and mutual support. A team develops through a shared level of dependency and mutual interest and is most effective when its performance as a unit is of greater value than the performance of the individual team members.

The team should document its own risk control plan, identifying the particular cyber risks to which the organisation is exposed and the solutions or controls to be adopted. It should dovetail with the organisation's business plan. If the principal business plan changes, the risk control plan should be amended to take account of any new risks to which the organisation may be exposed.

Roles

The structure of the team should be documented, so that the framework for the management of the project is clearly understood. A documented job description clarifies areas of responsibility and accountability.

A convenient way of clarifying accountability should be to make each team member accountable to the risk manager in the first instance. In turn, the risk manager should be accountable to a specific director, partner or committee for the performance of the team – in effect, a line management approach.

There should be specific assignment of responsibility for particular functions – technology risks, legal compliance risks and operational risks. In addition, there should be a board or partnership representative. The team may wish to co-opt specific members for particular projects. These might include, for instance, representatives in respect of finance, marketing or public relations.

Team members should be properly inducted on appointment and the new appointee should be informed of the responsibilities and functions of the other team members, their relationship with each other and team operating procedures. New Internet risks are always emerging because of the shifting and mercurial nature of Internet technologies so a framework for the education and training of all team members is necessary.

The composition of the cyber risk team might resemble this:

- the risk manager;
- the technology risk representative(s);
- the legal compliance risk representative(s);
- the operational risk representative(s);
- a board/partnership representative(s);
- other optional representatives.

Consultants will be drawn in where specialist expertise is required, especially for such issues as business continuity and disaster recovery.

It is important to ensure adequate awareness of:

- the objectives of the team;
- the steps to be taken by each team member;
- the respective responsibilities of each team member;
- the respective accountabilities of each member;
- induction procedures;
- training and skills development;
- audit procedures.

Strategies

It is important to link the operations of the cyber risk team with the business plan of the organisation to ensure that any risk arising from the business plan will be identified. The organisation's business plan should identify any new, extended or improved services to be provided. The response of the team should be to identify any cyber risks to which the new range of services exposes the organisation and to incorporate this in its risk control plan.

Thought should be given to the type of cyber risk that might result from any new business developments. For instance, if the organisation proposes to introduce a system of electronic payments for certain of its services, the cyber risk team should identify and address any new risks.

Business environments change so rapidly that long-term planning is often impractical. The team's risk control plan should reflect, in broad terms, the lifespan of the principal business plan. The rapid development of new technology solutions may require the team to recommend the adoption of a particular solution not available when the plan was conceived. The implementation of new legislation might give rise to a cyber risk that did not exist when the principal business plan was prepared. In such situations, the cyber risk team becomes a major asset to the operation of the organisation, its vigilance extending its function from reactive risk avoidance to proactive risk anticipation and introducing new ideas for business development.

Projects

The team will need to define closely the nature of the risk and the type of hazard presented to the organisation, and consider its likely duration and frequency, and whether it is an internal risk, for example the behaviour of employees, or an external risk, for example the risk of virus infiltration.

The first task is to define at an early stage how the project will be managed and resourced. It will also be necessary to identify the scope and objectives of the project. The project may be relatively straightforward, for example the design of a website. A much more complex project might involve the integration of a customer's or client's security systems with those of the practice.

Objectives

The team's objective is to control, reduce or eliminate the risk. A decision must, therefore, be made on the organisation's tolerance to each risk. For instance, the installation of anti-virus software will protect against known viruses, not against malicious code that is written at a later date. The best that can be done is to reduce or minimise risk by ensuring that anti-virus software is regularly updated.

There are three objectives open to the risk management team. First, the risk might be tolerated if it is not cost-effective to manage it. If an organisation proposes to advertise its services and is concerned about the infringement of applicable codes of advertising in foreign jurisdictions, the organisation might take an expedient view and place a notice on the site to the effect that the advertisement is directed to, say, those seeking advice or services in England and Wales only. The risk is reduced, leaving residual risk which can be tolerated.

Second, steps can be taken to eliminate the risk. Elimination of risk is problematic in terms of Internet technologies because of their novel features and the relative uncertainty of their implications. However, a simple example might be to eliminate the risk of infringing data protection provisions when obtaining marketing information about visitors to the firm's website by taking steps to ensure that informed consent is obtained to the process. Once eliminated, the risk can be monitored for any change from time to time.

Third, steps can be taken to transfer the risk. Probably the most likely example of this is to arrange insurance cover. Insurance cover is not a substitute for efficient management strategies, but is an essential support when all possible steps have been exhausted in addressing a specific risk.

In formulating a plan, a useful approach is to document the objectives in the risk control plan, including an executive summary, types of emergency, responses, identification of responsibilities and documentation.

Resources

Resources are ultimately for senior management to consider and will represent a balance between the degree of the risk and the cost of managing it in an acceptable way. The balance between cost and risk is a basic formula to be considered in every management strategy. As the use of Internet technologies develops, organisational expenditure on its risk management strategy will increase.

In deciding the budget, the organisation will need a good understanding of the level(s) of risk to which it is exposed and the degree of its vulnerability. Internet technologies introduce a wide variety of risk and the budget should be proportionate to the risk involved. As the organisation is taking a strategic approach to budgeting, enterprise-wide financial support should be provided. There is little point in providing support departmentally.

In terms of technology risks, the principal items of expenditure are likely to involve hardware and software requirements for implementing solutions, importing whatever technology solutions are needed to meet identified risks. In terms of legal compliance risks, recourse to a daily or weekly legal updating newsfeed or news service may be necessary. However, there may be other items. For instance, if the team were to recommend that the firm should achieve certification under relevant British or international standards, the anticipated expenditure would need to be included in the budget. From time to time, legal and professional advice is likely to be required.

Financial resources should be allocated in accordance with the agreed priorities. It is important that expenditure is shown to be a return on investment. The effectiveness of a strategy is not governed by the amount of expenditure, but by the effectiveness of the expenditure in terms of meeting the organisation's need. The easiest way to identify potential expenditure is for each team member to assess expenditure required in his or her own domain and to present a case for it to the risk manager. The Board or Partnership ultimately sanctions expenditure for resources, emphasising the importance of partner-level involvement in the team.

Authorisation

Authorisation procedures should be in place. This is an indication of commitment at the highest level to managing cyber risks and it ratifies any subsequent action that may be taken by the management team.

The level at which authority for a particular action should be given will depend upon the nature of the action to be taken. The Directors or Partners may agree to delegate all decisions to the management team, particularly if there is a board or partnership representative. On the other hand, the decisions that the management team are required to take may have significant strategic, operational or financial implications. In that case, the Directors or Partners may prefer to receive recommendations for strategies for formal endorsement or amendment as appropriate.

Decisions

Once the risk control plan has been developed, thought must be given to the way in which the risks can be treated. It can be helpful to prepare a matrix for this purpose, which can take the form of a grid of four squares. One illustration of how simple this can be is to create a grid. Along the base line is a measurement of consequence, from 'low' to 'high'. Along the vertical line is a measurement of likelihood, also from 'low' to 'high'.

The bottom left square of the grid represents a risk of low consequence and low likelihood and, therefore, may be a risk requiring toleration, or no action. The bottom right square represents a risk of high consequence but low likelihood and, therefore, might be a transferable risk, perhaps through insurance. The top left square represents a risk of high likelihood but low consequence and, therefore, should be covered in the risk control plan. The top right square represents a risk of high likelihood and high consequence and, therefore, requires immediate elimination.

Unless a particular risk, or set of risks, can be eliminated entirely, there will be some residual risk. It is important to understand the distinction between this residual risk on the one hand and inherent risk on the other hand.

Management is largely concerned with inherent risk, namely risk that is critical and requires immediate attention. In the first instance, the team will be concerned with the control of inherent risk. Once inherent risk is controlled, some residual risk may remain. Senior management will be concerned that this remains residual and that it is manageable without further action. The level of residual risk, therefore, depends upon the degree to which the inherent risk can be controlled.

Implementation

Responsibility for implementation lies with those involved in complying with any policy developed by the management team. For example, those using e-mail will be responsible for ensuring that both they and their subordinates comply with any declared e-mail acceptable use policy.

Responsibility also lies with the risk management team itself. The management team will be accountable to the Board or Partnership for ensuring compliance with adopted policies and solutions. The authority of the management team might be underpinned by the presence of a director or partner on the team, so that compliance is ensured.

Records

There are important reasons for maintaining adequate records of incidents. A full record will state the problem, the progress and the objectives of any solution. Adequate details will also be available in the absence, for example through illness, of the team member responsible. Records will also help in the event of any claim against insurers and enable the organisation to develop an archive of experience in handling incidents and problems, as well as helping with audits.

Some record will be needed to identify and distinguish the different projects in which the team might become involved. The projects may vary considerably. The team might be asked to undertake a risk assessment on the installation of software for an electronic payments system. It may be asked to investigate the feasibility of providing services via an extranet, or to assess the implications of allowing a particular customer or client access to the organisation's intranet. There will also be what may be termed 'casework', where the team investigates security incidents, client complaints or other external issues arising from its electronic services.

It is sensible to maintain a case file for each ‘case’ assigned to the cyber risk team. Certain information should be recorded, such as: the team member responsible; the nature of the incident; any risk assessment details; external assistance required, for example from consultants; the interests of any third parties; the policy approved by the team; and critical dates for the project.

The team should make recommendations for the adoption of policies and procedures to manage a particular risk. The most obvious examples are the adoption of e-mail use or Internet access policies. More specifically, particular measures may be needed for a particular customer or client.

It is important that procedures adopted by the organisation are properly documented and circulated. They should be accessible to others with whom the organisation has dealings, such as financial service advisers.

The team will collect a considerable body of data. It is sensible to maintain a formal database to avoid duplicating original research.

There should be an index of each incident, identifying the team member responsible for its management. There should be a record of the action identified by the team and a progress chart to indicate the steps taken, identifying any key dates. The objectives of the strategy and its potential impact, internally and externally, should be noted. Changes in the adopted strategy should be noted. If capable of assessment, there should be some record of the costs involved at each stage, so that appropriate and timely budgetary control can be exercised.

The use of external resources, for example consultants, should be recorded, together with a note of all others whose participation is essential for the effective management of the solution. These may include specific individuals in the practice, or even whole departments where the involvement of departmental heads will be required.

The organisation should be able to analyse the cost of each cyber risk ‘incident’ that arises. Records should be maintained detailing the cost in terms of expense and time in rectification of any security breaches, resolution of communication problems or addressing of compliance problems.

Monitoring

Risk management is a continuous process and must be flexible enough to meet continuously evolving changes. After implementation, it will be necessary to monitor progress on both a short-term and long-term basis.

Monitoring and review of incident files is important because it tests the effectiveness of a proposed solution adopted to meet a particular problem or risk and offers an opportunity for a change in strategy, or adoption of an alternative solution, if the chosen solution is ineffective.

The monitoring process will be concerned with a number of different outcomes. The most immediate will be the extent to which the risk has been eliminated or resolved in accordance with the project plans. The risk manager will also need to ensure that the controls remain in place and that awareness training continues as required.

There should be specifically assigned responsibility for the monitoring and supervision of the team’s risk management strategy. There should be regular review and reporting procedures, perhaps as an agenda item for each meeting of the management team.

Logically, the leader of the management team should be responsible for the review, perhaps with any board or partnership representative. Reports would be received from each of the specific risk area (technology, legal and operational) representatives. Each representative would report upon existing risk areas, and discuss the impact of the adopted strategy, and review and evaluate its impact.

If for any reason the risk control plan or the project plan has not been implemented as required, appropriate adjustments will be needed. The same applies if the results are not as intended, even though implementation is proceeding as planned. Either situation may involve minor corrective action or the need to revisit the risk assessment.

Audits

Audits are a critical part of the risk management process. Organisations are now under considerable pressure to identify and address risk issues. Boards of directors and partnerships have to show stakeholders that risks are being acceptably managed. Audits evaluate the effectiveness of risk management strategies and recommend improvements. They determine whether key risks are being controlled, if controls are operating effectively, and whether management is identifying and responding to emerging risks, through efficient and effective accountability.

In undertaking an audit, either internally or externally, management should establish the purpose of the audit; identify the key factors supporting the evaluation of its findings; identify the key factors to employed in audit testing; and, when receiving the report, it should then evaluate, implement, report, monitor and improve its risk management systems and procedures.

Any audit of risk management processes should include a focus on governance structures. There should be an unambiguous assumption of leadership by the Board or Partnership, supported by: clear documentation specifying lines of responsibility and accountability; clearly identified policies and procedures; and identifiable processes for planning, detection, monitoring, reporting and reviewing risk management strategies.

Information security is a critical area of risk management for all organisations. Typical areas that the organisation will need to audit include the effectiveness of:

- network security technology;
- website security technology;
- IT systems security technology;
- remote, mobile and wireless security technology;
- PCI compliance technology;
- communications (e-mail, instant messaging, VoIP) security technology;
- data security technology.

Richard Spooner, Head of IT Advisory at Baker Tilly, says that audits are highly challenging for the accountancy profession:

> From the perspective of professional accounting practice, one consistently worrying risk relates to the provision of auditing services. The proliferation of electronic transactions gives rise to considerable auditing risks. Electronic transactions are not transparent in the same way as paper-based transactions. They are difficult to identify and there may be no formal permanent

records of transactions. In turn, this makes it very difficult, if not impossible, to establish an audit trail.

Auditing the business of, for instance, city traders and, say, Internet gaming companies, presents considerable professional risks to auditors when audit trails are so difficult to identify. Furthermore, this extends over organisations of all sizes, including, for example, supermarkets in the context of complex supply chains controlled by computerised ordering systems.

Audit services are offered by a number of organisations and various resources are available offering help and guidance in approaching an IT audit – see, for instance, Praxiom Research Group Ltd. (www.praxiom.com) for an example of critical issues to be addressed in information security auditing.

From an IT governance perspective, what are the procedural criteria for an IT security audit?

Alan Calder[5] suggests auditors should conduct a risk-based audit, usually based on four procedures:

1 Determine the scope of the analysis of the IT processes by their support of critical business processes and processing of financial information.
2 Obtain background information about the supplier's IT environment, its underlying platforms and networks.
3 Identify the IT processes which have a direct and important effect on processing financial information.
4 Evaluate the effectiveness of each of the major IT processes and related internal controls.

Documented processes, procedures, mechanisms, tools and controls should be available to the auditors and the audit

[5] *IT Governance: A Practitioner's Guide*, Calder A, IT Governance Ltd. (2005).

should cover architecture, platform and application technologies. Specialist auditors may be required for specific IT systems, and a range of audits may be needed to address individual objectives.

Chapter 5 identified IT and project governance frameworks that might underpin an Internet risk management project and this chapter suggests how a management framework might be constructed in order to meet the demands of the many and various types of Internet risk.

It is important not to confuse governance and management. Governance is not management and management is not governance. Management is concerned with the actual conduct and implementation of a strategy. Governance is a framework which supports effective management and provides tools such as industry standards and methodologies that help assure the success of management strategies and the outcomes of projects undertaken in their implementation.

Standards certification

A number of British and international industry standards, many supported by codes of practice, have been developed for the certification of organisations with regard to management of information security strategies and their risks. This section identifies the principal standards available. Every organisation is different and will need to identify the risks to which it is exposed and then consider which, if any, of the standards are most appropriate for the management of its risks.

Corporate governance of information technology

BS ISO/IEC 38500:2008

Chapter 5 identified principles of corporate governance; in particular, the need for governance principles to be applied to IT strategies and how BS ISO/IEC 38500:2008 provides a framework for this. The standard is not directly concerned with risk, but rather provides a framework of good practice for organisational processes and procedures which, if adopted, help minimise exposure to risk in the execution of business processes.

Project management

BS 6079:2002

As explained in Chapter 5, the adoption of a strategy for managing Internet risk and information security is a project in the same way as any other business project. On the same principles as BS ISO/IEC 38500:2008 above, this standard provides an organisational framework of processes and procedures which help to minimise exposure to risk arising in the development, management and execution of projects.

Risk management

BS 31100:2008

The code of practice, BS 31100:2008, for risk management provides recommendations for the framework, process and implementation of risk management. It is designed for: CEOs, CFOs, CROs, CIOs, COOs, CTOs, chairmen and company secretaries, managing, finance and IT directors, and risk managers, among a number of other categories.

The standard provides recommendations for the framework, process and implementation of risk management and should be used for:

- ensuring a business achieves its objectives;
- ensuring risks are proactively managed in specific areas or activities;
- overseeing risk management in an organisation;
- providing assurance on risk management strategies;
- reporting to stakeholders, for example through annual financial statements, corporate governance reports or corporate social responsibility reports.

The standard establishes the principles and terminology for risk management. It also gives recommendations for the model, framework, process and implementation of risk management gained from experience and good practice.

Business continuity

BS 25999-1:2006 business continuity: code of practice

BS 25999-2:2007 business continuity: specification

These standards represent respectively the code of practice and the specification for business continuity. The code provides a comprehensive set of controls based on best practice throughout the business continuity management life cycle.

The standard specifies the requirements for establishing, implementing, monitoring, reviewing, exercising, maintaining and improving a documented business continuity plan. The standard does not seek to impose uniformity; organisations should develop strategies for their own needs.

BS 25777:2008 information and communications technology continuity management; code of practice

This code of practice is intended to support a wider business continuity plan and addresses the subset of ICT. The code covers such issues as ICT continuity programme management and ICT continuity strategies and their development, implementation exercising, testing, maintenance, review and improvement.

The code supports the process towards certification under BS 25999-2:2007: Specification for business continuity management.

BS ISO/IEC 24762:2008 information technology: security techniques: guidelines for information and communications technology disaster recovery services

This standard offers guidance on the provision of disaster recovery services as part of business continuity management. The standard is expressed as especially suited to outsourced service providers as it describes the best practices that suppliers should consider. It highlights specialist requirements such as special encryption software, secured operation procedures, equipment, knowledgeable personnel and application documentation.

Information security

BS ISO/IEC 27001:2005 information security

This standard provides a benchmark for the management of information security management systems (ISMSs). It provides a specification for ISMSs and the foundation for third-party audit and certification. It is compatible with other management system standards, such as ISO9001 and ISO14001, and will assist in the integration and operation of an organisation's overall management systems. This specification replaces BS 7799-02:2002.

The principal elements of the standard address:

- definition, requirements, establishment, implementation, monitoring, review and improvement of an ISMS, together with supporting documentation;
- management issues including responsibilities, resource issues, resource provision, commitment, training awareness and competence;
- audit and review processes, including input and output, improvement processes and corrective and preventative action through prescribed control mechanisms.

There are also a number of related standards addressing the management of ISMSs. They include:

- ISO/IEC 27005:2008: Information security techniques;
- ISO/IEC 27002:2005: Information technology security techniques: code of practice;
- BS ISO/IEC 27004:2009: Information security techniques: information security management: measurement.

BS ISO/IEC 27003:2010 information security management systems: implementation guidance

BS ISO/IEC 27003:2010 focuses on the critical aspects needed for successful design and implementation of an ISMS in accordance with ISO/IEC 27001:2005.

It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

The process described within this international standard has been designed to provide support for the implementation of ISO/IEC 27001:2005.

BS ISO/IEC 27003 is intended to be used by organisations implementing an ISMS. It is applicable to all types of organisation of any size. Each organisation's complexity and risks are unique, and its specific requirements will drive the ISMS implementation.

BS ISO/IEC 27004:2009 information security management – measurement

BS ISO/IEC 27004 is the standard that provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an ISMS and controls or groups of controls, as specified in BS ISO/IEC 27001.

This would include policy, information security risk management, control objectives, controls, processes and procedures, and supports the process of revision by helping to determine whether any of the ISMS processes or controls need to be changed or improved. It needs to be kept in mind that no measurement of controls can guarantee complete security.

The implementation of this approach constitutes an information security measurement programme. The information security measurement programme assists management in identifying and evaluating non-compliant and ineffective ISMS processes and controls, and prioritising actions associated with improvement or changing these processes and/or controls. It may also assist the organisation in demonstrating ISO/IEC 27001 compliance and provide additional evidence for management reviews.

BS ISO/IEC 27033-1:2009 information technology security: network security

The majority of commercial organisations have their information systems connected by networks, with the network connections being one or more of the following:

- within the organisation;
- between different organisations;
- between the organisation and the general public.

The purpose of BS ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their interconnectivity.

Those individuals within an organisation who are responsible for information security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements.

Data protection

BS 10012:2009 specification for a personal information management system

Data protection issues involve both technology and compliance issues. A British standard has been published specifying the requirements for a personal information management system. It provides an infrastructure that includes the implementation of a framework for compliance with the DPA.[6]

It is intended for adoption by organisations of any size and provides a framework for managing personal data that meets compliance standards of both internal and external audits.

Even a brief examination of the key principles of these standards demonstrates their importance to organisations using the Internet as a business strategy. Certification under ISO/IEC 27001:2005, for instance, is recognition of the commitment of the organisation in aspiring to particular levels of excellence in the management of ISMSs. The cyber risk team model is an appropriate vehicle for moving toward certification. The cyber risk team could easily assume responsibility for the certification process.

