

Assessing and managing **DIGITAL RISKS**



*A guide for businesses published by
The International Underwriting Association and The Department of Trade and Industry*

“In today’s business world companies rely heavily upon new technology that 20 years ago would have been almost unrecognisable. This sea change has created major new exposures that must be carefully managed, regardless of the level of individual technology usage. Failure to properly address such risks will undoubtedly damage a company’s ability to operate effectively. The only question is not will there be any disruption, but how extensive will it prove.”

Paul Skinner

Senior ICT Underwriting Specialist, Chubb Insurance Company of Europe

Chairman of the International Underwriting Association’s Digital Risk Working Party



Assessing and managing digital risk

In recent years there has been a great deal of publicity about business risks arising from the use of digital technology, yet considering how to address such issues can be a daunting prospect. This guide is designed as a starting point, for risk managers in particular and business leaders generally, to deal with potential exposures to digital risks and information security breaches. It outlines basic actions to take and provides references and contacts for further research and advice.

About the IUA

The International Underwriting Association of London (IUA) is the world's largest representative organisation for international and wholesale insurance and reinsurance companies. It is both a trade association, representing its members' interests internationally, and a market association supporting the business environment in London. Since 2001 the IUA has operated a Digital Risk Working Party, bringing together senior practitioners within the London insurance market. The group's principle objectives are to demystify the issue of digital risk and encourage a transfer of information between IT managers and underwriters.