[6] Permission to reproduce extracts from the British standards quoted on pages 97, 106, 149-155 is granted by BSI. British standards can be obtained in PDF or hard-copy formats from the BSI online shop: www.bsigroup.com/shop or by contacting BSI customer services for hard copies only: telephone +44 (0)20 8996 9001, e-mail cservices@bsigroup.com.

Robert Jackson of Capgemini says:

> Standards in Internet risk and security are vital – they are the currency of information security. They are the only reliable evidence of assurance.
>
> The problem with standards is that there are many of them and it is difficult to keep up with them. They are not a panacea; and the question needs to be asked as to whether some standards go far enough. Standards are the start and not the end.

However, certain practicalities require consideration. Seeking certification is likely to be expensive, particularly in terms of staff time. A glance at the key principles illustrates the procedures to be in place to comply with the standard.

Smaller organisations, in particular, may find it difficult to divert the significant resources required for compliance. Larger organisations with employees dispersed over a number of offices may find the quality of control and management that the standard offers to be an attractive proposition.

Andrew Rose of Clifford Chance has strong personal views on benchmark standards:

> My personal view, which may not be widely shared, is that the legal sector would benefit from more clearly defined regulation – perhaps in the form of a requirement to conform to ISO/IEC 27001:2005, the standard concerning information security. Although the solicitors' representative and professional body has issued, for instance, guidelines on the use of e-mail and information security, they are generally very broad because they have to address the needs of both the largest law firm and sole practitioners.
>
> We are now finding that clients are developing and increasing interest in, and influence over, compliance with ISO/IEC 27001:2005. There is also a drive in this direction from cyberliability insurers.

Certainly insurers are now likely to take more than a passing interest in whether an organisation has achieved certification; and, as Andrew Rose asserts, certification may also become a marketing issue, as customers, clients and strategic allies become more sensitive to the need to ensure the security of increasing volumes of sensitive data passing between networks, and insist on certification under the standard.

However, Emily Freeman of Lockton International cautions against complacency over achieving certification:

> While adoption of such standards is desirable, it should be remembered that certification is not a guarantee of security but simply a benchmark of best practice. A continuously improving defence in depth is recommended with regard to data security.

Risk compliance provisions

Two further provisions require consideration in the context of managing Internet risk.

Sarbanes-Oxley Act 2002

This Act applies to publicly listed companies and management and public accountancy firms in the USA, together with UK subsidiaries of these organisations, providing the holding company has a significant interest and influence over the internal controls and profitability of the subsidiary. The Act does not apply to private companies.

Organisations are categorised by 'large accelerated filers' with a worldwide market value of over $700 million; 'accelerated filers' with a worldwide market value of over

$75 million but less than $700 million; and 'non-accelerated filers' comprising small companies.

On 23 May 2007, the Securities and Exchange Commission issued guidance to non-accelerated filers (*Sarbanes Oxley (SOX) compliance, SOX 404, Sarbanes Oxley information for non-accelerated filers*) setting out the requirements for management and audit reports for organisations with a worldwide market value of under $75 million.

The provisions of the Act are extremely complex and the consequences of non-compliance are serious. An organisation that is concerned as to whether it is caught by a requirement to comply with the Act and then subsequently to meet compliance requirements, should seek professional advice in every case.

The key provisions which apply to listed companies, and to which subsidiary UK companies should have regard, are broadly summarised below:

- Section 302 prescribes the content of periodic statutory financial reports and certification requirements.
- Section 401 requires financial statements to be accurate and include material information.
- Section 404 requires publication in annual reports of the scope, adequacy and effectiveness of the internal and financial controls.
- Section 409 requires disclosure of changes in financial circumstances.
- Section 802 imposes penalties of imprisonment for acts committed in respect of financial records with intent to obstruct a legal investigation.

Basel Committee

In February 2003, the Basel Committee of the Bank for International Settlements published *Sound Practices for the Management and Supervision of Operational Risk* to address risk issues in the banking sector. This provides guidelines for good practice in the areas of:

- development of an appropriate risk management environment;
- risk management procedures;
- the roles and responsibilities of supervisors;
- risk disclosure requirements.

Further details are available at *www.bis.org*.

Financial Services Authority

The Financial Services Authority (FSA) periodically publishes guidance and white papers relating to systems and controls, suggesting good practice. Further details are available at *www.fsa.gov.uk*.

These three sources introduce compliance provisions which relate primarily to the financial services sector. However, the importance of the provisions lies both in their regulatory enforceability, and also in their alignment with principles of good governance and risk management. To the extent that effective management of Internet risk and information security has financial implications and consequences for an organisation, the system of internal controls required by these provisions should be implemented.

PART 3 – CYBER RISK SOLUTIONS

CHAPTER 8: TECHNOLOGY SOLUTIONS

Chapter 2 identified the key IT risks arising from the use of Internet technologies. This chapter considers how these risks can be addressed through the implementation of certain IT solutions. The categories of technology considered are:

- communications;
- information and data;
- business continuity and disaster recovery;
- networks;
- identity and access management;
- outsourced IT;
- Web 2.0.

Communications

The principal technology solution for securing electronic communications is the application of cryptography, which is a technique employed for the concealment of the content of communications.

E-mail encryption

The method of cryptography employed within electronic communications is encryption. Currently, the two most common drivers for the encryption of data generally are: first, the need for compliance, especially with regard to data protection requirements; and second, the need to protect data from loss, interference or exposure, most especially in the case of sensitive data. Data encryption is a risk management strategy.

Encryption disguises the content of a message. Decryption reveals the content of a message. The encryption process is performed by the creation of a numerical key that disguises the content in such a way that it can only be deciphered by a corresponding key. The security of the key depends upon its length. The widely used industry standard is 128-bit encryption. There are two types of encryption: symmetric encryption and asymmetric encryption.

Symmetric encryption

In this case, sender and recipient use the same key to both encrypt and decrypt, so the parties must have the same key to communicate with each other. If a sender wants to communicate with a large number of recipients, the same key must be held be each recipient. This is hardly practical as it severely limits the level of confidentiality.

Asymmetric encryption

In the asymmetric model, two keys are connected by a set of numbers. One key (the first set of numbers) is made public and is distributed as required. It is referred to as the public key. The second key (the second set of numbers) remains private. This is called a private key and is coded to decrypt a message encrypted with a specific public key.

The procedure can be more easily understood when broken down into stages:

1 A wishes to send a confidential e-mail to B using asymmetric keys. A obtains B's public key from a public

key repository (*see Certification and Registration Authorities page 168*), which is a public storage facility.

2 A encrypts the e-mail with B's public key (the first set of numbers) and sends the message to B.
3 B receives the e-mail and combines his or her public key (the first set of numbers) with his or her private key (the second set of numbers).
4 The combination of the first and second sets of numbers enables B to decrypt the e-mail.

The use of this model, known as public key encryption, is an effective solution to two uncertainties of using e-mail: privacy is preserved since only B can open the message; integrity is preserved since the message cannot have been tampered with as only B can open it.

The name given to the framework supporting the creation and administration of public key encryption is called public key infrastructure, commonly referred to as PKI.

Secure socket layer

However, PKI is not used exclusively. The size and cost of installing a fully operational PKI is beyond the skill and resources of many organisations. Another solution has been developed – the secure socket layer (SSL). In this model, when a secure transaction is required, for example for the supply of confidential information over a website, the SSL protocol may be employed. The use of SSL technology is signified by a small padlock or key graphic appearing on the website.

Technologically, the web server and browser exchange public keys and use them to create another key, which is sent back down the line. The received key is combined with the original key to make a new key that is common to both. Third parties cannot intercept because they will have no knowledge of the original keys.

Secure electronic transfer

Secure electronic transfer (SET) is a model frequently used for the transfer of payment by credit card. The model differs from SSL in that, even at the merchant's site, the card number remains encrypted, so eliminating another stage of potential fraud. The encrypted card number is passed to the bank, where it is decrypted and the merchant then receives payment.

VoIP security

VoIP is the transmission of voice communications over Internet protocol networks. While VoIP technology offers the advantage of lower cost and more flexibility for voice and data communications, it has the potential to expose organisations to a number of security vulnerabilities. These were considered earlier.

Like any other digital data, voice communications travel in packets and although some of the traditional security measures, such as firewalls, can be employed to protect voice data, VoIP technology also requires additional measures. Some of these protective measures can affect the quality of the service in terms of disruption or delay.

For instance, firewalls are programmed to protect data by governing the traffic entering systems. The effect of this process on VoIP technology can render the system almost inoperative. Other tools, such as network address translation, can protect internal addresses by concealing them but at the same time also make calls into an organisation difficult to manage.

Furthermore, firewalls on their own will not always afford protection to VoIP communications and although VoIP communications can be encrypted, the management logistics become complex and inevitably reduce the quality of service.

Certain standards have emerged, such as session initiation protocol, but the adoption of an overarching benchmark standard for VoIP security has yet to emerge. In the meantime, certain observations should be noted in respect of both VoIP and its security:

- VoIP infrastructures are complicated and, if possible, voice and data infrastructures should be run separately.
- Firewalls need to be especially configured to allow VoIP communications.
- Encryption of VoIP communications should be applied centrally.
- VoIP communications are more vulnerable than traditional telephone communications because of their involvement with data transfers.
- If mobile devices are used for VoIP communications, Wi-Fi protected access technologies should be adopted.

VoIP technology is a complex and potentially resource-intensive infrastructure requiring personnel skilled and experienced in both security, and voice and data transfer technology. While the cost and varied functionalities of VoIP are a potential attraction for organisations, these attributes come at a price. Voiptalk is an example of VoIP solutions (www.voiptalk.org).

Instant messaging security

Instant messaging is rapidly becoming one of the most popular forms of business communication, mainly because of its ability to enable communications to be delivered in real time among employees and customers, and, of course, it can run in parallel with e-mail as an internal communication technology.

In many ways, IM resembles e-mail in respect of the immediacy of the communication and its ability to be transmitted to a large number of recipients. It also suffers from similar problems in terms of IT insecurity, legal and compliance issues, and potential abuse by users.

In terms of security, data transmitted by IM is governed by the DPA in the same way as any other electronic data and if not secured, it offers the opportunity of infection from viruses and other forms of malware.

These communications must, therefore, be treated in the same way as e-mail, with appropriate attention paid to security and confidentiality in addition to the deployment of protective measures that will ensure the network is not infiltrated by malicious code.

An example of one IM solution is MessageLabs' Instant Messaging Security Service (www.messagelabs.com), an IM security control and management service which offers protection against new, emerging and converging threats. Incoming messages are scanned for viruses and malware and links to websites containing malware. Outgoing messages are matched against control and IM use policies. Suspicious messages are blocked and all messages are logged in MessageLabs' secure infrastructure.

Instant messaging communications do not receive the high-profile exposure of e-mail, but in many ways IM resembles the state of e-mail a few years ago, when e-mail use was not governed closely and e-mail security was an embryonic concern for organisations. However, some commentators have expressed the view that in the near future, IM will overtake e-mail as the mainstream medium for electronic communications.

Digital signatures

Digital signatures should be distinguished from electronic signatures. The latter refer to any method used to connect an individual's identity with an electronic document, for example the sender's name typed at the foot of an e-mail. Digital signatures refer to specific technology (asymmetric encryption) which binds an individual's identity to an electronic record.

The characteristics of a digital signature are that as only one person creates it, there is protection from fraud or forgery; it provides present and past confirmation of identity and it can be easily stored and generated.

PKI may ensure secure communication between A and B and authenticate each party by reference to key technology. However, there remains the risk that A is not genuine and that an impostor is using A's public key. Addressing this risk involves two more keys: the public signature key and the private signature key. When a document is digitally signed and transmitted, A's private key forms an attachment which includes a partial copy of the document being sent, together with a certificate from a certification authority to confirm the identity of the sender. B will obtain the public key from the certification authority and can check the signature.

Digital signatures are recognised by the Electronic Communications Act 2000 and are intended to have the same legal effect as a handwritten signature. The object is to identify unequivocally a party to the message in a document. An algorithm – a private key tied to the user's identity – is embedded in the message, recognisable as the sender's signature only by the recipient's key. In addition to the digital signature which authorises the origin of a communication, there is also a time stamp which verifies the time of the communication and the time of receipt.

Certification and registration authorities

A recognised and trusted infrastructure is required to support PKI. Organisations known as certification and registration authorities fulfil various functions in this area. They are recognised under the Electronic Communications Act 2000.

A certification authority is responsible for the management of certificates for certificate users and may also be responsible for generating key pairs for the encryption process. Its primary role is as an independent and trusted authority for authenticating the relationship between individuals and their public keys.

A registration authority is a representative of a certification authority and can undertake some of its management functions. These might include registration of parties for entitlement to certificates, or administrative functions undertaken by a certification authority such as updating certificates.

The certificate bears certain authenticating information. It contains the name of the certification authority and the public key holder. It also contains the holder's public key and is digitally signed with the certification authority's private key. Various types of information are included in the certificate; for example, the period of its validity, the range of transactions for which the certificate is valid and the identity and description of the certificate holder.

In order to understand how the procedure works, it is helpful to return to A and B. If A wishes to acquire a public key certificate, application is made to a certification authority. When A sends a message to B, the certificate is also sent and this confirms to B that A is genuine and that the certificate is current.

The certification process resolves two further uncertainties. A's authenticity is confirmed because A's public key is validated by a certification authority. B, therefore, knows that the message that purports to come from A does, in fact, do so. Repudiation is impossible, because the certification of A's public key means that B can be satisfied that A is the actual person from whom the communication originates, and, therefore, the contract cannot be repudiated, at least not without the risk of some legal liability on the part of A.

Products and services

Certification software may be installed 'in-house' where an enterprise wants to control its use of public key encryption, and take sole responsibility for the issue and use of certificates in its operations. As well as being employed externally, there is also the potential for securing internal privacy. An example of a PKI solution, beTRUSTed, can be seen on the website of Entrust (*www.entrust.com*).

Smaller enterprises are less likely to use an external certification authority, because PKI can be too complicated for small business and consumers. However, certification authorities can offer PKI services to communities without the problem of the infrastructure.

The cost of an in-house PKI will be significant in terms of the resources, skills, organisation, administration and human resources required. Encryption will be employed almost exclusively for the benefit of clients. Organisations must weigh up the value of the clients against the cost of importing the technology and training. There is also the question of legal liability arising in favour of any party who, in the ordinary course of business, relies upon a certificate which is subsequently found to be defective.

Digital certificates are published in directories. These hold a record of certificate notifications, revocations and suspensions. The digital certificates contain individuals' public keys. An individual proposing to send a message refers to the directory for the recipient's public key and digital certificate.

Encryption keys need careful storage. They should not, for instance, be left exposed on the organisation's web server. Organisations providing such services include Thales (*www.thalesgroup.com*) of which the original providers, nCipher, are now part. The Regulation of Investigatory Powers Act 2000 (*see Chapter 9*) enables authorities to require encrypted messages to be decrypted in certain circumstances. For this reason also, the secure storage of encryption keys is essential.

As an alternative to PKI, some communities rely on trust and good faith in the use of encryption technology for those with whom they wish to communicate securely. This avoids the complex administrative framework of certificated PKI, as well as the cost and impracticality for small organisations. An example of a software product that serves such 'communities of trust' is Pretty Good Privacy (*www.pgp.com*), now part of Symantec.

Some suppliers provide Cloud-based encryption services. In this case, encryption management is performed by a supplier organisation which provides encryption software, manages the encryption keys, administers encryption policies and provides records, reporting and administrative services on an on-demand basis. An example of this is the service offered by Proofpoint (*www.proofpoint.com*).

At present, the industry is self-regulated. Tscheme Ltd. (*www.tscheme.org*) is a United Kingdom organisation with a membership of leading business, professional and commercial organisations. It is a self-regulating non-statutory body established for the approval of organisations operating electronic trust services. Such organisations are called trusted service providers.

Certification and registration authorities, and trusted service providers, should be distinguished from PKI vendors, which, it is suggested, are organisations selling PKI hardware or software infrastructures. They may be organisations that provide PKI for authentication within a company that is only used internally, or part of a complete solution. They might also provide certification and registration authority services.

The PKI Challenge, launched by the European Forum for Electronic Business (EEMA), ran from January 2001 to

April 2003 and introduced solutions to PKI interoperability problems arising throughout Europe.

Concerns about digital signatures have been expressed, and have yet to be fully resolved, over the potential for a digital signature to fall into the hands of a third party and the transfer of risk of fraud to the owner of the signature.

Information and data security

Information and data must be properly stored with access controlled according to the value and sensitivity of the information at risk, and the qualifications and entitlement of personnel concerned. Over networks, in particular, it is necessary to identify the information that needs to be secured and ensure that access to the information is carefully controlled. Information must be authentic, valid and pure; that is to say, free from distortion through tampering or attack.

Information security levels

Information security needs consideration at various levels. This will depend upon the nature, size and structure of the enterprise. There are three aspects of security:

- **General defensive capability**: this means the general awareness of the potential for external and internal attacks on the organisation's network.
- **Defence in depth**: this involves security at desktop level, security at network level and security throughout the system.
- **Vigilance**: this involves staff training and regular vulnerability assessments.

This approach involves awareness and participation by all employees. Security vigilance is particularly important. A security breach may just as easily occur at junior or subordinate level as it might at senior level. No matter how sophisticated the systems, nor how well briefed those at senior management level, if employees are either insufficiently aware or inadequately trained, the security system will not be effective.

A typical example of one of the most common data security incidents surrounds the use of laptops and portable media. Frequently, these are left in public places by accident, but may also be the subject of theft.

Portable media should always be encrypted as a basic security measure – it is suggested to the requirements of the Federal Information Processing Standard (FIPS) 140-2 issued by the National Institute of Standards and Technology. This standard prescribes four levels of security, level one being the most basic and level four being the most advanced. The standard is supported by a testing and validation process, although it does not prescribe the level of security for any particular application.

Framework

There must be a framework governing the environment in which the information is stored and accessed. This applies both to those inside and outside the organisation. An information security framework can be likened to a hard outer shell, inside which is an internal shell that protects the organisation's data.

The electronic environment is collaborative and new alliances may involve outsiders having access to internal systems. In some professional services, for instance, IT systems allow clients access to organisations' internal systems to track the progress of ongoing instructions or projects, or to obtain up-to-date billing information.

Firewalls

Firewalls are computers which guard access to a network, block malicious files, and prevent unwanted intrusion. They are the principal defence mechanism for preservation of information security and operate by means of the Internet protocol breaking down data into information packets, with routers directing the information packets to the correct source. Once an organisation decides what kind of material is to be allowed into and out of the network, a firewall is configured appropriately.

Firewalls protect information entering and leaving the network, and within the network itself. There should be a firewall between the web server and the internal secure network. The web server sits in isolation with firewalls on guard externally and internally. This isolation area is sometimes referred to a demilitarised zone (DMZ). While information exchanged with the outside world needs careful control, some internal information might need to be sent externally, requiring conversion into a form that will not compromise the internal secure network.

Depending upon the configuration of the firewall, access can be allowed to certain internal information for certain external parties, and to internal parties for certain external information. If the firewall has been correctly programmed, only 'permitted party' communications should be able to penetrate the firewall and pass through. If firewalls are not properly configured, the risk to the organisation is almost worse than if there were no firewall – because of the temptation to assume that the mere existence of the firewall is the complete solution to information insecurity.

In some situations, firewall protection may be limited. For instance, e-mails with attachments that masquerade as program updates but which, in fact, contain viruses may not be prevented from entry, despite the presence of a firewall. Other instances might include the transfer of files or software infected with a virus. There are many different viruses, and numerous new viruses being devised and discovered regularly.

A firewall operates as a sole gateway for the purposes of identifying unauthorised intrusion and protecting information. However, in the case of a network, each access point is potentially vulnerable to attack and must, therefore, be protected.

Although firewalls can be operationally complex, there are a number of benefits beyond their security function. The monitoring and auditing procedures involved in firewall administration can provide valuable management data.

A firewall either allows complete access or prevents any access. The flexibility of the electronic business model demands a position somewhere between the two extremes. One approach is a combination of firewalls through which the party seeking entry to the system is able to pass until reaching the specific level of information to which access is allowed.

Using this formula, the ‘black and white’ approach to the deployment of firewalls is avoided and a degree of flexibility can be introduced which can still be controlled by the organisation seeking to protect particularly sensitive information. Firewalls can be deployed for both intranets and extranets, effectively creating a virtual enterprise network.

Firewalls, however, have a number of limitations. Sophisticated threats, increasing traffic volumes and the cost and time of management are all significant challenges. Stonesoft (*www.stonesoft.com*) has developed its Stonegate 'Next Generation Firewall', which integrates the functions of security, availability, scalability and management. Details can be found in its white paper: *The Evolution to the Next Generation Firewall*.

Passwords

Passwords are commonly used but have a number of weaknesses that were identified earlier. If their use is widespread and viewed favourably in organisations, it is sensible to adopt a common approach by all who use them.

If, therefore, it is management policy that passwords should be used, there are some useful guidelines to observe. They should be as long as permitted and employ as many keys as possible. More effective are pass-phrases. Useful tips when employing these include:

- the use of upper and lower cases randomly;
- the mixing of numbers and letters;
- deliberate misspelling of words;
- regular changes of procedure;
- avoidance of words with personal associations;
- avoidance of passwords recorded in writing.

Increasingly, organisations are moving towards technology-driven passwords in the form of keys requiring two-factor authentication or the generation of random passwords which expire by the effluxion of time and require renewal. Some alternative password solutions involve biometrics.

Viruses

With the proliferation of viruses, and the potential damage that can be caused, the installation of software is essential to protect information. While firewalls offer some protection, in certain cases viruses can still infiltrate under the guise of acceptable software, containing a damaging element which is released once inside the system.

Anti-virus solutions may perform some or all of a number of different functions, for instance they may:

- act as a device for warning of suspicious activity;
- look for malicious code;
- warn of unexpected system changes;
- act as an agent to identify viral signatures.

The extent to which an organisation achieves these objectives as part of its virus defence strategy depends upon its preferences and its risk assessment. It seems sensible, however, to install software that will as far as possible provide most, if not all, of these functions.

There are numerous proprietary anti-virus software products but anti-virus software will be ineffective, unless selected and installed appropriately for the organisation it is intended to serve.

The installation of virus protection software is the responsibility of those with appropriate skills in the IT department. Anti-virus software will never be a complete solution because of the number of new viruses that are constantly being created.

Returning to the risk assessment principles described earlier, the real issue to address is how to reduce the threat to an absolute and acceptable minimum, and minimise possible damage.

Intrusion detection and prevention systems

Firewalls control access to systems and information. Anti-virus software attempts to prevent damage to systems and information. In an attempt to avoid the consequences of hacking activities, another mechanism is available – intrusion detection (IDS) or prevention systems (IPS). The aim of these systems is to identify unauthorised use, both internally and externally. The idea behind the solution is that the intruder's course of action will be easily distinguishable from that of an authorised entrant to the system.

Intrusion detection and prevention systems can seek out known problems such as defective passwords and also act either as scanners, tracing events as they occur in the form of abnormal activity, or as agents for detecting hostile activity. These systems check internal network operations and traffic. This enables a track to be kept of attacks and other illicit activity, as well as the origins of attacks themselves.

In assessing whether these systems are appropriate, organisations should consider the resources to be protected and the importance of those resources to the operation of the organisation and its clients or customers. As these systems require skilled and knowledgeable personnel to be deployed to manage the installation, management issues also arise.

Returning to risk assessment principles, there is an obvious need to balance cost against the likelihood of risk. A large organisation with a vast network and numerous access points, with many at remote locations, will be far more vulnerable than a small organisation with only two or three networked computers. Resources are also an issue. The monitoring and analysis of incidents that the system detects will be labour intensive and demand personnel time.

IPSs block or prevent activities identified by IDSs and allow legitimate traffic. The technology may be regarded as an extension of IDS technology. An IPS should be programmed to minimise the rate of false positives.

Penetration testing

Penetration testing is a method of establishing the quality of security provided within a network or system. A number of tools exist that are specifically designed to identify weaknesses and vulnerabilities within a network or a system. Specialists are usually employed to undertake penetration testing if the results are to be relied upon for expenditure to increase the quality and degree of security.

External penetration testing involves probing a site and checking, for example, the security and configuration of firewalls. Internal penetration testing involves examining internal activities and is an important checking mechanism, particularly since vulnerability most frequently arises from internal sources. An example might be the need to check any patterns of use in connection with newsgroups to which there is an outside connection.

Password testing involves an audit of password application and use and checks the quality of management surrounding the employment of passwords, both internally and externally.

Databases

Database security is a highly specialised area. However, observing certain high-level principles can significantly help in the safe preservation of data. The following steps are suggested:

- identify data categories;
- assess the risks attaching to each category;
- implement an identity and access management strategy;
- implement measures (such as encryption) to address and manage risks;
- regularly monitor, audit and review.

Networks

The emergence of the global market as a result of the development of Internet technologies has had a significant impact on the infrastructure of many organisations. IT networks that were once relatively confined are now frequently extended over global locations, both nationally and internationally.

Extended networks

Pressure arises on network management, not only from geographical spread, but also from the employment of a wide variety of portable and mobile devices on which vast amounts of confidential data can be stored and transferred seamlessly from system to system. Examples of these devices include: laptop computers; mobile devices, such as Blackberrys and smartphones; iPods; memory sticks and CD-ROMs. They are most frequently employed by personnel who may be remotely located and from time to time need to transfer data from such devices on to corporate networks.

The expression given to the artificial and uncoordinated extension of networks in this way is 'deperimeterisation'. This means that the traditional perimeter boundary of a network (usually the desktop computer) is extended by a proliferation of other devices, all of which extend network perimeters.

The general expression for the securing of various entry points to an extended network is 'end-point security'. End-point security involves securing the particular device at the perimeter of the network – for instance mobile phones, laptop computers or memory sticks. As every network is different, this raises different security issues, in turn presenting significant problems for network administrators.

There are various solution providers who can supply software to address end-point security issues – see, for instance, Symantec's suite of end-point protection software for servers, desktops, laptops and mobile devices, which also includes network access controls and end-point encryption (*www.symantec.com*).

Reported examples abound of the loss of portable devices loaded with vast amounts of data. At the same time, the flexibility of portable devices enables dishonest personnel to store and remove large quantities of corporate data without authority and frequently without any danger of discovery until after the event.

Real challenges exist for organisations wishing to protect themselves from these vulnerabilities, with enforcement of use policies, securing data on portable devices and prevention of data loss, while at the same time maintaining user productivity. While firewalls may protect traditional networks, the range and complexity of portable devices make firewall protection impossible.

One strategy adopted to address the problems posed by portable devices has been to create special users or groups who are assigned specific encryption keys and are authorised with access to the same data. In a white paper entitled *Extending enterprise security beyond the perimeter (2008)*, Secuware (www.secuware.com) explains how its C2K solution creates computer profiles to govern the use of specific devices, and user profiles that authorise access to data by specific personnel. Devices or users which do not conform to prescribed profiles will be denied access to protected data. In this way, it is claimed that the organisation can control what device and encryption procedure is to be adopted and which users or groups can access the data.

Wireless networks

Increasing numbers of organisations are now deploying wireless networks for internal use by personnel and for use by external sources, such as clients and strategic allies.

The principal vulnerability of wireless networks lies in the ability of hackers to gain access to the network from rogue access points which exist without the knowledge of the wireless administrator. Frequently, these access points may be created by the hackers themselves.

Some measures can be taken to address wireless network security. Routers should be programmed to the WPA2 standard, currently the highest level of security available. Passwords should be complex, difficult to decipher and changed regularly. Encryption software, such as PGP and Truecrypt, should be employed where possible.

Various solutions are available to alert administrators to the possibility of unauthorised attempts to access or penetrate a wireless network. These tools are generically referred to as network scanners or sniffers, for instance NetStumbler (*www.netstumbler.com*). The methods they employ involve identifying and alerting the administrator to dubious or inadequately protected access points. Network scanners also perform other tasks, including identifying hardware and system vulnerabilities and interference.

Some devices, such as Bluetooth, Blackberry and certain PDAs, have built-in security mechanisms, in which case a check should be made to ensure network compatibility. However, these security measures do not necessarily offer protection against viruses and other malware for which traditional anti-virus protection should be obtained.

Virtual private networks

Earlier, a number of risks were identified as arising from personnel accessing systems and networks from remote locations while networked to the organisation. One solution is the creation of what has become known as a 'virtual private network (VPN)'. The demand for VPNs springs from the increasingly global spread of organisations and the consequent need to connect employees to the organisation. A VPN has a flexibility of application in a number of different environments that, in many respects, makes it an attractive proposition for firms whose offices are geographically spread, both nationally and internationally. A VPN may be used in connection with the firm's intranet, extranet and remote-access employees. Examples are the solutions offered by Novell (www.novell.com).

The principal technologies comprise three devices: first, the installation of a personal firewall on the remote device to provide protection; second, the installation of regularly updated anti-virus software; and third, the installation of encryption software.

Intranet VPN

An intranet VPN allows secure communication among internal departments, branch offices and the principal office of an organisation. The important features are that sensitive internal communications can be protected by means of encryption; information and documents can be securely stored; and the network can be constructed to accommodate growing numbers of users and offices.

Extranet VPN

An extranet VPN connects the organisation with strategic allies, clients and suppliers, as well as other agencies. The attraction of this technology is that the employment of commonly recognised security standards by all those linked within the extranet generates confidence in the security of communication and information passing between them. Traffic using the extranet can be controlled and monitored.

Remote access VPN

A remote access VPN connects the firm's network with remote mobile employees. The important feature of this technology is that strong authentication processes can be introduced to ensure that there are no issues as to the identity of a remotely placed employee communicating with the organisation. Management controls can be centrally operated and, where necessary, additional employees can be accommodated.

Operating a VPN

A VPN creates what are sometimes termed secure tunnels between networks connected over the Internet. To this secure tunnel is added a capability for authentication and encryption. The most common methods of authentication are passwords; uncertificated public and private key encryption; and certificated public/private key encryption.

Identity and access management

The competent management of both the identity of personnel seeking to access a network and the categories of data to which access may be authorised is critical to the adequate protection of an organisation's confidential data. Identity and access management (IAM) is now a significant governance issue in terms of information security.

The objectives of a formal IAM scheme are to provide a straightforward, transparent and methodical approach to the management of personnel and the data to which they may have access. Not only should this approach bring about efficiencies in terms of improved service, better organisation and lower costs; more importantly, the level of control that an organisation maintains over its data is an important governance principle in the context of risk management and regulatory compliance.

Security concerns are addressed by automating and simplifying the categories of personnel and the classifications of data to which they are permitted access. Compliance concerns are addressed by transparency and clear allocation of permissions to named users or groups of users. Risk management concerns are addressed through the comprehensive application of an IAM scheme at all levels of the organisation. Improved business performance is achieved through a clear understanding of the roles, responsibilities and accountabilities of users or groups of users in respect of the data to which access is authorised.

It is common for IAM schemes to include a category for privileged users – privileged user access – for instance, by function (system/database administrator) or seniority (CEO, CIO, or COO). Some commentators suggest that overuse of this category risks the abuse of IAM schemes.

CA IT Management Software Solutions has commissioned a helpful independent report, *Privilege User Management,* from Quocirca Ltd. on the subject. CA offers two IT solutions: *CA Security Management* and *CA Access Control* (*see www.ca.com*).

The process for establishing an IAM framework will vary between organisations because each organisation and its respective data protection requirements are different. However, some general principles can be identified. The organisation's policy document should define:

- the governance principles on which the IAM framework is based, its purpose and its intended objectives;
- the legal, regulatory and compliance provisions it is designed to address and any industry codes and standards that support compliance;
- procedures to be adopted for compliance with the organisation's IAM scheme;
- the categories of users and groups of users who are subject to the IAM scheme;
- any technologies deployed within the organisation that support compliance with the scheme.

Various solutions are available for developing IAM schemes. Microsoft® offers the Access and Management series which provides a template for an IAM scheme (*http://technet.microsoft.com/en-us/library/cc162924.aspx*).

General information and data control

E-mail content

Organisations should monitor and control potentially damaging e-mail. The ideal solution is an automated system that monitors e-mail, and detects and quarantines questionable messages for further review. Conventional keyword searches do not identify underlying meaning, but simply search for words or phrases that indicate unacceptable content. The result can be that numerous meaningless search results are generated. An ability to discern between questionable and innocent messages is required.

Software that is intended to monitor and control e-mail content should have certain features. For instance, there should be mechanisms to prevent the leakage of confidential documents and data, and to filter e-mail with inappropriate content by preventing it from entering or leaving the organisation. Linked to this is the need to block attachments with particular file types and to limit the size of attached documents that can be sent or received. There should also be a capability to add legal disclaimers to outbound mail, or corporate messages to inbound mail. Some software is able to block and quarantine, or even delete e-mail from specific sites. It should be possible to remove quarantined e-mail to a quarantine area for further review.

E-mail access

Access control involves authorising who can send e-mail and to whom. Software is available to enable controls to be applied to individuals, groups or entire messaging domains, authorising communications at specifically selected levels. By combining this with content control, it becomes possible to direct who sends what to whom and, in so doing, prevents the loss or unauthorised distribution of secure information and supports IAM policies.

E-mail sensitivity

The ability to control how sensitive information is handled is an essential feature of preserving information security. It is also a compliance requirement of the DPA, which specifies that data which is defined by the DPA as 'sensitive' requires special protection. Messages can be given security labels, and software is available to perform checks that will denote the sensitivity of the information being conveyed.

Examples of suppliers of software enabling such control of e-mail content include Websense (*www.websense.com*) and Omniquad (*www.omniquad.com*).

World Wide Web controls

There are four principal issues with which an organisation will be concerned in respect of access to, and use of, information obtained from the Internet in the workplace. The issues to be addressed are: control of access generally to the World Wide Web; control of access to specific sites which, if accessed, may expose the organisation to legal and professional sanctions; control over the downloading of material; and monitoring those with access to the Internet.

There are a number of software solutions able to detect and control inappropriate use of the Internet in the workplace. It is important to appreciate, however, that introducing technology to address these types of risk also requires the organisation to have in place appropriate guidelines and policies for their use. Because the software allows monitoring and surveillance of users in the workplace, the use of this type of software also has legal compliance implications. These are discussed in the next chapter. The question of suitable policies to both guide and control employees in this respect is considered in Chapter 10. Websense also offers solutions to address these issues. An example of this type of solution is offered by Pearl Software (*www.pearlsw.com*).

Online payment systems

As online business develops, consumers expect organisations to accept payment for their services over the Internet. Several technology solutions are now emerging that protect information given by online purchasers of services and enable such transactions to take place in a secure environment. The dominant payment methods to date are credit and debit cards.

Credit cards

Credit cards are the most familiar method of payment and have a number of advantages. They are easy to use for both card merchant and consumer. Protection is available for the client under Section 75 of the Consumer Credit Act 1974, which gives the consumer certain rights of action against either the supplier or the card issuer in certain circumstances where loss has been incurred. There is also a clear audit trail of transactions performed.

The two principal technologies employed in connection with the use of credit and debit cards over the Internet are SSL and secure electronic transaction (SET). The processes underlying these technologies were discussed earlier.

Managing electronic payments

Most banks are willing to offer an organisation a merchant account to enable it to accept credit cards. If an organisation proposes to provide services electronically, it seems sensible to consider providing facilities for payment by credit card.

However, a number of questions need to be considered by an organisation proposing to provide online payment facilities for consumers. Although technology solutions are available for online payment, various operational issues arise. Are there sufficient personnel resources available to support the operation? Are there sufficient facilities to provide education, training, supervision and monitoring? Can the costs of establishing a mechanism for introducing an electronic payment system be justified on a cost-benefit analysis in terms of the fees payable, the technology systems to be installed and operated, and the anticipated marketing benefits?

One useful barometer is whether or not the organisation is already offering any form of electronic payment facilities. If so, it may conveniently carry on. If not, the organisation needs to consider whether it has a sufficiently large number of clients who would find the service of value to justify the cost of setting up and operating of the facility.

In respect of invoicing or billing procedures, software is now available that will deal with invoice completion and delivery, whether to clients or suppliers. The software is developed to standards set by the Business and Accounting Software Developers Association (*www.basda.org*).

There are a number of technology solutions available for the adoption and management of online payment systems including:

- Cybersource (*www.cybersource.com*);
- Netbanx (*www.netbanx.com*);
- PayPal (*www.paypal.com*);
- RBSWorldPay (*www.rbsworldpay.com*).

The selection of solution providers listed above gives an idea of the types of electronic payment products and services accessible to organisations of all sizes and types. A visit to their websites provides full details of the available services and the terms and conditions that apply.

The PCI Security Alliance provides services to members of the payment card industry, for instance retailers, e-commerce organisations and organisations that must achieve compliance with the PCI Data Security Standard.

The PCI Data Security Standard has been developed by the PCI Security Standards Council and provides controls around data to address potential credit card fraud (*see www.pcisecuritystandards.org*). Essentially, the standard involves the taking of certain steps to protect the payment system operated by a provider of goods and services. The principles addressed by it concern:

- secure network infrastructure;
- protection of confidential cardholder information;
- adequate protective measures;
- access management procedures;

- rigorous testing and monitoring;
- an information security policy.

The standard specifies within these categories the types of measures needed in order to demonstrate compliance. Compliance with the standard is invariably a contractual requirement carrying legal responsibilities.

Business continuity

The prospect of attack whether by malicious code in the form of a virus, or from external or internal hackers raises the possibility of a 'denial-of-service' incident should, for some reason, the deployed firewalls or anti-virus software fail. 'Spamming' is a potential threat to business continuity because when sent in large volumes, spam e-mail can overload systems and networks to the extent that they are unable to function.

Software is available to combat spamming. One example is: the Mail Abuse Protection System (*www.mail-abuse.com*) owned by Trend Micro.

The need for business continuity planning arises from an organisation's responsibility to its clients and the need to comply with requirements imposed by legislation, practice rules, regulators and insurers. Such planning requires resources in terms of adequacy of finance and the appointment of staff with appropriate skills. As a protective, as opposed to an income-producing, strategy, it is not likely to be popular. It is, therefore, important that the risk assessment and management strategy evaluate the proportionality of the cost against the risk to be addressed.

In formulating a risk policy, there are some useful questions to ask. What would happen to the organisation if there was a significant interruption to the functioning of its IT and Internet technology systems? Have the various IT functions been assessed for risk and prioritised? Are there any documented plans in place for testing and revising? Are staff aware of any plan in respect of their roles and responsibilities?

Considerations

In terms of Internet technologies, there are likely to be implications for business continuity in three areas: the functioning of the network or systems, both internally and externally; access to, and preservation of, data; and the availability of key personnel.

Networks and systems

Most systems will be networked or distributed. In the event of discontinuity, the question to be considered is whether it will be possible to reconstruct the network to the original configuration within a reasonable time and at a proportionate cost. Many organisations use back-up tapes to support their systems. The question arises as to their adequacy, their management and the reliability of their continuing operation. Are plans in place, tested and reviewed, and has adequate time been allowed for training?

The ideal enterprise has a business continuity plan to which it can devote appropriate resources in terms of cost and time, supported by suitably skilled employees to test and implement a suitable recovery plan. However, many organisations do not have the time, financial resources or personnel to take control of business continuity plans. In many cases, the most practical solution is to outsource the responsibility to an expert hosting service.

Outsourcing involves sharing the responsibility between the supplier and the organisation. The supplier needs an appropriate brief as to the organisation's requirements and should be able to assist with risk assessment, planning and management by providing the right skills within defined agreed time limits. Outsourcing is a continuous process and the organisation will need to allocate resources on an ongoing basis as its use of the Internet technologies develops.

Data

Data should be backed up on a regular, usually daily, basis. There is a strong argument for identifying a facility that will back up data off-site in the event of a physical or technological threat. It is important to remember that in addition to business continuity issues, the safe storage and preservation of data is also an obligation under the DPA.

Adequate data storage is essential for business continuity. This is all the more important because data is scattered all over an organisation in servers, desktop computers, laptop computers, memory sticks, mobile phones, iPods, CD-ROMs and DVDs. Furthermore, there are numerous different types of data held, for instance, about personnel, clients and business partners.

Three technology approaches are involved:

1 **Network attached storage (NAS):** this integrates with a local area network.

2 **Storage area network (SAN):** this can be scaled for use in terms of performance and capacity.
3 **Direct attached storage (DAS):** this comprises a dedicated server with its own storage resource.

For organisations unwilling to risk installing solutions that have not been developed to recognised standards, the alternative option is to outsource the function. Some issues in respect of outsourcing are considered in the next section.

Data back-up requires careful thought. Although a technology issue, it is also a management issue. Typical issues which an organisation should address include ensuring that data can be retrieved with the minimum of delay; the need for a data storage infrastructure that caters for increased business activity; ensuring that suitable encryption solutions are applied to all stored data; ensuring that adequate reporting, auditing and monitoring processes are in place; and obtaining the services of a suitable supplier with an acceptable reputation in the market.

Personnel

In the event of business discontinuity, the firm will need to locate relevant staff as quickly as possible to address the difficulties that have arisen. In practical terms, contact details of key personnel should be safely stored and be easily retrievable, and such personnel should be engaged on the basis that they might be called upon out of conventional hours to cope with the event of business discontinuity.

Every organisation is different and will have its own priorities in such an event. However, some commonly applicable principles emerge:

- Plan for business discontinuity and consider how the collapse of the organisation's systems, loss of data and the absence of key personnel might be overcome.
- Be ready for such an event and have a business discontinuity plan in place and operative.
- Ensure personnel are familiar with the routine to be observed in such an event, in much the same way as a rehearsal for fire drill.
- Implement a regular system of personnel training and education, including reporting procedures.

Resources

There are numerous resources available for organisations requiring assistance and guidance in creating and developing business continuity strategies.

The Business Continuity Institute (*www.thebci.org*) was established in 1994 and certificates its professional membership with competence to perform business continuity management to a high standard.