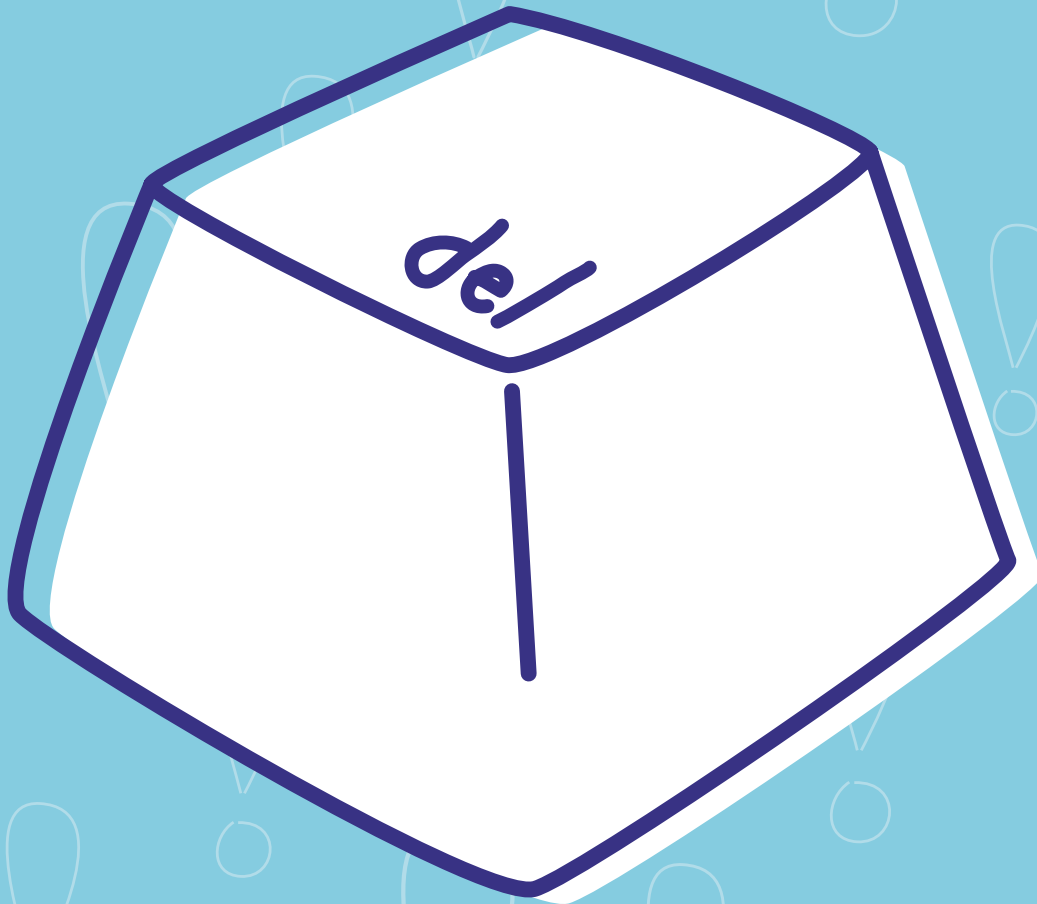


About the DTI

The Department of Trade and Industry (DTI) aims to increase the productivity of UK businesses and encourage confidence in the use of new information and communications technologies. The DTI works with business to raise awareness of the importance of effective information security management and to encourage the adoption of security standards such as ISO/IEC 17799 and BS 7799.



*A disgruntled former employee of a sheet metal company hacked into the firm's computer network and maliciously deleted key data records and files. Repairing the damage cost in excess of **£50,000***



What are digital risks?

There are few, if any, businesses that do not today rely in some way upon information technology. For many e-business is integral to day to day operations; without it competitiveness and profitability cannot be maintained. This growing reliance on technology usage has created major new exposures that must be carefully identified, assessed and managed. Perhaps the best way to start thinking about exactly what dangers digital risks pose is to consider some real life loss scenarios that have been seen in recent years by the London insurance market.

Example 1

A disgruntled former employee of a sheet metal company hacked into the firm's computer network and maliciously deleted key data records and files. Repairing the damage cost in excess of £50,000.

Example 2

Hundreds of thousands of pounds were paid to settle a legal action arising from a rogue email which incorrectly alleged a prospective government investigation into illegal practices at a leading financial firm.

The risks faced by firms using technology fall into one of two categories:

First party losses

These involve direct losses that your own business suffers because of damage done to your systems or other assets. Example 1 is a first party loss.

First party losses may also include theft of data, production secrets or other valuable documents perpetrated through unauthorised access to your information technology systems. A virus or computer hacking may prevent you from operating your business at full efficiency for days or even weeks. This may involve loss of revenue during the downtime, costs of recovering lost information and damage to your business reputation affecting the prospect of new business.

Third party losses

These are losses that occur due to claims made against you by a third party who is demanding compensation for damages that your actions are alleged to have caused.

Example 2 is a third party loss. Emails and the Internet can prove all too effective vehicles for the publication of libellous statements.

Third party losses may also arise from claims for breaches of rights of privacy; if customer information is inadvertently published online the Data Protection Act may be breached. Further third party risks can be caused by a failure to meet your obligations in the provision of products or services to your clients.

Many of the risks outlined above are little different from those traditionally encountered in the 'offline' world. Theft of key data, for example, has always been a threat. Yet the way in which such threats can now emerge is quite distinctive from any previous loss scenarios, marking out a new category of digital risk.

*Virus infections continue to account for by far the largest number of security breaches with two thirds of organisations that suffered any security incident claiming it was their **worst one***



Why should businesses be concerned?

Surveys have shown that many businesses believe their existing general insurance policies provide cover for digital risks. This is extremely unlikely to be the case. Traditional policies will normally only protect tangible assets and will generally exclude such risks. Other companies erroneously believe that there is simply no real protection available.

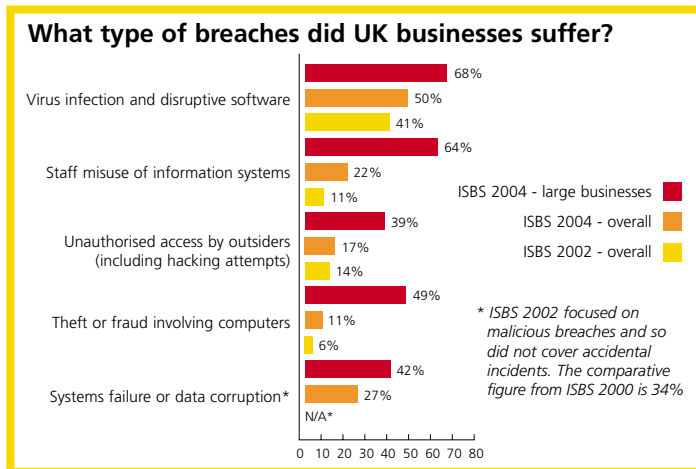
The result is that many businesses are operating without any proper management strategy for dealing with digital risks and are gravely exposed to potential losses. Ernst & Young's Global Information Security Survey 2004 revealed that nearly 70% of boards of directors do not receive a quarterly report about their organisation's information security status.

Yet there are important regulatory requirements that demand companies take digital risks more seriously than is apparently the case. The Turnbull Report places a duty on public company directors to identify, manage and mitigate all business risks while data protection legislation obliges organisations to ensure the security of their IT systems against breaches of confidentiality.

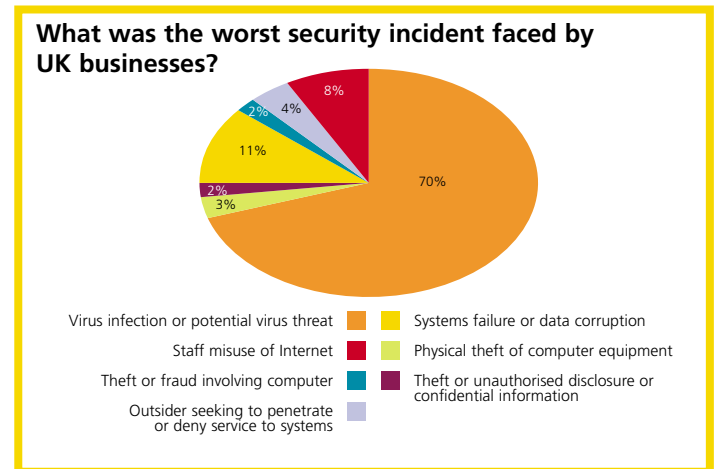
Furthermore a tendency to tempt fate can have catastrophic effects on both business continuity and reputation. Failure to properly manage just one risk can place an entire operation in

danger. The Department of Trade and Industry's 2004 Information Security Breaches Survey showed that the average UK business' worst e-security incident cost between £7,000 and £14,000. For larger businesses the typical range was from £65,000 to £190,000. The majority of such expense was accounted for by disruption caused to the day to day running of the business. Costs were also incurred in the time and money required to respond directly to the incident and there were direct financial losses such as loss of assets and damage to reputation.

The DTI survey also showed that all types of malicious security incidents have shown an increase since the same poll was last conducted in 2002. Virus infections continue to account for by far the largest number of security breaches with two thirds of organisations that suffered any security incident claiming it was their worst one.



© DTI Information Security Breaches Survey 2004



© DTI Information Security Breaches Survey 2004

The most important *first step* in tackling digital risk is to appreciate that it is not an issue that can just be left to an IT department or risk manager alone. The *interconnectivity* of *global e-systems* dictates that vigilance is essential at a number of different levels within an **organisation**



How can businesses deal with digital risks?

Risk assessment

The most important first step in tackling digital risk is to appreciate that it is not an issue that can just be left to an IT department or risk manager alone. The emergence of such risks is an overall business issue and has had a revolutionary impact on corporate governance requirements. The interconnectivity of global e-systems dictates that vigilance is essential at a number of different levels within an organisation.

Traditional risk managers with financial backgrounds are often divorced from the day-to-day operation of IT security programmes. A successful digital risk management strategy must therefore be a strategic, board-level topic with solutions implemented throughout a company and full cooperation between technical and business managers.

A risk assessment must be conducted to identify both a company's current areas of vulnerability and possible future problems. Issues to consider are day to day management and administration procedures, internal security measures and external protection. The risk assessment process itself should also be examined – is this a task that is regularly reviewed and updated?