BS 25999-1:2006: business continuity code of practice, BS 25999-2:2007: business continuity specification and BS 25777:2008: information and communications technology continuity management code of practice were discussed in the context of risk management on pages 150-151.

Global good-practice guidelines for business continuity management and related disciplines can be downloaded from the Business Continuity Planning Group's website.

Traditional outsourcing

A detailed examination of the IT outsourcing process is beyond the scope of this book. Outsourcing IT is a complex strategy which can significantly affect an organisation's position in the market. Legal advice should always be sought before embarking on an IT outsourcing strategy.

Outsourcing involves a supplier offering an organisation the option of transferring responsibility for the operation of a part or the whole of its IT function. The service may be a combination of standardised software, implementation, infrastructure, service and support, and is usually designed to meet the specification of small to medium-sized organisations.

A decision to outsource the IT function goes to the heart of any organisation's business strategy since IT is an essential business tool for every organisation. Entrusting a business tool that is so critical to the survival and success of an organisation to a supplier about whom the organisation may know little or nothing carries significant risk. Many IT outsourcing projects benefit both organisation and supplier, but almost equally as many result in project failure. A principal reason for the high incidence of project failure is neglect by the organisation in addressing and managing adequately the process and risk that surround the project – in other words neglecting to apply principles of governance.

The traditional IT outsourcing model involves a process of identifying how and why an outsourcing strategy should be adopted, within the context of the organisation achieving its objectives and business goals. There follow the processes of: supplier identification and selection; due diligence, tender negotiations; the contractual and service level agreement (SLA) processes; transition, implementation and change control through contract management; and termination.

Each of these processes calls for systematic and focused strategic, managerial and operational skills to ensure that:

- the most suitable supplier is selected;
- the contract supports the organisation's business goals;
- the SLA provides levels of service that will satisfy the needs of the organisation's end-users;
- the project is implemented efficiently and effectively.

As outsourcing projects typically continue for several years and can involve many millions of pounds, the need for the organisation to ensure the project's success becomes critical.

Underpinning the actual mechanics of the transaction, several other issues arise:

- the project must have top-level support or sponsorship;
- the interests of the stakeholders must be accommodated;
- the relationship with the supplier must be managed;
- strategic, IT, legal and compliance, operation and financial risks must be identified and managed.

IT outsourcing is a process of considerable complexity and significant risk, which has the potential to destroy an organisation either as a commercially viable entity or simply in terms of its reputation. It requires that principles of governance are not only understood, but adopted then rigorously applied.

Suppliers claim to provide a number of benefits. Assuming the service is provided to acceptable standards, there is no doubt that its availability relieves an organisation of its concerns in this area and can be both a relief from the burden of managing IT and also cost-effective. For relatively low initial investment, the organisation's responsibilities can be transferred with the assurance of maintenance and support from the supplier. The need to wrestle with the installation of new technology is removed and if adequate service is provided, there should be little or no disruption to the organisation's ongoing business activities.

Supplier

At present, there is no standard type of supplier recognised by a trade or industry benchmark, so care must be taken to ensure that the prospective supplier is not simply a software vendor. It is necessary, therefore, to establish the market reputation, technical competence and financial position of the prospective supplier, and particularly to ensure that the supplier has the skill and competence to provide the service required.

This will involve a comprehensive due diligence exercise. On a general level, the organisation should be satisfied that the supplier is experienced in the market, has adequate qualifications, and has a shared vision of the project.

More specifically, the organisation's due diligence exercise should check that the supplier is a strategically, technologically, legally, operationally and financially suitable partner with which to enter into a formal outsourcing agreement which may last many years.

Contract

Before, or as part of, entering into a contract for the supply of business continuity services, it may be a sensible precaution to consider implementation through a pilot scheme in the first instance. The contract contains the principal terms of agreement and is supported by the SLA, which sets standards of performance and the benchmarks for maintaining those standards. A check should be made to ensure that responsibility under any contract is not shared with another party. Related to this is the need to establish the precise extent of the liability of the supplier for loss, both direct and indirect, and the available remedies, together with any termination provisions. Payment methods should be scrutinised. In particular, there should be an awareness of hidden costs, which might be incurred through consultancy fees or the cost of integrating systems.

Service level agreement

The SLA defines the levels or standards of service required by the organisation. The objective is to obtain clear and consistent levels throughout the lifetime of the contract.

Typical issues to which particular attention should be paid include targets, measurable objectives, improvements and innovations, supported by appropriate monitoring and review processes. These issues are measured by a series of metrics included in the SLA.

The purpose of metrics is to ensure supplier compliance with the contract. Metrics should fall within the competence of the supplier and should be realistic or performance disputes will arise. They should be relevant, capable of analysis, and consistently applied; yet, at the same time, care should be taken to ensure that metrics are not too complex. Technologically, the organisation will wish to consider volumes, responsiveness, efficiency and quality.

Traditionally, this process has been conducted manually. However, in the case of multiple SLAs, the process can easily become cumbersome, costly, labour intensive and prone to dispute. Technology employed to date has included the *ad hoc* use of spreadsheets and Word documents, which have done little to simplify the process.

Software is now available to automate the service level management process. Oblicore (*www.oblicore.com*), now acquired by CA Inc (*www.ca.com*), has developed a solution which maps out the management of the portfolio of services and the levels at which they are provided.

The portfolio (or catalogue) of services defines the services to be offered, activates them and defines the standards by which they are to be measured. This is referred to as service portfolio management. The solution can also be programmed to manage the services levels, establishing the contract, defining relevant measurements, defining reports and setting performance parameters, all in collaboration with the supplier.

The benefits are significant. The process is standardised and the data gathering process is more consistent. Different metrics, for example performance, usage or financial, can be applied without difficulty. The infrastructure allows oversight network monitoring of all types of application and enables instant comparisons to be made with past performance.

Audit

The effectiveness of metrics can only be measured against a properly conducted audit. The audit process presents clear evidence of compliance, or non-compliance, with the contract and SLA. It is also a key risk awareness and risk management process. It can identify trends in performance that may lead to problems further ahead and can recommend controls that address inconsistencies. The potential range of an audit can stretch from minute examination of detailed metrics to discrepancies, investigation into fraudulent activity and even the activity of other management teams.

Technologically, the Board or Partners will wish to check the performance of the supplier's systems, applications and infrastructures; and if the contract is for a period of years, the frequency with which they are upgraded.

The audit may be conducted by the supplier but, although auditors are bound by professional standards, there is obvious potential for a conflict of interest to arise. Therefore, the organisation should consider obtaining the services of its own auditors to whom data for the purposes of the audit will be supplied by an audit team.

Data and security

In an IT outsourcing contract, it is likely that the organisation's data will be processed in some way by the supplier. It is, therefore, vital that the organisation satisfies itself that the data is secure and safe from interference, contamination and theft. Benchmark security standards are available against which to measure the suitability of the supplier in this respect.

BS ISO/IEC 27001 provides a benchmark for the management of information security management systems. It is expressed as being most effective for supplier organisations which manage information on behalf of other organisations as it can be used to assure organisations that their data is properly protected. This is considered in more detail on page 152.

There are also other relevant standards addressing third-party management of information security issues:

- BS ISO/IEC TR 14516:2002 information technology security techniques – guidelines for use and management by trusted third parties;
- BS ISO/IEC 27004: information security techniques: information security management: measurement.

Service management

Any outsourcing contract should incorporate a best-practice infrastructure for effective IT service management. The IT Infrastructure Library (ITIL) is widely recognised for providing comprehensive documentation on best practice for IT service management (*www.itil-officialsite.com*). Version 3 of ITIL presents the concept of life-cycle management from the design stage to identification of measurable service levels, operation, monitoring, support, data gathering and feedback, to renewal through continuous improvement.

Disputes

The contract should establish a procedure for dispute resolution, perhaps by graded procedures from informal, to alternative dispute resolution (ADR), to expert determination, to arbitration and litigation. In connection with this, it is sensible to establish escalation procedures for assistance in resolving practical problems and support issues

Cloud Computing

Cloud Computing raises the potential for a wide range of significant information security risks to arise. Given that the Cloud model can apply to most features of an IT infrastructure, for instance at infrastructure, platform and software levels, the extent of the potential security issues becomes readily apparent.

Areas in which technology risks might arise in the Cloud model include business continuity and disaster recovery; application security; storage technology; virtualisation processes; encryption procedures; data management; and data centre performance.

Presently, there are no easy answers to Cloud security issues, although some solutions are emerging, such as Commensus' (*www.commensus.com*) development of its Virtual Infrastructure Platform, which claims to offer a secure virtual solution for data stored and compartmentalised in virtualised servers.

Therefore it is incumbent on organisations outsourcing through the Cloud model to obtain confirmation of adequate performance of the following from the supplier.[7]

[7] *Outsourcing IT: a governance guide*, Kendrick R, IT Governance (2009).

Management information

- records of past performance levels;
- records of forecast performance levels;
- IT systems and server management records;
- governance and enterprise risk management infrastructure;
- processes for managing data.

Compliance

- evidence of ability to comply with the contract;
- evidence of ability to comply with the SLA;
- evidence of compliance with any relevant standards and methodologies;
- proposals for compliance audits;
- compliance with electronic discovery processes.

Security

- security of servers;
- security of networks;
- security of IT platforms and infrastructure;
- security of applications;
- application of intrusion detection and prevention systems;
- application of encryption technology and standards applied;
- business continuity and disaster recovery procedures;
- incident response and notification procedures;
- identity and access management procedures;
- data storage procedures.

Performance

- procedures for monitoring the service;
- procedures for reviewing the service;
- reviews of metrics and service levels.

No matter how thoroughly due diligence procedures are undertaken, the organisation can never be certain of the quality of the supplier's performance until operations begin. An organisation should, therefore, be rigorous in its assessment of a Cloud supplier before the contract begins.

Andrew Rose, Clifford Chance, regards the Cloud model as:

> … probably the most significant developing Internet risk in 2010. Effectively, this involves outsourcing IT into a shared commonly virtualised environment where confidential data is stored on remotely located servers, in many cases, internationally. This inevitably raises questions surrounding: the safety and security of data; the confidentiality of data; the auditing of the supplier's service; and the whereabouts of data; with all the subsequent compliance issues connected with international data transfers and access.

Cloud models can be both internal and external. Key areas an organisation should address include legal and compliance issues (in particular with regard to data protection); data security management; incident management; IAM schemes; and encryption and key management.

Two white papers have been published on Cloud security issues:

- *Cloud Cube Model version 1*, Jericho Forum, April 2009 (www.opengroup.org);

- *Security Guidance for Critical Areas of Focus in Cloud Computing*, Cloud Computing Alliance, April 2009 (*www.cloudsecurityalliance.org*).

Web 2.0 security

Web 2.0 is fast emerging as a recognised business tool in terms of its ability to generate and foster new business connections and to communicate rapidly and widely with a range of strategic allies, prospects and clients.

The principal components of Web 2.0 technologies currently comprise entities such as Wikipedia, FaceBook, YouTube and Twitter, and were initially designed for consumer interests. Now that organisations have taken a greater interest in these communication channels, a number of security considerations arise. Many organisations now allow their personnel to access Web 2.0 sites, mostly for business purposes but to a lesser extent, for social purposes also.

The nature of Web 2.0 is an extension, or development, of Web 1.0 in that Web 2.0 is interactive and this interactivity is the foundation of both its value and the interest supporting its rapid development. Underpinning this interactivity is the ability for users to access rich user-generated content through social interaction in the form of collaboration and information sharing. The initiative for the development of Web 2.0 is led primarily by the younger generation who frequently use social networking channels as their communication of choice, both socially and in the workplace. As the future of business and commerce depends upon their input and performance, it is clear that Web 2.0 technologies will not be a passing phenomenon.

Vulnerabilities

Like all Internet technologies, Web 2.0 technologies present a number of security vulnerabilities that were identified earlier. Hackers and criminals gain access in order to infect Web 2.0 sites or to assume false identities with a view to the commission of various types of fraud.

There are also significant threats to the safety, security and confidentiality of data posted on, or exchanged within, these sites, giving rise to the potential for major leakages of data. Furthermore, the interactivity that Web 2.0 encourages means that the flow of data, whether or not infected by malware, is both inward and outward and potentially distributable to large numbers of individuals.

The attraction of Web 2.0 technologies is that they offer access to large numbers of other users and their systems and are, therefore, an ideal source for exploitation in terms of propagating malware, distributing spam, creating 'botnets' or implanting spyware.

Security practices

While traditional devices, such as firewalls, anti-virus solutions and spyware identification tools have some use, the ease and speed with which data is exchanged through Web 2.0 technologies frequently mean that these solutions are unable to keep up with the changing nature of the threats presented by the continuous sharing and exchange of large volumes of data and information. Only a security solution that is able to respond to new threats in real time is likely to provide adequate protection in terms of the ability to monitor inbound and outbound communications, and the nature of the content being exchanged between systems.

Furthermore, where organisational policies allow access to, and participation in, selected Web 2.0 sites, any security solution must be able to identify and allow access to those and prevent access to other unacceptable sites.

Another issue is that of users accessing Web 2.0 websites from remote locations while on the legitimate business. It is just as simple for mobile devices to be infected with malware or to be a source of data leakage.

In summary, any security solution should be able to:

- control communications and content in real time;
- identify and prevent malware and data leakage incidents;
- discriminate between acceptable and unacceptable Web 2.0 sources;
- enforce a policy which includes all IT communication devices;
- provide monitoring, activity and performance reports.

Technologies are emerging to address these requirements. For instance, Websense (www.websense.com) offers two modules:

- **Web Security Gateway:** identifies sites and their content and addresses malware threats;
- **Threatseeker Network:** enforces behavioural protocols and identifies potentially unsafe content, including the encryption and decryption of content before entering the network.

Of course, security solutions alone are not a complete answer to data and security threats. Equally critical is the behaviour of those in the organisation using these and other Internet technologies. This aspect is considered in the context of operational issues in Chapter 10. Likewise, the employment and deployment of IT security solutions gives rise to a number of legal and compliance issues, which are examined in the next chapter.

CHAPTER 9: COMPLIANCE SOLUTIONS

This chapter considers key legal and regulatory provisions relevant to the use of Internet technologies for providing advice and services. A wide range of legal compliance provisions applies and they are categorised for easier reference and understanding:

- **Website management:** identifies provisions for consideration when using websites to provide information and advertise services.
- **Clients and services:** identify specific legislative and regulatory provisions governing the use of the Internet to provide services to clients.
- **Jurisdiction and applicable laws:** considers provisions governing the supply of legal services involving foreign jurisdictions.
- **Internet abuse:** identifies legislation that governs certain types of Internet activity that might expose directors, partners and staff to civil or criminal liability.
- **Monitoring and surveillance:** discuss legal provisions that apply to the monitoring of employee use of e-mail and the Internet in the workplace.

Website management

When providing services over the Internet, an organisation must address a number of issues relating specifically to the management of its website.

Domain names

There are many millions of domain names registered worldwide. A domain name is the way in which an organisation identifies itself on the Internet, both to its clients and other organisations. Steps must, therefore, be taken to ensure that the selected domain name is properly protected.

The selection and registration of an appropriate domain name involve two aspects. First, the selection must ensure that the organisation's professional image is both asserted and protected in a way that is most suitable. Second, the process must ensure that there is no infringement of copyright as regards existing domain names.

Levels

Domain names have a number of constituent parts. The principal constituent part is almost always the name of the organisation to which the domain name belongs. However, beneath the principal name are a number of other 'levels' of name, which define certain aspects of the organisation's status.

Top-level domain names are in two parts:

- the name of the country (for instance – .uk);
- the generic top-level domain (gTLD) name:
  - .com – commercial organisation;
  - .org – not-for-profit organisation;
  - .net – Internet network providers;
  - .edu – educational establishments;
  - .mil – military establishments;
  - .int – international treaty organisations.

Second-level domain names are usually assigned by country code administrators by reference to the country code. In the United Kingdom, such domain names end in .uk. Some of the more common examples are:

- .co.uk for commercial enterprises;
- .org.uk for organisations;
- .ac.uk for academic institutions;
- .gov.uk for government bodies;
- .net.uk for Internet service providers (ISPs).

There are two further levels of domain name, usually selected by the domain name registrant for specialist purposes. In 2000, the ICANN (*www.icann.org*), the body responsible for administering domain names, introduced seven new gTLD names:

- .biz – for *bona fide* business and commercial use;
- .info – available to all;
- .pro – for use by medical personnel and lawyers;
- .coop – for use by co-operative organisations;
- .aero – for use in the air transport sector;
- .name – for registration by individuals;
- .museum – for use by museums.

Further gTLD names were introduced in 2004: .asia, .cat, .jobs, .mobi, .tel, and .travel.

ICANN is in the process of introducing new domain names. These are expected to include brand and city names. Regular reference to the ICANN website is suggested.

Searches

The ability to include a brand name within a gTLD is especially significant for brand owners, who will be particularly concerned to ensure that no confusion or trademark infringements arise through competitors adopting a similar strategy.

When selecting a new domain name, it is sensible to submit searches in just the same way as a client is advised to conduct a search at Companies House. Domain name registration agencies can assist. Domain names are allocated on a first-come, first-served basis.

A search will identify whether any selected domain name has already been adopted, or whether a similar name has already been adopted which might cause confusion. Some countries have restrictions on the type of domain name that can be used. There is also the problem of ensuring that the selected name does not infringe another party's intellectual property rights.

As there are various categories of search, the domain name registration agency should be clearly instructed as to the type of search to be conducted. The broadest possible is advisable as registration of new domain names occurs continually around the world.

Registration

Nominet is the agency in the United Kingdom responsible for maintaining the register of domain names. Just as Companies House holds record of companies' names, Nominet maintains the database of 'uk' registered Internet names. It is not a governing body, but a public service for the Internet community.

However, provisions in the Digital Economy Act 2010 may result in the UK government taking additional powers to control the domain name jurisdiction.

Nominet's website (*www.nic.uk*) provides an overview of what is involved in the selection of a domain name, how to register, post-registration procedures, and changing domain names. While it is possible to register a domain name direct through Nominet, the agency encourages registration through an ISP, the majority of which are members of Nominet. A careful check should be made of issues such as fees, payment mechanisms and dispute resolution policies, if any.

Domain name registrations are valid for two years. Most ISPs will inform the organisation when the name is due for renewal. Transfers of domain names are also possible. Nominet has terms and conditions which are applied where changes are to be made.

Disputes

Because of the number of domain names being registered at any one time, there is considerable potential for dispute. Nominet provides a dispute resolution service, details of which are available on its website.

Nominet's website explains how the service operates, the rules by which it is governed, some of the definitions involved and how to use the procedure. Parties are encouraged to reach a mediated settlement. Nominet states that it claims no right to transfer a domain name without consent or an order of the court, or to offer legal advice or issue judgments over the correct use of domain names.

There are also other dispute resolution resources. ICANN offers a Uniform Domain Name Dispute Resolution Policy and details can be obtained from ICANN's website.

Cybersquatting

Cybersquatting occurs where an individual or organisation registers a well-known trademark owned by another individual or organisation as their own domain name. Two cases, which arose some years ago, are good examples of the problems that can arise. Both attracted wide publicity at the time.

In *Harrods v. Network Services (1996)*, an individual had registered the domain name Harrods.com with NSI in America. Harrods took proceedings for infringement of trademark and passing off in the United Kingdom courts. In summary, there was eventually a consent judgment in favour of Harrods. The decision first highlighted the practice of 'cybersquatting'.

The second case was *Marks & Spencer plc and Others v. One in a Million Ltd. (1998)*. This was regarded as an authoritative case on domain names and was taken to the Court of Appeal. The plaintiffs were leading 'brand name' companies and took action against the defendant, which had registered domain names incorporating their trademarks. The Court of Appeal upheld the plaintiffs' successful judgment in the High Court in 1998.

This is a simple summary of certain domain name issues. However, the adoption and use of domain names can raise complex legal issues and are frequently inextricably linked with brand names and trademark law and practice, both of which are beyond the scope of this book.

Therefore, any organisation seeking to obtain a new domain name should obtain specialist professional advice to ensure: the correct registration procedure is observed and that the intended domain name does not infringe the rights of any other organisations.

Website content

Legal liability may arise from information posted on a website, arising from a duty owed to those to whom information is given. This arises from the decision of *Hedley Byrne & Co Ltd. v. Heller and Partners Ltd. (1964) AC 465*, where the negligent provision of information gave rise to liability in law. Relying upon advice in such circumstances raises the question of whether it is reasonable that a client or casual browser should rely on the advice provided.

Whatever may be the legal position on the facts, the key issue is that organisations must be aware that inaccurate or misleading information may expose it to proceedings. Steps should, therefore, be taken to ensure that the content of the organisation's website complies with all relevant legislation, regulations and professional and commercial codes. Examples of some typical difficulties that might arise were described earlier.

To address these concerns, legal developments must be monitored. This applies in two respects. First, any advice provided on the site must be accurate and up to date. Second, there must be compliance with any legal requirements in respect of the use of the site to provide information, advice and services. Responsibility for updating the site might most conveniently be that of the IT manager. The organisation should identify an individual to collate the necessary information to ensure compliance and provide this to the IT manager. Published content should be checked and monitored regularly for accuracy and timeliness.

Website contracts

Although apparently a risk relating to clients and services and identified as such in Chapter 3, the issue of online contracts is also a website management issue, both in respect of the actions of personnel and the display of appropriate notices on the organisation's website. In deciding whether liability arises beyond the mere supply of information, the question arises as to whether the information constitutes an offer capable of acceptance, or an invitation to treat.

As services become more commoditised, websites routinely offer fixed-price services. It should be made clear to visitors to a website that (if it is intended to be the case) any services offered are intended as an invitation to treat (as in a conventional retail outlet), and are not a formal offer, the acceptance of which by a visitor will result in a binding contract. This might well form part of the terms and conditions (*see next section*) by which the organisation requires visitors to the site to be bound.

Terms, conditions and disclaimers

In certain circumstances, an organisation may wish to attach terms and conditions to the facility of viewing information or seeking services from its website. It is a general principle of contract law that terms and conditions must be brought to a prospective contracting party's attention before a contract is concluded and it is likely that this would be applied by English courts.

In practical terms, a visitor might be required to scroll down through a number of web pages before accessing the relevant terms and conditions. How can a website owner be sure that the terms and conditions have come to the visitor's attention? Probably the most obvious way, if lacking in user-friendliness, is to post the terms and conditions before the visitor can enter the full site area.

The same problem might arise in the case of linking. Terms and conditions attached to a primary site might also have relevance to a linked site. Steps will need to be considered with the owners of the linked site on the posting of relevant terms and conditions, so that they are correctly and adequately brought to visitors' attention.

One widely adopted solution to potential exposure to liability has been to post a disclaimer notice in respect of information on the site. It is a basic principle of law that such a notice must be drawn to the attention of the party to whom it is directed. Any disclaimer notice should, therefore, be prominently displayed, so that each web page carrying information or advice that is the subject of the disclaimer will be seen by the visitor.

The scope of a disclaimer notice is likely to be governed by the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Regulations 1999. Both seek to protect the consumer from the enforcement of unfair terms.

In broad terms, any attempt to disclaim liability in a contract is subject to a test of reasonableness.

Two general points should be borne in mind when considering the placement of disclaimers on a website. First, if an overall view of the site demonstrates a clear assumption of responsibility on the part of the site owner to the visitor for the validity and accuracy of information or advice on the site, the mere appearance of a disclaimer notice will not operate against the substance of the relationship. Second, any disclaimer should be carefully drafted, excluding liability for indirect, as well as direct, losses.

A website can be accessed worldwide and can, therefore, give rise to consequential liability for any information displayed. A global limitation or disclaimer will not be enforceable in practical terms because of the numerous jurisdictions in which it will fall to be interpreted, and so a residual risk remains whenever a disclaimer is posted.

Patchett and Patchett v. Swimming Pool & Allied Trades Association (2009) EWCA Civ 717 decided that where a visitor relied on website information which was found to be incorrect, the website owner owed a duty of care to ensure that the information was correct only if it was to be reasonably expected that the visitor would act on the statement without further inquiry. The disclaimer advised visitors to obtain more information before purchasing services from third parties listed on the website, and the website owner was not, therefore, held liable for inaccuracies. Further, one judge implied that interactive sites are more likely to owe a duty of care to visitors than passive sites.

Advertisements

The Advertising Standards Authority (ASA) (*www.asa.org.uk*) is an independent, self-regulatory body for non-broadcast advertisements in the United Kingdom. A new advertising code is effective from 1 September 2010. It has been produced following a consultation by the Committee of Advertising Practice and comprises a non-broadcast code (CAP code) and a broadcast code (BCAP code).

It is available for download from the ASA website and the principles are well established. Broadly, advertisements should be legal, decent, honest, truthful and responsible, and should not bring advertising into disrepute. However, the new code also introduces sector-specific provisions governing ease of use, protection for children, social and environmental issues, health, consumer protection, and specific activities (for instance, charities).

The ASA is not a law enforcement agency but adverse publicity will often result from infringement of the code. Certain cases may be referred to the Director General of Fair Trading. The International Chamber of Commerce also publishes a number of guidelines, codes and rules relating to marketing and advertising, to be found on its website at *www.iccwbo.org*.

The ASA regulates advertising claims in the traditional media but in the context of digital advertising only covers pushed advertising, such as e-mails and website sales promotions .The ASA has limited jurisdiction over website marketing, which is under consideration for extension.

Professional services organisations are often required to observe codes of practice in the course of publicising and promoting their services. Regard should, therefore, be paid to any guidance or best-practice advice offered by relevant professional bodies and regulators.

Linking

It is possible for web pages to contain links to other websites. These are termed hyperlinks. The name originates from the language – hypertext mark-up language (HTML) – that is used to perform the link to the other site. It is usually signified on the web page as a blue highlighted website address. Clicking on the address takes the visitor directly to the linked site. Linking can give rise to risks in respect of copyright and disclaimers.

Copyright

A typical example of how copyright issues can arise from links to other websites can be found in a case when the Internet was in its earliest stages of development. In *The Shetland Times v. Dr Jonathan Wills and Zetnews Ltd. (1996)*, the defendants published the Shetland News and linked their site to the plaintiff's site. The plaintiff objected as the defendants were bypassing the plaintiff's revenue-producing home page and linking directly to an interior page. As there was no indication that the plaintiffs owned the interior page, it could have seemed to a casual visitor that the internal page was that of the defendant.

This was a Scottish case and an interim interdict (injunction) was granted to the plaintiff. Before the case was heard in full, a settlement was reached. Broadly, the terms were that defendants should not 'deep-link' into the text of the interior pages on the plaintiff's site, but only to the home page, and that any links should clearly and appropriately indicate that the material originated from the plaintiff.

Further problems can arise under the Copyright and Rights in Databases Regulations 1997 (S I 1997/3032). These regulations are designed to protect databases into which considerable effort has been invested in their compilation. A basic website may fall within the definition of a 'database', particularly if valuable information is posted. In such circumstances, there may be infringement if there is unauthorised extraction or use of information posted on the site. It is, therefore, a sensible precaution to post a notice warning visitors of the danger of copyright infringement. Such a notice should at a minimum state:

- that any posted material is protected by copyright worldwide;
- whether or not permission is given to download and print off any material;
- the use, if any, that is permitted to be made of such material;
- that use for commercial purposes is prohibited without consent;
- a point of contact for permission.

For some examples of model notices, see *eCommerce: a Practical Guide to the Law,* Singleton S, Gower Publishing (2001).

Notices and disclaimers

These were considered earlier. Linking to another site can give rise to problems in respect of notices and disclaimers.

Following general principles, the most sensible course is to ensure that where a hyperlink is contained, the site to which it takes the visitor displays a disclaimer in appropriate terms which cannot escape the notice of the visitor when entering the site. Alternatively, the original site might contain a disclaimer in respect of any site to which it is linked, but this is subject to the test of 'reasonableness', as explained earlier.

Clients and services

This section identifies some key legislative provisions that govern both the supply of information and the services to clients. First, they provide a framework for the provisions of services over the Internet. Second, they provide consumers with certain rights.

Electronic Commerce Directive

The Electronic Commerce Directive's full title is Directive of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (2000/31/EC).

Commonly referred to as the E-Commerce Directive, it was adopted on 8 June 2000 and governs the formation of online contracts. It broadly includes:

- the general information to be provided;
- the provision of certain information to be provided for commercial communications;
- the sending of unsolicited communications;
- provisions applying to regulated professions;
- provisions applying to electronic contracts;

- the provision of facilities for out-of-court settlements.

The Directive became law with the introduction of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) on 21 August 2002, save for regulation 16 which came into force on 23 October 2003.

Since then, these regulations have been extended to include additional provisions by a number of 'extension' regulations in 2003 (SI 2003/115 and SI 2003/2500) and 2004 (SI 2004/1178).

Electronic Communications Act 2000

This Act came into force on 25 July 2000. Its origins lie in the Electronic Signatures Directive 1999/93/EC (*see next section*).

Two parts of the Act are of particular importance for electronic legal services. Part I relates to the establishment of cryptographic service providers for the provision of cryptography services to provide a framework for secure and confidential messaging. Part II establishes a framework for the legal admissibility of electronic signatures and the process under which they may be generated, communicated or verified.

The Act permits digital signatures to be admissible as evidence on questions of authority and integrity in respect of electronic communications or data. The courts will decide whether a digital signature has been correctly used and what weight it should be given against other evidence. As an indication of the universality of application, the Act sets out wide-ranging definitions of 'documents' and 'communications' in an electronic context.

The importance of the Act lies in its aim of facilitating the conduct of transactions – the delivery of services – electronically. Underpinning the commercial forces of consumer demand, together with the other elements already driving the demand for electronic services, the Act provides a framework for the development and provision of services, electronically.

Electronic Signatures Directive

The Electronic Signatures Directive's full title is Directive of the European Parliament and of the Council on a Community Framework for Electronic Signatures (1999/93/EC).

The previous chapter described the technological aspects of digital signatures and digital certificates. This Directive was published on 19 January 2000. Its aims were to prevent a patchwork of laws on digital signatures emerging from individual member states, to make the use of electronic signatures easier, and to establish criteria for their legal recognition.

The Directive tries to ensure that digital signatures are accorded legal admissibility on certain grounds and to establish benchmarks for signature creation devices and certificates used to support such signatures.

Voluntary accreditation schemes

Member states may introduce voluntary accreditation schemes to provide enhanced levels of certification services. Under the Electronic Communications Act 2000, a voluntary approval scheme was established – the tScheme (*www.tscheme.org*) – by a group of trade organisations which called itself the Trust Services Group.

Qualified certificates

Article 2.10 of the Directive provides for the issue of qualified certificates which provide confirmation of competence and integrity.

Advanced electronic signatures

Article 2.2 of the Directive introduces the advanced electronic signature, which is uniquely associated with the signatory and in certain circumstances may be seen as the equivalent of a handwritten signature.

The Electronic Signatures Directive became law with the introduction of the Electronic Signatures Regulations 2002 (SI 2002/318) on 8 March 2002.

Data Protection Act 1998

The open and insecure nature of Internet technologies makes personal data particularly vulnerable. Data protection principles and regulations aim to balance the right to hold information with the right of those about whom information is held to have the information properly handled. As organisations collect increasing amounts of information from and about consumers and other sources, data protection compliance becomes extremely important.

Data protection legislation originated with the European Data Protection Directive (formally named Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data 95/46/EC). In the United Kingdom, the DPA 1984 provided the original legislative framework for data protection. This was replaced by the DPA which came into force on 1 March 2000.

The ICO administers data protection compliance. There are various publications providing help and guidance on compliance issues. Current information and developments can also be found on the ICO's website at *www.ico.gov.uk*.

Parties

The Act introduces three parties: data controllers – who decide the way in which data is to be processed; data subjects – who are those about whom information is held; and data processors – who are responsible for processing the information.

Data

Data includes data relating to an individual who may be identifiable from that data, or from that data and any other data that might be in the possession of, or likely to come into the possession of, the data controller.

Requirements

Under the DPA, a data controller must (except in exempted circumstances) notify the ICO of his or her identity and provide specific information about the type of data and the reasons for its processing by the data controller.

Additionally, the data controller must process any data in accordance with the eight data protection principles stipulated in the Act, and provide access to processed data by the data subject, when requested to so, for the purpose of checking for accuracy and to prevent unacceptable processing.

Data protection principles

These are set out in the Act. In broad terms, the Act states that personal data shall:

- be obtained and processed fairly and lawfully with the consent of the individual except in certain circumstances;
- be obtained and held for one or more specified or lawful purposes which are stated in the Data Protection Register, and must not be used for any purpose incompatible with the purposes;
- be adequate, relevant and not excessive in relation to the purpose for which the data is held;
- be accurate and kept up to date;
- be held no longer than is necessary for the stated purpose(s);
- be processed in accordance with the rights of the data subject conferred by the Act;
- be the subject of proper security measures in respect of loss, damage, destruction and unauthorised processing;
- not be transferred outside the European Economic Area, unless the recipient country's protective measures comply with the EU Data Protection Directive.

Enforcement

Under Section 55 of the DPA it is an offence to knowingly or recklessly obtain, disclose, sell or procure the disclosure of personal data without the consent of the data controller.

In order to ensure compliance with the principles, the ICO has certain enforcement powers. These include: the service of an enforcement notice under Section 40 of the DPA requiring steps to be taken to comply with a specific principle; the service of a deregistration notice cancelling wholly or partly a user's entry on the Register; and the service of a transfer prohibition notice, preventing the transfer of information overseas if a potential breach of a principle is likely.

Criminal sanctions take the form of fines. For instance, in recent years, a number of law firms have been convicted and fined for failure to notify the ICO of their data processing activities.

Section 55 of the DPA has been extended by the Criminal Justice and Immigration Act 2008 by the insertion of Section 55A, allowing the ICO to serve a monetary penalty notice for any sum up to £500,000 in respect of serious breaches of the DPA principles.

This has been given effect by the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (SI 2010/31) which came into force on 6 April 2010. They prescribe a maximum fine of £500,000 for deliberately or knowingly seriously contravening the data protection principles. They also prescribe the details to be inserted in a notice of intent and a monetary penalty notice.

The Coroners and Justice Act 2009 also confers new powers of inspection upon the ICO and powers to issue assessment notices.

The ICO issued statutory guidance in respect of these powers on 12 January 2010, which can be found at *www.ico.gov.uk* via the 'Tools and Resources – Document Library – Data Protection – Practical Application – Detailed Specialist Guide' links.

Another issue has arisen as a result of widespread publicity surrounding the loss of data, particularly in the public sector. Currently, there is no duty under the DPA to report or disclose a breach of security involving loss of data. This is inconsistent with the legal position in a number of other countries, including EU countries. The UK government has indicated that the issue is under consideration but that it introduces a number of complexities which need to be addressed before any measures can be considered.

However, where a breach arises, the ICO advises that it is good practice to report this if there is likely to be serious loss or damage; the volume of data involved is significant; or sensitive data is involved. The ICO's Guidance on Data Breach Notification, dated 8 July 2010, details best practice and is complemented by Guidance on Data Breach Management, issued on 27 March 2009, both of which can be found at *www.ico.gov.uk* via the 'Good Practice – Data Protection Guidance – Good Practice Notes' links. The ICO advises that failure to report a breach voluntarily will be taken into account.

In practical terms, a legal duty to report may also arise under a contract, in which case relevant parties should be informed, so that risks are reduced. The parties concerned should be informed of the nature and volume of the data and when and how the breach arose.

Data processing

The collection of data through interactive websites is a potential marketing opportunity. Data may be collected by visitors to a site completing an online information form that asks for certain personal data. In respect of the first principle, the processing of personal data, at least one of the following must apply:

- the data subject must have given consent;
- processing must be necessary for performing a contract with the data subject;
- processing must be required to perform a legal obligation;
- processing must be necessary to protect the interests of the individual;
- processing must be necessary to perform public functions;
- processing must be necessary to pursue the legitimate interests of the data controller (unless prejudicial to the data subject).

Certain data is categorised as ‘sensitive’ under the DPA. Sensitive data involves the data subject’s racial or ethnic origin, political opinions, religious or other similar beliefs, trade union status, physical or mental health, sexual life, and commission of offences. Sensitive data calls for particular conditions to be met:

- there must be explicit consent by the data subject;

- processing should be necessary to comply with the law in connection with employment;
- processing should be necessary to protect the data subject's interests where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain consent;
- processing must be carried out by certain bodies which are not-for-profit and exist for political, trade union, philosophical or religious purposes;
- the data was made public by deliberate action of the data subject;
- processing must be necessary for legal proceedings, legal advice, or exercising the defence of legal rights;
- processing must be necessary for administration of justice or the exercise of any function by government or under an enactment;
- processing is necessary for medical purposes, undertaken by a health professional or an individual owing a comparable duty of confidentiality.

Transborder data

The development of global e-commerce and the establishment of international locations make it increasingly likely that data will be transferred abroad. It is, therefore, important to understand the regulatory provisions governing this activity.

Under principle eight of the DPA, there is a restriction upon the transfer of data to any country outside the European Economic Area, because certain countries are considered not to have adequate data protection measures in place.

Originally, the United States of America was included in this category. Negotiations resulted in the Safe Harbor Principles, under which data may be transferred to an organisation in the United States provided, in broad terms, that:

- the organisation informs the data subject of the reasons for collecting data, to whom data will be disclosed, and the processing controls;
- data subjects have the right to 'opt out';
- data will not be transferred to another country, unless it is a Safe Harbor subscriber, subject to the EU Data Protection Directive, or subject to another approved agreement;
- adequate data protection policies are in place regarding disclosure, protection and destruction of information;
- data is processed in accordance with the first principle;
- data subjects have a right of access to the information and to correct errors;
- a complaints and resolution of disputes procedure is published.

In 2001, the European Commission adopted standard clauses for data export, which many companies had already started using when contracting with parties outside the European Economic Area for the export of data. These involve a detailed contract which imposes obligations on the recipient of the data, similar to those under European Union data protection law.

The European Commission has now updated its model clauses for inclusion in contracts provided for the transfer of data overseas. From 15 May 2010, all such contracts should include these model clauses. Details of the

Commission's decision of 5 February 2010 on the standard contractual clauses can be found at www.europa.eu in the EUR-Lex section of the website.

Personal Information Online Code of Practice

On 7 July 2010, the ICO published a code of practice for the handling of personal information online – the *Personal Information Online Code of Practice*. It contains recommendations for handling personal information and is aimed at helping organisations with an online presence to negotiate areas of legal uncertainty by adopting good practice.

Typical examples of the issues addressed include: collection of individuals' details through online application forms, creation of visitor profiles by analysing online activity, collection of data for the purposes of marketing, and use of Cloud Computing facilities for processing personal data.

A recent development in EU law has caused concern to business and the professions. A proposal has been advanced that website hosts should obtain the consent of a visitor to the site when downloading 'cookies' which involve the visitor's personal data on to the visitor's computer. 'Cookies' are programs which collect data from website visitors, so that on subsequent visits, the visitor is provided with information and advice tailored to his or her interests.

This proposed legislation was approved on 26 October 2009 and requires member states to ensure that the storage of information or the gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent. EU member states have 18 months to incorporate this into legislation.

Privacy and Electronic Communications (EC Directive) Regulations 2003

The Privacy and Electronic Communications (EC Directive) Regulations 2003 came into force on 11 December 2003. In summary, the Regulations:

- require businesses to obtain prior explicit 'opt-in' consent before sending unsolicited advertising e-mail to individuals, unless there is an existing relationship;
- require the use of cookies to be brought to a recipient's attention so they may reject them;
- allow network operators and their partners to provide advertising services provided recipients consent and understand the data protection implications;
- ensure stronger rights for individuals to decide if they wish to be listed in subscriber directories.

By Regulation 30, anyone who has suffered damage through a breach of the regulations has the right to take proceedings against the person responsible for compensation.

Consumer Protection (Distance Selling) Regulations 2000

These regulations govern how contracts performed at a distance should be lawfully undertaken and came into force on 31 October 2000. The substance of the legislation is that consumers or clients must be given information about goods or services offered, receive confirmation after the purchase or supply, and be allowed a cooling-off period of seven working days.

A 'distance contract' is a contract for goods or services under an organised sales or service provision scheme at a distance. Certain contracts are exempt from the regulations. A 'consumer' is a person who is acting for purposes which are outside their business.

Distant communication is a means of communication that involves the presence of neither party. Schedule I of the regulations specifies these methods in detail and includes e-mail communications. Where a consumer is seen by an organisation for a face-to-face interview, the regulations do not apply. However, where contracts are concluded, for instance, by telephone, e-mail or fax, or by the provision of online legal advice or services delivered by an interactive website, the regulations will apply. The distinction is based upon whether or not a face-to-face meeting has taken place.

Information

Certain information must be given to the consumer prior to conclusion of the contract. This includes, for instance:

- the identity and address of the supplier;
- a description and price of the goods or services and delivery and payment details;
- the existence of a right to cancellation;
- the cost of using the means of distance communication where it is calculated other than at the basic rate;
- the period of validity of any offer;
- the minimum duration of the contract.

By Regulation 8, certain additional written information must be given prior to the conclusion of the contract, and in the case of services, during the performance of the contract.

The requirement for written information to be provided could be fulfilled by e-mail or even via a website, provided the provision was clearly notified before a contract was formed.

Cancellation

Regulation 10 provides for the right of cancellation. The period within which consumers can cancel contracts for services is seven days, or longer if certain information is not provided. An exception arises under Regulation 8(3), where written notice is given to the consumer that the contract cannot be cancelled once performance has begun with the client's agreement. A cancellation period of three months applies in the event of failure to give notice of the seven-day cancellation period.

Under Regulation 19, services must be provided within 30 days from the date when instructions were given. If there is non-compliance, the consumer must be informed and any sums paid reimbursed, unless the consumer agrees to substitute services or a revised supply date. If the consumer does not agree, the contract is cancelled and any sums paid in advance must be repaid.