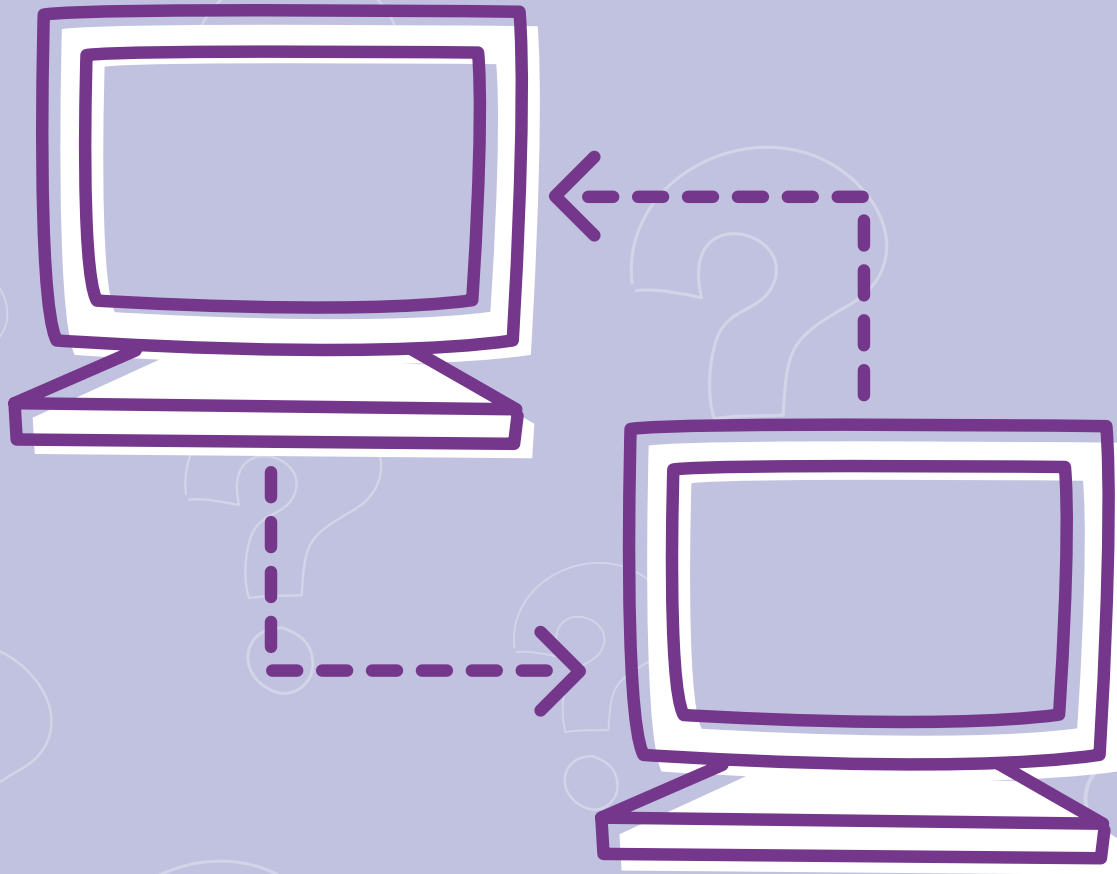
Information for this exercise may be obtained through interviews with key employees, a review of existing security documents and procedures and the conduct of dummy tests of current protection measures. For every risk identified, a set of proposals should be drawn up for its management together with further plans for how the risk can be reassessed in future. Furthermore each risk must also be assessed for its impact right across different internal areas of the company and, indeed, externally on clients and business partners.

The risk assessment process should keep in mind the business objectives of a company at all times. If this is not done it is likely that any resulting management strategy will be unbalanced with scarce risk management resources not focussed on the most pressing and relevant threats.

Key questions

- What are the threats to my company systems?
- How vulnerable are my systems?
- What is the likelihood that these threats could exploit these vulnerabilities and cause a serious incident or security breach?
- What impact would these incidents have on my organisation?

An employee Internet and email use policy should be drawn up, together with **guidelines** for the vetting of new employees. Such guidelines must also apply to outside contractors when they are provided with **access** to your **IT systems**



Risk mitigation

The best defences against the threats posed by digital risks are those that start at the very top of an organisation with effective management and corporate governance procedures that consider information security a priority.