Equality Act 2010

The exclusion of visually impaired visitors to inappropriately designed websites could result in legal proceedings against the website owner under the Equality

Act 2010. This received the Royal Assent on 8 April 2010 and the main provisions are effective from October 2010 and others in April 2011. Chapter 2 of the Act contains the provisions governing disability discrimination, which codify and replace the Disability Discrimination Act 1995.

The World Wide Web Consortium has developed a set of accessibility guidelines – the Web Content Accessibility Guidelines (WCAG). Version 2.0 was published on 11 December 2008.

This requires website owners, designers and developers to ensure websites comply with certain principles in the context of accessibility – perceivable, operable, understandable and robust. Within these principles are 12 success criteria. Each of the principles is assessed on the levels – level A, level AA and level AAA.

The requirements and standards are technically complex and are supported by documentation offering guidance on implementation. Various surveys conducted in the past have shown that many websites have not complied with even the basic level A standard.

Organisations seeking to comply should refer to the 'accessibility' section of the World Wide Web Consortium at *www.w3.org*.

Provision of Services Regulations 2009

These regulations came into force on 28 December 2009. They contain a list of compulsory information to be given to clients by most providers of services. Relevant 'services' include activities of the professions, among other business activities.

In summary:

- Regulation 7 addresses the contact details which must be made available.
- Regulation 8 requires certain information to be provided in respect of the organisation's professional activities, such as registration with a trade or professional body, contractual terms and conditions, the holding of professional indemnity insurance, the main features of the service, and the application of any non-judicial dispute resolution procedures in the contract.
- Regulation 9 provides that making the required information easily accessible is sufficient compliance.

These regulations are complex and detailed and care should be exercised over their implementation.

Companies Act 2006

Section 82 of the Companies Act 2006 provides that a company must comply with any regulations made by the Secretary of State regarding the disclosure of company information in specified locations, which almost certainly include a website.

Failure to provide the information specified may mean that any subsequent action for breach of contract by the company might fail in civil proceedings under Section 83, while Section 84 provides that a criminal offence is committed for which a fine may be imposed.

Jurisdiction and applicable law

Jurisdiction

As commerce and industry extend their activities on a global basis, organisations are routinely expected to respond by offering their services internationally. This could extend to developing countries where there may be no appreciation of jurisdictional issues. Issues of jurisdiction may emerge in the following ways:

- a dissatisfied consumer from abroad may seek legal redress against the organisation for allegedly unsatisfactory advice and services;
- an organisation may collaborate with an international agency for the provision of services which have proved inadequate and give rise to legal remedy;
- legal issues may arise over the direction and receipt of website pages in a foreign jurisdiction.

Jurisdiction is the power of a particular country, through its courts, to hear and adjudicate upon a dispute.

The question of jurisdiction can become confusing. Some years ago, the French courts took action against the American ISP, Yahoo! Inc., when its website made available Nazi memorabilia for auction, in contravention of French law. Yahoo® claimed the French court had no jurisdiction because its site was based in the United States of America. Experts decided that the site could be blocked in France and the French court ordered that steps be taken to make sale of the items impossible to French citizens through its site. This is a typical example of how confusion and uncertainties can arise where different jurisdictions become involved.

The present framework for establishing jurisdiction in the European Community is founded upon the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters 1968 – often referred to as the 1968 Brussels Convention. It contains provisions governing which country has jurisdiction over specific actions at law relating to civil and commercial matters with an international element.

The Civil Jurisdiction and Judgments Act 1982 enacted the provisions of the Brussels Convention in the United Kingdom. If a jurisdiction clause is to be included in a contract, the parties should specify which of the jurisdictions of Scotland, Northern Ireland, or England and Wales should apply. In default, this Act will be applied.

In essence, the Brussels Convention determines the court in which proceedings may be brought by a claimant in one European Union country against a defendant residing in another. The general principle is that a claimant should take legal proceedings in the courts of the member state where the proposed defendant is domiciled, unless there is a ‘jurisdiction’ clause, although certain exceptions arise.

The Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Regulation 44/2001) – the Brussels Regulation – was adopted on 22 December 2000. This is the principal law in the European Union on jurisdictional issues. It is a complex provision and requires specific reference for professional advice in any circumstances involving its possible application.

It addresses the question of where disputes should be resolved. The Regulation applies to civil and commercial matters and also specifies certain excluded legal proceedings. Individuals domiciled in a member state may, whatever their nationality, be sued in the courts of that member state. Individuals who are not nationals of the member state in which they are domiciled will be governed by the rules of jurisdiction applicable to nationals of that state.

Broadly, a consumer can bring proceedings against a potential defendant either in the consumer's country or the defendant's country. However, proceedings can only be taken against a consumer in his or her country.

Parties to a contract may opt to include a provision for jurisdiction should a legal dispute arise, although ultimately the assumption of jurisdiction is a matter for the court. Nevertheless, the inclusion of such a clause will be clear evidence of the parties' intentions.

The Regulation permits parties to enter into 'non-exclusive' jurisdiction agreements to sue or be sued in selected courts.

Professional advice should always be obtained before entering into any contract involving jurisdictional issues.

On 21 April 2009, the European Commission adopted a report and green paper on the function of jurisdictional rules and recognition of foreign judgments. The Commission has decided there is a need for free circulation of judgments in European Union civil and commercial matters, and mutual recognition of judgments among member states. The green paper launched a consultation on a proposed revision of the existing Brussels Regulation, requiring responses by the end of 2009.

Applicable law

Applicable law concerns the law that is applied by any court of jurisdiction. Applicable law was governed by the Rome Convention on Applicable Law 1980, introduced to harmonise approval of legal principles throughout the European Union. In the United Kingdom, it is enacted by the Contracts (Applicable Law) Act 1990. This was changed by the Law Applicable to Contractual Obligations Regulations 2009 (SI 2009/3064), in force from 17 December 2009, and referred to as the Rome I Regulation.

Effectively, the Rome Convention allows virtual freedom of choice to choose which law should apply to a contract. In view of the uncertainty that can arise in respect of an electronic contract, it is sensible for the parties to specify in any contract the law that is to apply in the event of dispute. In the absence of any expression of choice, the court can infer the applicable law from the content of the contract or the circumstances surrounding it. If no such inference can be made, the law to which it is most closely connected governs the contract.

Rome II (Regulation EC No 864/2007) was adopted by the European Union on 11 January 2009 and applies to certain actions (for instance, product liability claims) occurring from 20 August 2007. It creates a set of rules within the European Union to govern the choice of law in civil and commercial matters, subject to certain exclusions, and contains particular provisions for certain specific types of claim. In certain cases, the parties may agree upon the applicable law in proposed proceedings. There has been particular discussion over applicable law in defamation and road traffic cases.

The Rome I Regulation covers contract claims and relates to choice of law in contractual matters. Confusingly, it came into force following Rome II.

In general within the EU, the Rome I Regulation and Brussels Regulation on jurisdiction effectively provide that, in business-to-business contracts containing choice of law and jurisdiction clauses, whatever is agreed by the parties will prevail.

This does not change current practice on clauses. It is only where there is no contract that the legislation applies and, even then, only applies within the European Union. However, many commercial organisations do not conduct business on the basis of written contracts, giving rise to considerable potential for disputes in this area.

Applicable law issues can be extremely complex and professional advice should be obtained before entering into any contract involving questions of applicable law.

Beyond the European Union, there are no universal provisions applicable to the establishment of jurisdiction. Therefore, the laws of each country must be considered in every case. If the parties contract for jurisdiction to be given to the courts of one country, the choice of law for that country will normally be applied, provided the country has a substantial connection with the parties and the contract.

Internet abuse

Earlier, various risks were identified that arise from the way that Internet technologies are abused. These are activities or acts of misconduct with the potential to expose both any individual(s) concerned and directors or partners of organisations to civil or criminal liability. This section considers the legal consequences of such activities. An understanding of the misconduct involved enables senior management to specify unacceptable behaviour in an e-mail or Internet use policy.

Defamation

Defamation may occur either internally, as between employees within an organisation, or externally to third parties. Defamation can most commonly and easily arise from the casual use of e-mail. It is most likely to arise internally from use by employees or from comments posted to newsgroups or social networking sites, but can also arise from statements posted on a website. The global reach and accessibility of websites mean that defamatory material may be posted and accessed anywhere in the world. Liability might, therefore, arise outside the United Kingdom.

An employer may be vicariously liable for the acts of an employee performed in the course of employment, even if performed without the consent or approval of the employer. Careless employee use of e-mail may, therefore, expose the employer to legal proceedings. Even if the employer attempts to avoid liability by showing that the employee concerned was acting on their own, the employer may be caught by the provision that a publisher and editor may be liable for defamatory material.

In *Western Provident Association v. Norwich Union Assurance Co (1997)*, the defendant settled the complainant's claim for the sum of £450,000 for an allegation in a defamatory e-mail suggesting that the complainant was in financial difficulties.

Defamation may take various forms and may arise quite unexpectedly in purely informal circumstances. For instance, organisations have been known to dismiss employees for allegedly posting unfavourable comments on social networking sites regarding their employers or, in other cases, for posting allegations regarding their working environment or conditions of employment.

The Defamation Act 1996 may provide a defence in 'Internet' cases. In broad terms, the defence is available where it can be shown that the defendant:

- is an operator only of equipment and not author, editor or publisher;
- took reasonable care;
- had not caused, or contributed to, publication.

The interpretation of these provisions is being provided by the courts only as proceedings arise so there is no comprehensive guidance currently available. In *Godfrey v. Demon Internet (1999)*, the complainant successfully sued an ISP for failing to remove defamatory comments about the complainant posted on a bulletin board by another party. The 'Internet' defence was held not to be available to the ISP, which was considered to have had power to remove the offending material, and, therefore, control over its dissemination.

The case of *Bunt v. Tilley and others (2006 EWHC 407 QB)*, decided that ISPs could avail themselves of this defence, provided they had no notice of the posting of any defamatory material, and if notice had been received, they took reasonable steps to remove it.

However, organisations whose employees post or send defamatory material over the Internet are likely to be 'publishers' and may, therefore, have difficulty raising this defence. Evidence that an employer took reasonable care might be the inclusion of some provision regarding such conduct in an e-mail use policy.

In *Dow Jones & Co. Inc. v. Gutnick (2002) HCA 56*, an Australian court decided that the claimant in an Internet defamation case was not bound to launch proceedings in the jurisdiction in which the defamation originated, nor in the jurisdiction in which they resided. As material on the Internet is available everywhere, it was decided that the claimant could select any jurisdiction.

Various cases in the UK courts have cited this case, and it seems likely that if the case were raised in UK litigation, this principle would be followed.

The general principle surrounding publication of defamatory material is that each act of exposure is potentially actionable. In the case of the Internet, this means that on each occasion the material is accessed, a separate cause of action arises.

In the case of *Yousef Jameel v. Dow Jones & Co. Inc. (2005, EWCA Civ 75)*, it was decided that trivial publication, for instance a few 'hits' on a website, was insufficient to bring a claim for damages. In this case, the material was accessed five times.

In the case of social networking sites, the defence may be available, but this implies that that the hosts of the site should take reasonable steps to monitor postings for potentially defamatory material. As this seems rather impractical, the more likely position is that hosts should be quick to respond to requests to remove alleged defamatory material (*see Godfrey above*).

Pornography

The various ways criminal liability can arise in respect of obscene and offensive material and behaviour was considered earlier. There are several sources of legislation governing this area, together with case law providing interpretation. This consideration focuses on the key legislative provisions.

Obscene Publications Act 1959

This Act makes it an offence to publish or distribute obscene material. It is a criminal offence to display it on a website or despatch such material over the Internet. In practice, prosecutions are brought against the original source of the offence. A defence is available if it can be shown that the accused did not examine the material and had no reason or cause to suspect that publication would lead to liability.

Obscene material

Under the provisions of the Indecent Displays (Control) Act 1981, it is an offence to publicly display indecent material or to cause or permit indecent material to be publicly displayed. A website, with its global accessibility, almost certainly falls within the definition of a public place. Further, the Criminal Justice and Immigration Act 2008 prohibits the holding of certain extreme images.

Telecommunications systems

It is an offence under the Telecommunications Act 1984 for any person or corporate body to send a message that is grossly offensive, indecent or obscene by means of a telecommunications system. There seems no reason why this should not apply to users of the Internet, particularly in respect of e-mails, but there have been no decided cases on the subject to date.

Photographs of children

The possession of indecent images of a child (aged under 16 years) is an offence under the Criminal Justice Act 1988. It is a defence to show that an individual or organisation either did not see the image, or had no knowledge or suspicion that the image was indecent, or that there was a legitimate reason for publishing or distributing the image. It is a further defence to show that the image was not requested nor kept for an unreasonable period.

Sexual discrimination and harassment

Typical conduct amounting to sexual discrimination or harassment might include sending internal or external e-mails of an unacceptable nature, or with explicit references to an individual. The offence was originally governed by Section 41 of the Sex Discrimination Act 1975.

It is a defence to show that reasonably practicable steps were actively taken to prevent the harassment. The burden is on the employer to show an attempt to prevent the act in question and harassment generally. Evidence of this may be demonstrated by its inclusion in any Internet or e-mail policy implemented by the employer.

Racial discrimination and harassment

Racially discriminatory or harassing behaviour was originally governed by the Race Relations Act 1976, which contains similar provisions to the Sex Discrimination Act 1975. Additionally, public order legislation makes it a criminal offence to publish threatening, abusive or insulting material intended to stir up racial hatred. Liability can rest upon an employer when it can be shown that the situation was sufficiently within their control. No specific legislation exists to address racial harassment.

Both Acts are codified in the Equality Act 2010 which, for the most part, is in force from October 2010.

Remedy lies through a claim to a tribunal, which has power to award unlimited compensation, including an award for injured feelings.

Illegal file-sharing

This is addressed by the provisions of the Digital Economy Act 2010.

In broad terms, the Act addresses certain abuses of the Internet, including infringement of copyright. Fairly draconian powers are included, such as blocking off access to certain Internet locations for those found to infringe copyright persistently. Further, the Act amends the Copyright Designs and Patents Act 1988 by increasing the penalty for infringement (including recordings) to a maximum fine of £50,000.

The Act places a duty on ISPs to monitor their networks and report suspicious customer activity to copyright holders, or face a fine of £250,000 for non-compliance.

Monitoring and surveillance

Earlier, a number of risks were identified that might arise from the behaviour of employees in the workplace. Internet technologies have features enabling employees' activity to be monitored. Monitoring and surveillance of employees' use of e-mail and the Internet introduce some controversial and legally complex issues. A balance must be struck between the entitlement of an employer to expect appropriate behaviour from employees, and the rights of employees to be respected.

Monitoring in the workplace involves two activities: checking the performance of the employee, and checking the behaviour of the employee. The monitoring under consideration is concerned with employee behaviour.

There are four pieces of legislation that have implications for the question of monitoring:

- the DPA;
- the Regulation of Investigatory Powers Act 2000;
- the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- the Human Rights Act 1998.

The DPA was considered earlier. Monitoring activities involve the collection of personal data assembled from surveillance of an individual's behaviour. Organisations will need to be aware of the implications of the DPA and the potential for exposure to criminal liability.

This section outlines the key legislative provisions in respect of monitoring activities and considers the steps that an employer might reasonably take, both to comply with existing legislation and to observe employee rights.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 is a measure designed to control the interception (monitoring) of secure (encrypted) messages. Its purpose is to provide the United Kingdom's law enforcement agencies with power to intercept (Internet) communications. Under this Act, ISPs are obliged in law to allow access to certain messages and to reveal the content of any encrypted messages in a form capable of being understood.

Employers will be primarily concerned with Part I of the Act. This relates to unlawful and unauthorised interception of communications. The Act has a number of implications for the use of secure e-mail communications. Broadly:

- the unauthorised interception of communications on a public telecommunications system is a criminal offence;
- the operator of a private telecommunications system who carries out interception of any communication on a business's own system can be liable in tort and may be the subject of civil proceedings;
- where the interceptor has reasonable grounds to believe that both the sender and recipient have consented to the interception, the Act permits the interception of communications;

- the Secretary of State has power to make regulations authorising businesses to intercept communications on their own systems without consent for certain purposes.

Enforcement is by warrant issued by the Home Secretary to the police, security services or HM Revenue and Customs. The grounds on which the Home Secretary may authorise a warrant are that it is: in the interests of national security to do so; or justified for the detection of serious crime; or in the economic interests of the United Kingdom to do so.

Organisations encrypting communications data should be aware of Part III of this Act, which came into force in October 2007. This empowers law enforcement officers to gain access to the content of evidence held in computer files even if they have been encrypted. This means that prosecuting authorities may call for the production of cryptographic keys to decrypt data required for prosecutions. Criminal proceedings may follow for failure to produce encryption keys under Part III.

Under the Act, an employer can only intercept communications if there are reasonable grounds to believe that the users have consented; or a warrant has been issued by the Home Secretary; or if the interception is undertaken within the provisions of the Telecommunications (Lawful Business Practice) Interception of Communications) Regulations 2000.

Therefore, the basic principle is that interception of communications is prohibited, unless the interception, or monitoring, falls within one of the exempted circumstances, under either the Act itself or the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. It is with the implications of these regulations that employers will be most concerned.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Although an employer's monitoring of employees' communications in the workplace is a managerial issue, these Regulations govern an employer's legal right to monitor employee behaviour.

The Regulations allow employers lawfully to intercept business communications without the consent of an employee in a range of circumstances. All types of communication are covered by the Regulations, so the provisions will include e-mail. In broad terms, the Regulations permit the recording of communications to:

- establish factual evidence;
- monitor compliance with office practice and protocol;
- monitor service and training compliance;
- safeguard national security;
- detect or prevent crime;
- detect or prevent misuse or unauthorised use of telecommunications systems – for example, e-mail;
- maintain the safe and secure operation of the system;
- monitor voluntary and charitable helplines.

The Regulations provide that this conduct is authorised only if there have been all reasonable efforts to inform those using the systems in question that communications may be intercepted.

The Regulations require the communications to take place in the course of business and on a system provided for use in the course of business. It follows that the interception or monitoring of private communications, e-mails and Internet use is not permitted.

An employer must, therefore, decide whether to permit or prohibit personal use of business communications systems. If an employer decides to permit personal use – and to monitor that use – the consent of the parties involved must be obtained, although it seems in order to monitor private communications at 'traffic level' (the identity of the parties to the communication only), but not 'content level' (the actual content of any communication).

If an employer decides to prohibit private use, it should be borne in mind that this might be held to be a breach of an individual's rights under the Human Rights Act 1998. Although, this applies to public organisations, a private sector employer who is challenged before an Industrial Tribunal, or another court, will find that the principles of the Human Rights Act are applied.

Human Rights Act 1998

The Human Rights Act came into force on 2 October 2000 and incorporates the European Convention on Human Rights. Schedule 1 contains the provision relevant to monitoring – Article 8 of the Convention. This conveys a right to privacy, which includes correspondence. Arguably, this includes 'correspondence' in the workplace.

One early case on the subject of the interception of communications was *Halford v. United Kingdom (1997) IRLR 471*. The European Court of Human Rights found that interception of the claimant's calls (to her lawyer) from the office was a breach of her rights under Article 8.

In *Max Mosley v. News Group Newspapers Ltd. (2008) EWHC 1777 (QB)*, the High Court awarded the claimant, who was engaged in lawful activities in private when photographed covertly for the *News of the World*, £60,000 damages and costs for breach of confidentiality and privacy under the Human Rights Act 1998.

Employment Practices Code 2005

In June 2005, the Information Commissioner's office published the Employment Practices Code. Part III of the Code concerns the monitoring of employees' use of telephones, e-mail systems and the Internet. This adds to the debate on monitoring by suggesting certain practices that employers should observe when monitoring employee use of e-mail and the Internet.

In respect of monitoring, the core principles are that any monitoring must, of course, be lawful. The employer should undertake an impact assessment looking at the purpose of the monitoring, any adverse impact, any alternatives to monitoring and whether monitoring is justified. Any consent to monitoring must be freely given. In general, the intrusion should be kept to a minimum and there should be a published policy of which all employees must be aware.

The general presumption is that monitoring is intrusive and that employees are entitled to privacy. There must, therefore, be a clear purpose to any monitoring exercise and employees should be informed of its nature and extent.

Any monitoring must be proportionate. This is for the employer to decide. For example, a search of office employees for cigarettes might not be proportionate, but may be so, for instance, in respect of employees working at an oil refinery. Where possible, monitoring of traffic is preferable to monitoring of content, and automated monitoring is considered less intrusive than targeted monitoring.

The Code explains clearly and in detail the obligations of employers in these circumstances. No monitoring exercise should be undertaken without reference to the Code. It is available as a downloadable document from the website of the ICO at *www.ico.gov.uk*.

This network of legislative, regulatory and codified provisions is confusing. In summary, the Regulation of Investigatory Powers Act, in general, prohibits the interception or monitoring of communications except in closely defined circumstances, for example those described in the Telecommunications (Lawful Business Practice) (Interception of Communications) Telecommunication Regulations. These Regulations permit monitoring within another set of closely defined circumstances. However, they appear to conflict with the Human Rights Act 1998. In addition, the Employment Practices Code establishes further principles in respect of monitoring.

Organisations would be wise to ensure that well-documented processes and procedures are followed when performing a monitoring exercise, for example:

- any policy or protocol should be in writing – and communicated to all staff;
- the rights and obligations in respect of use of electronic communications and the World Wide Web should be clearly stated;
- prohibited uses and applications should be specifically stated;

- any steps to be taken to monitor staff should be clearly defined;
- any privacy rules to be observed should be clearly stated;
- any disciplinary sanctions for failing to comply with the established policy or protocols should be specified.

Professional and regulatory codes

In addition to generally applicable statutes, regulations and codes of practice, business professionals should also have regard to codes of conduct and best practice issued by their professional bodies. Comprehensive coverage of the codes of every professional body is beyond the scope of this book but some typical examples are listed below.

Institute of Chartered Accountants of England and Wales

The *Members' Handbook* specifies a code of ethics which includes the need to exercise due care and preserve confidentiality in providing services. In particular, certain duties of disclosure are imposed.

Solicitors Regulation Authority

The *Solicitors' Code of Conduct 2007* requires solicitors to preserve client confidentiality and display competent standards of service. In particular, under Rule 5, solicitors' firms are required to exercise proper standards of supervision, ensure compliance with regulatory requirements and have in place appropriate strategies for the management of risk.

The Law Society

The Law Society is the representative body for solicitors practising in England and Wales. In November 2005, the Law Society published *E-mail Guidelines for Solicitors*. On 11 September 2008, the Law Society published an *Information Security Practice Note* for solicitors. Both documents can be found at *www.lawsociety.org.uk*.

Royal Institute of Chartered Surveyors

This body published *Rules of Conduct for Firms* on 4 June 2007, which were updated in January 2010. Included in the rules are provisions that members shall avoid situations inconsistent with professional obligations, provide necessary training and perform to required standards of competence.

How such codes are applied is a matter for each professional body, having regard to the facts and law in each case. It should not be overlooked, however, that these codes may be applied to all aspects of professional practice, including the management of Internet risk.

The legal and regulatory provisions described have a number of implications. First, in order to achieve maximum compliance throughout an organisation, it is necessary for the behaviour of everyone in the organisation to be regulated in some way. In this way, the risk of infringement may be minimised, even if it cannot be eliminated. It is unlikely that legal compliance risks can be eliminated entirely because of the uncertainty that tends to surround interpretation of the law.

There is also a need for employees to understand what is expected of them. Employees who have no clear guidance on the standards of professional conduct expected in the workplace cannot be expected to conform to the standards required of them. Lack of authority and absence of clear guidelines are likely to result in a failure to observe appropriate procedures, some of which may be vital to the organisation's reputation or business function.

CHAPTER 10: OPERATIONAL SOLUTIONS

An organisation might employ the most sophisticated technology and develop meticulous compliance procedures, but exposure to Internet risks will remain inadequately addressed, unless operational use of Internet technologies is effectively managed. The types of operational risk that might arise were discussed in Chapter 4.

Operational controls help to protect directors, partners, personnel and the organisation as a whole from exposure to liability, while at the same time helping to identify any steps to minimise the impact of risks. Controls define the organisation's expectations of the use of Internet technologies. Without a policy defining their acceptable and unacceptable use, an organisation may find it difficult to discipline an employee legally.

Internet policies

An organisation should have policies which amount to a framework for the guidance of all personnel in the way they use Internet technologies. There is no universally appropriate set of policies because organisations differ from one another in their use of Internet technologies.

Policies may be placed on the firm's Intranet, included as a section in an office procedures manual or included as part of each employee's contract of employment. However this is approached, it is important that the policy is easily accessible to all employees. A sensible approach is to ensure that the policy is explained to each new employee on induction.

The policy should be a framework governing an employee's use of Internet technologies and establishing the legal relationship of the parties in much the same way as a contract of employment. It should contain reference to disciplinary sanctions. The policy should be drawn with care with the possibility in mind that its production may be required in legal proceedings.

This section identifies some key components for inclusion in an Internet technology security policy. By selecting relevant components, it should be a relatively simple task for an organisation to create and develop its own suite of policies as its use of Internet technologies develops to meet consumer demand.

Why is an Internet technology security policy necessary? A policy, drawn up to meet organisational requirements serves a number of purposes:

- the protection of directors, partners, personnel, and the organisation as a whole from exposure to liability;
- the identification of difficulties and steps to minimise any impact on the organisation;
- the definition of an organisation's policy in respect of the use of Internet technologies;
- the promotion of awareness and the establishment of good practice.

Helpful general guidance in this area is provided by the Internet Watch Foundation, established in 1996 by ISPs to prevent criminal activity on the Internet and assist users in developing procedures to avoid damaging activities (*www.iwf.org.uk*).

Simple but important principles – a mixture of good practice and common sense – should be applied to the introduction and implementation of any Internet use policies. They apply to all the policies discussed in this section, with the exception of monitoring, which applies only to employee e-mail and Internet use policies.

Andrew Rose of Clifford Chance explains the firm's approach to Internet use policies:

> The firm is keen to ensure that personnel follow approved procedures when using Internet technologies. Although there is always an appetite for a very detailed and comprehensive policy set, we found that such a solution could be ineffective; policies were too detailed for staff to remember, too specific to various scenarios, and required constant revision and enhancement. Furthermore, with the amount of content required to cover all eventualities, the policy set could become fragmented and include a mix of policies, procedures and guidelines which were confusing to end-users.
>
> The lesson learned was that documentary guidance for staff should be relatively high level and easily accessible. The firm's Internet use policies are now posted on the Intranet and are reviewed quarterly. Personnel are issued with an information security handbook which is reviewed during induction training; then we rely on their commonsense.

Policy development

It is sensible to include the views of others in, and connected with, the organisation when creating a policy. All departments and individuals, including junior personnel, should be consulted. Customers and clients might also be involved as consultation will ensure the policy is convenient for them as well as demonstrating commitment to consumer interests.

Policy communication

A policy is unlikely to be effective, unless it is properly communicated and promulgated throughout the organisation. If the consultation exercise has been adequate, there should be sufficient awareness. The most obvious way of communicating a policy is the publication of a formal document. Some organisations may incorporate this in employees' contracts of employment, or require employees involved to sign a separate policy. Other methods might include posting on the firm's Intranet, and conducting seminars and workshops.

Clarity

A policy is unlikely to be useful if it is difficult to interpret or apply. When a policy document is consulted, especially in respect of cyber risks, it is most likely to occur in a crisis, and, therefore, guidance and instruction should be clear and accessible. It is worth remembering that a policy may be referred to by a relatively junior member of staff and that, therefore, in an emergency, clarity is a vital issue.

Monitoring

The legal position in respect of monitoring employee use of e-mail and the Internet was examined in Chapter 9. The key issue is that if monitoring is to occur, the employee(s) concerned must be informed. Any employee who is to be monitored should be informed, for instance, that e-mail use and Internet access may be monitored periodically and that software may be employed for the purpose. This notice should appear in the policy itself and in any contract of employment. Some useful steps might be to:

- inform personnel that privacy of use does not apply to Internet technologies in business hours or in the course of employment;
- inform personnel that inspection will take place periodically;
- inform personnel that unacceptable sites may be blocked;
- warn personnel to disconnect from any site containing unacceptable material;
- inform personnel that stored e-mail may be inspected periodically.

Data protection

Most components of an Internet technology security policy involve, in some way, the processing of personal data. Underlying all Internet activity is the need to ensure compliance with the DPA. In view of the ease with which personal data can be transmitted, it is important that employees using Internet technologies have a general awareness of its provisions and the need for compliance. Examples of particular categories of employees concerned would include those involved in marketing activities and management of the firm's website, in both of which cases information is frequently gathered from visitors.

Policy management

An employee who is required to observe policies and procedures in the workplace should be aware of how the policy is to be administered. The policy should, therefore, set out the framework for the management of the organisation's Internet technology security policy. It should identify, for instance, responsibility for implementing the policy, staff training procedures, disciplinary offences and sanctions, and dispute resolution procedures.

Richard Spooner of Baker Tilly comments on the firm's approach to use policies:

> The (Internet risk) management structure is supported by a computer usage policy which governs access controls, physical controls, the security of e-mail and the encryption of data, for instance, on USB memory sticks.
>
> It is a comprehensive resource and there is a provision in the contract of employment of all staff that they will observe the firm's code of conduct in this respect. While there is no formal staff monitoring to ensure compliance, there are IT controls that monitor, for instance, e-mail, for inappropriate content and abuse. Beyond this, staff are expected to behave responsibly and any serious breach is referred to the HR department for disciplinary action.

An outline of some key features of the more important Internet security policies are discussed below.[8] They are not comprehensive because every organisation will have particular requirements and preferences. However, they may help as a baseline from which to develop policies which can then be tailored to the organisation's needs.

The policies considered are for:

- use of e-mail;
- use of the World Wide Web;
- use and operation of websites;
- management of the delivery of electronic services;

[8] Certain passages have been drawn from protocols contained in the Internet Policies Toolkit, published by the Law Management Section of the Law Society.

- management of data;
- business continuity and disaster recovery issues;
- Web 2.0 and social networking.

Specific policies

E-mail use policy

The issues to be addressed in an e-mail use policy can practically be considered in the following categories: business use of e-mail; personal use of e-mail; e-mail security; legal implications of e-mail; and e-mail notices.

Business use

The policy should establish standards of conduct expected of all those using e-mail in the workplace and can be divided into categories. The first category addresses the potential for exposure to legal liability. The policy should contain guidance on the need to avoid breaches of confidentiality, negligent misstatements and unsupervised conclusion of online contracts.

The second category concerns the handling of e-mail in the course of business. The policy should set out the position on accepting instructions by e-mail; stating the sender's identity and position in the organisation; professional undertakings given by e-mail; the preferred style and content of e-mail communications; forwarding e-mail and the checking of e-mail during a recipient's absence.

The third category addresses the subject of e-mail. The policy should address offensive, obscene, harassing, threatening or defamatory e-mail content including attachments; the despatch of unsolicited e-mail;

unauthorised participation in discussion groups and social networking sites; and interfering with others' e-mail without permission.

Personal use

The policy should state whether or not the use of e-mail for personal use is acceptable. If permitted, the policy should stipulate the circumstances in which personal use is allowed. There are two areas to address.

The first concerns use prejudicial to the organisation. The policy should prohibit personal use amounting to commission of a criminal offence, causing loss or damage to the organisation and infringing the rights of other employees. The second concerns the abuse of personal e-mail. The policy should specify that personal use must be on a reasonable scale and not for personal financial gain.

E-mail security

The policy should establish the measures to be taken to ensure that, where necessary, e-mail is secure from interference or corruption. The policy should contain instructions in the following areas: encryption procedures, virus defence, and e-mail storage.

The policy should contain instructions for the use and application of encryption procedures, and the need to consult recipients and review encryption requirements regularly.

The policy should contain instructions to address the risk of virus intrusion; specifically procedures for scanning incoming e-mail, the opening of attachments from unfamiliar sources and the use of any installed anti-virus software.

The policy should contain instructions for the storage of e-mails both sent and received, and procedures for ensuring that stored e-mails are secure from unauthorised access. While there is no time specified for the retention of archived e-mail, data protection provisions require a balance to be achieved between retaining information for no longer than is reasonably necessary, and ensuring that data subjects have access to any information to which they might be entitled under the DPA.

Legal implications of e-mail

The use of e-mail in the course of business has legal implications in the same way as traditional correspondence. The issues that arise can be considered in two categories. The first category addresses the validity of e-mail in legal proceedings. The policy should remind users that e-mail may be admissible in evidence and that computer records might be admissible in legal proceedings.

The second category addresses the need for e-mail to conform to legal and professional requirements. The policy should remind users that, where required to do so, the form of e-mail should comply with the Business Names Act 1985, the Companies Acts, and relevant business and professional codes.

E-mail notices

There are various situations in which an organisation may wish to endorse e-mail with one or more conditions relating to their despatch. Typical notices concern confidentiality, copyright and viruses. Where an organisation requires such notices to appear on e-mail, the policy should specify which notices and the terms in which they should appear.

Some e-mail notices attempt to disclaim liability for the content of the message. Disclaimer clauses are subject to the test of reasonableness In addition, the endorsement of such a notice if giving advice to a consumer is not likely to engender confidence in the organisation.

Many organisations place notices on e-mail in respect of precautions taken by themselves and those to be taken by the recipient. The object is an attempt to avoid any legal liability that may arise for the transmission of a virus.

Notices in respect of the formation of online contracts also appear on e-mail. These might typically state that the views expressed in the e-mail are those of the author only and do not represent the enterprise, unless specifically stated; and the author has no authority to enter into or conclude a contract by e-mail.

E-mail notices do not automatically carry legal validity. This is ultimately a matter of interpretation by the courts, and there may well be instances in which they are found not to be binding. Most notices of this type are subject to the test of reasonableness.

Internet use policy

Business use

The policy should establish principles of conduct that are expected of employees in the workplace. There are three areas requiring specific mention: social networks/discussion groups, downloading material and inappropriate material.

The policy should specify that only authorised personnel should take part in discussion groups and that when participating in such activities, unauthorised release of information will be a disciplinary offence.

The policy should state that when downloading material, this must be for business use only, and that downloaded material becomes the property of the firm. A requirement for virus-scanning procedures to be undertaken when accessing and downloading material should also be included.

The policy should specify that sexually explicit and other material inappropriate to the workplace should not be downloaded, stored or distributed. The policy might also stipulate that accidental connection to a site containing unacceptable material must be terminated immediately.

Personal use

The firm must decide whether to permit use of the Internet for personal reasons. The legal position was explained in Chapter 9. If personal use is permitted in the workplace, the policy should specify any personal or non-business use that is permitted.

Security

The policy should detail the security measures installed to protect against unauthorised or hostile intrusion. The policy should state the firewall technology employed, how the firewall should be used and the business functions that it permits, together with a notice that attempts to avoid firewall technology may result in disciplinary procedures.

The policy should stipulate requirements in respect of passwords. Passwords are vulnerable to manipulation. The policy should be as specific as possible about their use.

Former employees

Disaffected former employees pose a particular threat. Some issues to consider include making regular security checks of the network perimeter, closing former employees' connections and ensuring all laptop computers are returned by employees leaving the firm.

Website management

A policy governing the use and management of the website is advisable both to guide personnel and to enable more effective management of relationships with casual visitors, consumers and others visiting the site.

Content

The policy should specify procedures that ensure content is accurate and legally up to date. There should be procedures established for checking that the site content has not been interfered with, or the site itself defaced. These procedures should be specified and responsibilities assigned.

Disclaimers

A disclaimer is published on a website to draw visitors' attention to the fact that the information on the site is not comprehensive and that further information and guidance may be appropriate. A policy should state that the website must contain a statement for visitors to the effect that information and advice posted on the site is accurate to the best of the organisation's belief, that no liability can be accepted for action taken as a result of visiting the site, and that visitors should realise that individual circumstances differ and that further advice is appropriate before action is taken. The legal validity of disclaimers was discussed in Chapter 9.

Jurisdiction

The policy should require a statement to be posted on the site to the effect that advice and information is given on the basis of the law of England and Wales, or whatever other jurisdiction is appropriate.

Linking

Difficulties that can arise in respect of linking to other sites were considered earlier. There should be a settled and defined policy in respect of links with other sites.

First, the policy should provide for a written agreement to be in place, establishing the terms and conditions on which the site will agree to be linked to another site. Second, there should be a policy document establishing the terms and conditions of any agreement to accept a link from another site. Third, there should be a disclaimer in respect of unlawful or unsuitable material on the linked site.

Copyright

Protection is required in respect of information and advice posted on the site, and also to ensure that personnel do not use material from another site without permission.

The policy should, therefore, require that copyright notices are displayed in respect of any material for which copyright is to be retained. Conversely, the policy should require there to be a written agreement for the use by the organisation of any material published on another site.

Security of data

It is helpful and reassuring for visitors to be informed of the steps taken to ensure security where information is to be supplied through a website. The policy for management of the organisation's site should specify the security measures in place and any procedures for their review and update.

Many data protection notices simply state that information and data collected from visitors to the site will be held in compliance with the DPA. A privacy policy should contain more detail It is suggested that the following information should be given: the fact that personal data is being gathered; how the personal data will be used; with whom, if anyone, the personal data will be shared; whether the personal data will be exported outside the European Union; the data subject's choices regarding the use of the collected data; safeguards in place to protect loss of, or damage to, collected data; procedures for amendment and updating; the right to opt out of marketing mailing; and the identity of the data controller.

Electronic services policy

A policy for the delivery of legal services electronically should address the following issues: the need for legal compliance, the content of contracts for the supply of services, and provisions governing electronic payments.

Legal compliance

The policy should identify the legal, regulatory and professional provisions governing the services delivered electronically. These include reference to basic consumer legislative and regulatory provisions applicable to traditional services. They will also specify legislative and regulatory provisions applicable to the Internet, as discussed earlier. The policy should ensure that each employee concerned is equipped with sufficient knowledge required for adequate compliance. The policy should also specify the jurisdiction and applicable law that will govern any contracts into which the firm might enter for the provision of online services.

Contracts

The policy should establish the terms and conditions upon which services are provided electronically, and display these appropriately on the website. It should contain the procedures concerned in supplying services electronically and any provisions seeking to limit liability.

The policy should specify the services to be provided, accompanied by a statement that the availability of a particular service does not constitute an offer, but merely an invitation to treat. The policy should also specify the information required under the Consumer Protection (Distance Selling) Regulations 2000 and any documentary evidence of the transaction to be retained as a record of any transactions conducted online.

The policy should address liability in respect of any ancillary services supplied through a linked site and specify that in respect of all transactions, the law of England and Wales (or as appropriate) will apply.

Electronic payments

It is important that those in the organisation who might be responsible for collecting and administering electronic payments are familiar with the PCI Data Security Standard. It is also sensible to inform consumers who are using the service how it is administered so as to provide reassurance over questions of privacy and security.

The policy should specify the measures in place; for example, the association with any electronic payments software supplier, and compliance with the PCI Data Security Standard. The policy should also state the security systems in place to ensure security of transactions taking place online.

Data management policy

The risks arising from mismanagement of data were considered earlier. In documenting a data management policy, certain issues should be addressed.

Data type

Consideration should be given to the type(s) of data being collected and stored. There might be various categories such as marketing, financial and 'personal interest' or family data. Some data might be 'sensitive' data within the meaning of the DPA. The policy should specify the measures to be taken to protect specific categories adequately.

Accuracy

Procedures should be specified in the policy to ensure that any data collected is both up to date and accurate. These will include the need to review data sources, and checking and storage procedures, as well as reviewing old data.

Security

The policy should state the measures in place to ensure safe storage of data and any procedures to be adopted for its transfer (such as obtaining consents), together with any precautions to be taken to prevent unauthorised access and transfer, whether internal or external. These measures should include both the technologies to be employed and the nomination of any personnel and their responsibilities with regard to the authorised handling of data.

Processing

The policy should identify the methods by which data is collected (for instance, through the organisation's website, by e-mail or by an extranet), and procedures to be adopted for its safe storage. The policy should specify procedures to be adopted for data subjects to 'opt out' of providing personal data, and those to ensure that data collected and held cannot be passed to third parties without authority.

The policy should identify procedures to be observed for obtaining any necessary consents in respect of its use or its release in the ordinary course of business or in response to legal proceedings. Procedures should be specified governing the handling of requests by data subjects for access to data; the correction and updating of data; and the storage, removal or deletion of data.

Implementation and compliance

The policy should set out the steps taken to ensure compliance. These are likely to include the need to document the technology to be employed and procedures to be adopted.

The policy must be promulgated, so that personnel with specific responsibilities are clearly identifiable to other personnel and all personnel are aware of the need to comply with certain procedural requirements.

The policy should establish the steps to be taken for personnel education and training, and the procedures for raising awareness of new legal and technological developments that may affect compliance issues.

Business continuity and disaster recovery policy

The risks arising from incidents that affect the ability of an organisation to function were considered earlier. Steps should be taken to ensure that in the event of such incidents, responsibilities and accountabilities for managing the situation are clearly defined and understood.

Committee

A committee should be formed of senior management representatives supported by specialists in IT, compliance and operational issues. Thought should be given to its composition, the qualifications and experience of its membership, and its remit on identifying, categorising and managing the risk.

Function

The committee's function will vary according to the requirements of each organisation but might include:

- identification of data needed for the organisation to function;
- identification of IT systems and networks for the organisation to provide a basic service;
- introduction of systems for retrieval of data;
- devising procedures for identifying solutions and their deployment and management;
- ensuring the availability of, and access to, any necessary documentation;

- allocating responsibilities in key areas of the organisation for the continuing operation of the organisation while the incident is addressed;
- devising recovery procedures and promulgating these throughout the organisation.

Web 2.0 and social networking policy

The rapid growth of social networking has resulted in this type of technology insinuating itself into the workplace. Employees familiar with social networking technologies routinely communicate with colleagues through these sites, both in and outside working hours. The popularity of social networking puts pressure on organisations to allow at least some use of this type of communication in the workplace.

The threats arising from social networking were discussed earlier. They expose an organisation to considerable vulnerability because of the danger that these sites relate to activities such as gambling, pornography, illegal software downloads and the posting of defamatory material.

Technology

As a matter of course, any policy should include provision for the use of technology that addresses the potential danger of employees accessing such sites. Technology is available that will check and filter malicious websites hosting both suspicious code and content.

Access management

The application of this technology should be supported by a rigorous policy of identity and access management, controlling the numbers and categories of employee who are permitted access to social networking sites. There are various controls that can be implemented. Controls may be imposed, for instance, by group, by department, or even by timing – by authorising access for non-business purposes at certain times, for example during lunch hours.

Employee behaviour

The somewhat anarchic development and use of social networking sites demands that employers should have clear and comprehensive guidelines for employees in their use of this method of communication. Specific issues on which an employer should provide guidance include:

- the type of data and illustrations to be posted;
- verification as to the identity of other users and contacts;
- the need for awareness of sensitive and personal data;
- the need for awareness of the potential for reputational damage to an organisation, and criminal and civil implications in respect of casual posting of information;
- the need to preserve confidentiality of personal data, both individual and organisational;
- the need to preserve confidentiality in respect of personal identity and passwords.

Monitoring

The use of social networking sites is a clear example of a situation where an organisation may wish to monitor the activities of its employees. The legal position regarding monitoring in these circumstances was considered in Chapter 9. Any policy that involves monitoring should state clearly that this is taking place, so that employees are fully aware of the position.

Other policies

As organisations develop the provision of Internet-based goods and services, consideration should be given to developing a suite of policies, or protocols, identifying and specifying the organisation's 'best practice' requirements regarding the use of Internet technologies.

The increasing trend for organisations to employ remotely located personnel using portable IT devices increases the need for clear and comprehensive guidance in this area. Specific issues on which an employer might consider providing guidance include requirements to:

- ensure the physical security of laptop computers and other portable devices;
- report any loss or damage to such devices;
- ensure that all data stored on any portable device is encrypted to an adequate standard, whether at file, folder or hard-disk level;
- back up all stored data at server level;
- ensure compliance with the organisation's identity and access management policy in respect of the use and

management of passwords and sign-in and log-in procedures;

- apply protective measures to secure data stored in portable devices, such as firewall, anti-virus, spyware and adware protection and updating procedures.

In the case of USB devices, advice and guidance should be issued governing the circumstances of their use, the need to encrypt stored data, the need for central management and the requirement to back up data.

As Internet technologies develop, the need to maintain and develop a suite of policies will increase. This function should be assigned to the organisation's risk management committee. This committee is best placed to identify the risks in each case and, therefore, to recommend strategies for their management.

Cyberliability insurance

In support of the management of its technology, compliance and operational procedures, an organisation's risk management processes may involve the transfer of its Internet risks to a specialist insurer. There are many and various brokers and underwriters now offering cover for this type of risk.

Typical areas for which cover is offered include:

- infringement of intellectual property rights;
- defamation;
- protection against reputational damage;
- misleading advertisements;

- breaches of confidentiality (for example, as a result of data breaches in respect of employees, clients and consumers);
- damage to systems, networks and computer hardware and software (for example, as a result of hacking intrusions or virus attacks);
- compensation for loss of revenue as a result of business continuity failure;
- breaches of statutory duty (for instance, non-compliance with certain e-commerce provisions);
- in certain cases, legal expenses insurance.

There is no uniform policy since the requirements of each organisation differ and specialist insurers may provide cover for individual risks. Further, a set of circumstances which may pose a significant risk for one organisation may be comfortably managed by another.

In each case, an organisation should return to its risk assessment and management plans and identify the critical risks to which it is most exposed and seek cover accordingly.

CHAPTER 11: THE CYBERSECURE ENTITY

The fundamental changes to the way in which professional services can be delivered through the Internet were described in Chapter 1. They introduce a new business model where the focus is on providing value-added services to clients, and the professional charges according to the value of services, rather than time spent.

The Internet also introduces new types of risk requiring a new approach. These risks affect all areas of an organisation at all levels. The rapid pace of change in Internet technologies means new risks are constantly evolving and, therefore, need constant control, management, monitoring, audit and review. The introduction of a team of skilled personnel influencing the management of key areas has implications for the overall framework governing the strategies and operations of an organisation.

Strategic and operational changes

An organisation's strategy is its overall plan for successful management and performance. Its operations are the mechanisms in place to achieve its objectives.

Strategic change

Strategic change involves three key stakeholders: the Directors or Partners of the organisation, its clients and its strategic allies.

Directors and partners

The approach of directors or partners is critical to managing cyber risks. As the use of Internet technologies increases, they must become familiar with the various risks arising within the organisation and the fact that these risks develop and change in irregular patterns. The risks are not structured and are difficult to anticipate because that is the nature of Internet technologies.

They need to become familiar with the concept of relying upon a team of experts for the development of strategies which, formerly, might have been their own responsibility. This consultative approach should be extended to clients and strategic allies who also need to be considered in the implementation of solutions.

They may be concerned about the viability of introducing a cyber risk management project and will want to identify some tangible benefits. They will have to understand the need for, and be willing to fund, new technology and any new personnel and services that may be involved, particularly as the initial investment may increase overheads significantly through the import of technology and the salary demands of skilled personnel.

Clients and consumers

Internet technologies empower clients and consumers in the relationship with a supplier. The consumer has the capability to be much more demanding. This will continue in an increasingly consumer-led market. Organisations need to address this as part of their client relationship management strategy. Clients should be involved in the implementation of security strategies, both in terms of their deployment and their compatibility.

The introduction of new ways of delivering services and their management has certain implications. Clients may eventually want routine access to professionals' information technology systems. The introduction of an e-mail policy may have implications for the way instructions are received from, and implemented for, certain clients. If the organisation proposes to introduce encrypted e-mail communications, consideration will need to be given to clients' systems and any interoperability issues.

Clients need to appreciate that their own interests are protected. Standards of legal compliance (for example, data protection), technology systems (for example, the employment of encryption systems) and operational management (for example, the management of e-mail communications) need to conform to levels that are acceptable to clients.

Strategic allies

Internet technologies enable online strategic alliances to be formed. Extranets enable parties to a transaction to be privately networked for exchanging information, as well as document sharing, and conducting transactions. Many professional organisations create these networks for the more convenient servicing of large commercial clients. These collaborations are sometimes referred to as 'virtual deal rooms'.

There is considerable potential for this type of network to penetrate all areas of professional practice, where accountants, financial services providers and surveyors might comprise a team or a 'supply chain' for providing services to specific consumer sectors.

Organisations need to address the security concerns of others in the supply chain as these strategic alliances develop. Agreement will need to be reached over suitable solutions. Strategic allies will almost certainly require some assurance in respect of the organisation's security policy before introducing new work.

Operational change

Operational issues arise from the activities that the organisation undertakes in developing and delivering its services. There are two key operational functions for which a cyber risk management strategy has implications – information technology and the firm's personnel.

Information technology

Traditionally, information technology has been a tool for the more efficient performance of an organisation and the more effective delivery of its services to clients. While this still remains the case, Internet technologies also change this perspective because they change the model for provision of the services.

Through the Internet, information technology becomes a tool upon which an organisation is likely to depend for its survival in an increasingly competitive marketplace. Poorly managed technology systems will not only affect the organisation's competitive advantage but also expose it to considerable risk. Effective management of information technology operations becomes critical. The approach must be to use technology not simply to provide a more effective service, but proactively to anticipate and manage client needs. Management of cyber risks is one aspect of proactive management.

Personnel

As electronic services become all-pervasive, personnel at all levels of the organisation are likely to be involved in some way, whether they are providing services, communicating with clients, or concerned with support services, for example administering electronic payment systems. The traditional model in which departments tend to operate autonomously will not help in the management of cyber risks – where a collaborative approach is required.

The efficiently managed organisation ensures that all personnel understand the principles required for the handling of personal data. Marketing personnel collecting personal data from an organisation's website need to liaise with the IT department to ensure secure data storage and with the legal department to ensure data protection compliance. Those in the IT department responsible for posting content on the firm's website need to work closely with the legal department to ensure regulatory compliance. The finance department needs to co-ordinate its operations with the IT department over the introduction of new technology. This introduces the need for a knowledge-sharing culture within the organisation – moving away from the hierarchical structure, towards a team-based approach.

Managing change

A methodical, carefully planned approach to change is more likely to succeed than a strategy developed in reaction to an unforeseen crisis requiring drastic action. The process of change differs between organisations, and individual organisations should devise strategies for managing change that fit most comfortably with their structure, culture and client base.

Character of change

The character of change depends on the style of management, the culture of the organisation and the rights or privileges enjoyed by the workforce.

Where particular individuals or groups have exercised influence, or have superior skills, account should be taken of possible changes of status, responsibility and accountability.

Directors and Partners will have most knowledge of the culture of their organisations. The shifting characteristics of Internet technologies mean that other personnel may have a greater knowledge of, for example, legal and IT issues.

The organisation must develop a flexible, proactive, measured response, but because of the pace of change must also be aware of the need to act collaboratively and with speed as the need arises.

Planning change

Change needs to be planned. The most effective method is to present details of the plans to all concerned and inform them fully of the implications.

An implementation plan can be devised with a chronological outline of the various steps to be taken. The plan should explain the new responsibilities and accountabilities of the personnel involved. It is helpful – and practical – to discuss the implementation process with those most affected. It is they who will have the greater understanding of the day-to-day impact of the changes upon their positions.

It is particularly important to take account of representations and comments made by personnel who have regular contact with clients or strategic allies. There will be no benefit if the plan alienates clients or agencies upon whose goodwill the organisation depends.

Implementing change

Those charged with introducing change must identify the key issues to be addressed, and ensure acceptance by both by those responsible for implementing it and those upon whom it will impact.

In respect of cyber risks, these features operate at board, partnership and cyber risk team level. The Directors and Partners define the plan at strategic level and the cyber risk team will be concerned with implementation at management level. There may be a strong case for change, but how can change be sold to those to whom the changes may be most inconvenient or even threatening? The introduction of a skilled and influential team of individuals at senior level could lead to a number of problems.

One analogy is the introduction of specialist financial management, marketing and IT professionals into law firms in recent years. Law firms now realise that their skills lie in providing legal advice and expertise, and accept that other professionals have greater expertise in their own areas.

A holistic approach to change is important in respect of cyber risks. Nothing will be gained by importing sophisticated technology to meet information security needs if corresponding investment is not made in educating and training personnel in its use and application. A broad view is required. Departmental hierarchies must be discouraged and personnel must become accustomed to working in teams with new ideas, concepts and performance standards.

The management of people in the context of managing change needs special attention. It is almost inevitable that there will be resistance to change from certain quarters. A key factor in successfully managing people during a period of change is the provision of timely and relevant information so there is a greater understanding and awareness of the aims and objectives of the project and a greater willingness to participate in its implementation.

Perhaps the easiest approach to implementation is the adoption of one or more of three methods. The first is a time-based trial. The project is introduced for a short period of time, during which areas of difficulty are identified and corrected before the project is launched substantively.

The second approach is to launch a pilot project. Defects in the project plan can be eradicated at an early stage.

The third approach is to adopt a phased implementation. The project should be implemented by acceptable stages over a period of time. Once each stage is reached and completed satisfactorily, the project continues to the next stage. This approach can be most useful where the success of the project depends upon the acquisition of new skills by personnel or perhaps where large numbers of personnel are involved. The value of the third approach lies in the ability to retain control of the changes that are being implemented on a bite-sized basis.

The cybersecure organisation

As the influence and use of Internet technologies develop, organisations face rapid change. Internet technologies are mercurial. Their development is rapid and uncontrolled – almost anarchic. Organisations must create and develop flexible strategies, supported by commitment and resources, which are implemented by those with adequate skills.

Six key characteristics are likely to develop in organisations adopting a comprehensively effective cybersecurity strategy. These are the ability to:

- manage increasingly demanding client expectations;
- form and manage online relationships;
- assemble and manage a multi-skilled professional team;
- comply with domestic and international law;
- harness the skills of personnel at all levels;
- develop collaborative strategies.

Managing client expectations

It is from meeting client expectations that cyber risks arise. Internet technologies enable clients to demand instant, global service. They will expect professional services to be available constantly because Internet technologies afford this facility and clients themselves employ the technologies within their own enterprises.

Commercial clients are, in general terms, more advanced in their use and understanding of technology. Large, but increasingly smaller, commercial clients use Internet technologies routinely. They have the same expectations of professionals who compete for their business, The cybersecure organisation needs skills and working practices to manage this demand, and reduce or avoid the risks to which the competition for business expose it.

Online relationships

Organisations need to develop confidence in forming online relationships. These include relationships and associations with strategic allies which may be global. As this confidence develops, organisations will widen their services, devising ways of using Internet technologies to improve delivery of existing services and create new services.

Multi-skilled teams

A cyber risk management strategy will be structured upon individuals and teams, according to the size of the organisation, highly skilled in specific areas. For example, the skills of the IT team might include experts in security issues to introduce new solutions to technology risks, offer new facilities to clients and, in so doing, present new business opportunities.

International law

The global feature of Internet technologies requires a strategy to ensure that within the organisation there is adequate knowledge, or access to such knowledge, of international law and its implications for the organisation's Internet strategy. As the Internet enables clients to develop their businesses internationally, they will expect professionals to be able to provide responsive services.

Personnel management

Organisations must develop skills in personnel management. Internet technologies involve personnel at all levels because the incidence of cyber risks has the potential to occur within all departments at almost every level. The cybersecure organisation must ensure that risks are managed at all levels, and personnel are encouraged to recognise risks and to take an interest in their identification and management.

Collaborative strategies

Both internally and externally, collaboration is a key feature of the cybersecure organisation, demanding an increasing dependence upon teamwork. The composition of the cyber risk team itself is an illustration of the need to develop strategies collaboratively. It comprises individuals from different areas within and beyond the organisation, working together to develop and implement cyber risk strategies. It is dependent upon others for its information and upon collaboration with the partners and consultants for its effectiveness.

The cybersecure organisation's strategy will rest upon the formation of collaborative relationships. Internet technologies provide an opportunity for collaboration among all participants in the supply chain, similar to the principle upon which the 'one-stop-shop' operates. Collaboration already arises in terms of marketing, as is evidenced by the importance of linking to the websites of strategic allies. In all collaborative arrangements, there are common ways of working, reciprocal arrangements and integrated systems. The particular interest of the organisation will be to ensure that there is appropriate integration and employment of compatible security measures throughout the supply chain for any given transaction.

Governance implications

Critical though a comprehensive cyber risk management framework is to any organisation using Internet technologies, it must also operate as part of the organisation's overall management infrastructure and perform as a logical and rational component of the organisation's business strategy.

In order to ensure this, the adoption of good governance principles and processes is necessary, so that the activities of the cyber risk management team remain aligned with the organisation's strategic goals. Chapter 5 explained the three components of governance of most importance to cyber risk management.

Corporate governance requires clearly defined roles of responsibility and accountability, transparent decision making, recognition of stakeholder interests, and a cohesive and relevant risk management strategy.

IT governance is a subset of corporate governance and requires the adoption of corporate governance principles with the objective of ensuring that an organisation's IT strategy remains aligned and operates to achieve organisational goals.

Project governance is also a subset of corporate governance and sits alongside IT governance – most IT activities are, in effect, individual projects. Project governance also embraces corporate governance principles and adds to them the need to identify resources to implement the project; monitor, review and audit the progress of implementation; deploy resources so as to obtain maximum value and benefit; adopt a formal risk management strategy; and ensure the project remains aligned with the strategic objectives of the organisation.

Integrating the cyber risk team

How does the cyber risk team integrate itself into the overall corporate, IT and project governance principles and procedures of an organisation?

The cyber risk team itself should adopt governance principles in the course of its operations. This is particularly important for establishing order and logic in the implementation and execution of the many projects it may face. Internet technology risks are anarchic in nature, emerging suddenly and without warning, and often requiring urgent and comprehensive solutions. The application of sound governance principles will help the team provide a coherent and relevant response.

The responsibility for setting the strategy (including the Internet risk strategy) is that of the Board of Directors or Partners and this responsibility should be undertaken with the application of corporate, IT and project governance principles at the outset. Below the Directors and Partners, management teams or committees ensure that the Directors' and Partners' strategies are overseen according to plan. Below management teams, executive teams or committees attend to implementation, monitoring, review and audit processes, then report back to management which, in turn, is accountable to the Directors and Partners.

The level at which the cyber risk team finds itself is that of a management team. It will receive strategic directions from the Board, the implementation of which it will delegate to appropriate teams or individuals within the organisation, from whom it will receive progress reports.

However, in view of its specialist knowledge, particularly in the area of Internet risk technology and legal compliance issues, it may also provide advisory services to the Directors and Partners on the management of existing cyber risks and management strategies for the adoption of emerging risks.

The size and composition of the cyber risk team will depend on the size, nature and activities of the organisation. A small organisation might confine itself to members comprising a director or partner, the head of the IT department, an external consultant for legal compliance issues, the head of personnel, a risk manager or officer and an external consultant in respect of information security issues.

Medium-sized and larger organisations will require a more complex framework. The cyber risk team(s) would recommend and, if authorised, adopt relevant governance tools and methodologies in implementing its various projects.

Conclusion

Internet technologies emerge and develop at a rapid pace and have revolutionised the way in which business, commerce and professional services are conducted, both domestically and globally. No trade or profession can escape their all-pervasive influence and for many organisations they have produced the considerable benefits of rapid expansion, increasing economies of scale and consequential profitability.

However, such a glittering scenario can only be achieved at a price – effective and comprehensive management strategies to address the sudden, unforeseen and anarchic range of risks that Internet technologies alone can present to organisations. These risks are many and various and are emerging continuously.

The prudent organisation should keep a vigilant watch because the consequences of not doing so are potentially catastrophic. At a stroke, the Directors and Partners may find the reputation of their organisation in ruins, quite apart from being exposed to criminal proceedings or civil claims for damages for illegal activities by their employees.

The prudent organisation that harnesses Internet technologies by engaging the necessary skills, adopting suitable governance frameworks and applying the correct governance tools for managing cyber risks will surely be assured of remaining well protected and competitive in its market.

ITG RESOURCES

IT Governance Ltd. sources, creates and delivers products and services to meet the real-world, evolving IT governance needs of today's organisations, directors, managers and practitioners. The ITG website (*www.itgovernance.co.uk*) is the international one-stop-shop for corporate and IT governance information, advice, guidance, books, tools, training and consultancy.

http://www.itgovernance.co.uk/white_collar_crime.aspx is the information page on our website for our white collar crime resources.

Other Websites

Books and tools published by IT Governance Publishing (ITGP) are available from all business booksellers and are also immediately available from the following websites:

www.itgovernance.co.uk/catalog/355 provides information and online purchasing facilities for every currently available book published by ITGP.

www.itgovernanceusa.com is a US$-based website that delivers the full range of IT Governance products to North America, and ships from within the continental US.

www.itgovernanceasia.com provides a selected range of ITGP products specifically for customers in South Asia.

www.27001.com is the IT Governance Ltd. website that deals specifically with information security management, and ships from within the continental US.

Pocket Guides

For full details of the entire range of pocket guides, simply follow the links at www.itgovernance.co.uk/publishing.aspx.

Toolkits

ITG's unique range of toolkits includes the IT Governance Framework Toolkit, which contains all the tools and guidance that you will need in order to develop and implement an appropriate IT governance framework for your organisation. Full details can be found at www.itgovernance.co.uk/products/519.

For a free paper on how to use the proprietary Calder-Moir IT Governance Framework, and for a free trial version of the toolkit, see www.itgovernance.co.uk/calder_moir.aspx.

There is also a wide range of toolkits to simplify implementation of management systems, such as an ISO/IEC 27001 ISMS or a BS25999 BCMS, and these can all be viewed and purchased online at: http://www.itgovernance.co.uk/catalog/1.

Best Practice Reports

ITG's range of Best Practice Reports is now at www.itgovernance.co.uk/best-practice-reports.aspx. These offer you essential, pertinent, expertly researched information on an increasing number of key issues including Web 2.0 and Green IT.

Training and Consultancy

IT Governance also offers training and consultancy services across the entire spectrum of disciplines in the information governance arena. Details of training courses can be accessed

at *www.itgovernance.co.uk/training.aspx* and descriptions of our consultancy services can be found at *http://www.itgovernance.co.uk/consulting.aspx*.
Why not contact us to see how we could help you and your organisation?

Newsletter

IT governance is one of the hottest topics in business today, not least because it is also the fastest moving, so what better way to keep up than by subscribing to ITG's free monthly newsletter *Sentinel*? It provides monthly updates and resources across the whole spectrum of IT governance subject matter, including risk management, information security, ITIL and IT service management, project governance, compliance and so much more. Subscribe for your free copy at: *www.itgovernance.co.uk/newsletter.aspx*.