From this starting point proper employee procedures and training programmes can be established; these must be regularly monitored, tested and adapted as necessary. Then, only after these management and employee level defences have been installed, can any technological barriers be effectively raised. IT security systems may include, for example, anti-virus software, firewalls, encryption programmes, intrusion detection and content filtering systems. All have the potential to provide a significant level of protection, but must be kept up to date and expanded as necessary to cope with any new technology that your business may choose to employ.

Technology, however, cannot be made completely secure simply through the addition of more technology. The human dimension cannot be ignored and an organisation's individual employees should be its strongest line of defence. IT security systems are reactive and should not be used in isolation, but dovetailed with a range of formal policies, procedures and training programmes throughout the company.

All policies should be clear and unambiguous in detailing the company's expectations about how to deal with any digital risks. They should provide explicit instructions and responsibilities for staff in the event of security breaches.

A basic information technology security policy will set standards for fundamental uses of, access to and storage of electronic data. In addition, an employee Internet and email use policy should be drawn up, together with guidelines for the vetting of new employees. Such guidelines must also apply to outside contractors when they are provided with access to your IT systems. Plans should also be drawn up for the frequent creation of back-up data. This should then be stored away from your company's main site and regular tests conducted to ensure that the back ups are operational. Any storage policy should include measures to guarantee the physical security of hardware and software. A business continuity plan is essential to ensure that all preventative action identified is properly undertaken to limit as much as possible the chances of an event occurring which may have devastating effects for the company. This plan will also include disaster recovery procedures allowing the business to react effectively in the event of any virus, computer hacking or other

loss scenario. Tests should be conducted on a regular basis to ensure that the business continuity plan still meets with the company's requirements and that the disaster recovery plan will run as smoothly as possible if or when it needs to be activated.

Alongside each of the above mentioned policies, appropriate training needs to be introduced for employees so that everyone is fully aware of their own individual obligations and accountability.

Key questions

What options do I have for managing the risks that have been identified?

- Reduce the risks by employing management, employee and technical controls.
- Avoid the risks by not engaging in particular activities or not deploying the technology that causes the risk.
- Transfer the risks through insurance cover or through legal or contractual means.
- Knowingly and objectively retain the risks.

What business objectives and legal or regulatory requirements do I need to consider in deciding the best way to manage the risks?

What are the costs and benefits for my company to ensure that we are minimising the risks whilst maximising company investments and business opportunities?

A best practice checklist

- Has an information security policy been established?
- Are employees given adequate training?
- Do employees know how to handle sensitive and critical business information?
- Are procedures in place for responding to security incidents and breaches?
- Is business information backed up on a regular basis?
- Is virus protection in place?
- Are risks regularly monitored and reviewed?

*It is vital to ensure that any coverage you purchase fits with the individual needs and risks of your own business. Buying insufficient cover or an inappropriate type of policy will result in a continual exposure to digital risks that may only be realised when it is **too late***



Risk transfer

Even the very best risk mitigation programmes can never be 100% effective. No matter how tight a security system may be, the possibility that it may be breached will always exist. Additional risk mitigation measures will also, of course, incur a cost that may offer diminishing returns in terms of a safer system.

Thus in order to properly manage digital risks most businesses will want to consider the possibility of transferring at least some of those risks to a third party through the use of insurance. The aim will be to limit potential financial losses by obtaining protective cover at a reasonable cost.

Insurance can be bought to cover most risks. It is vital, therefore, to ensure that any coverage you purchase fits with the individual needs and risks of your own business. Buying insufficient cover or an inappropriate type of policy will result in a continual exposure to digital risks that may only be realised when it is too late.

Traditional insurance policies do not cover the many new areas of digital risk. In recent years, however, specialised new products have been developed by insurers to help protect businesses. A lack of any historical claims data and concern over the potential scale of some digital risk losses initially restricted the amount of cover available. But in the London insurance market today there is an increasing number of specialist underwriters who meet the needs of a diverse range of businesses, from small firms with minimum requirements to the largest corporations.

The terms and conditions of different policies may vary greatly. Yet it may be possible to obtain cover for claims arising from both first party and third party losses. For example, insurers may meet claims to meet the cost of replacing or restoring electronic

records that have been corrupted by a virus or computer hacking. Lost income resulting from a temporary inability to conduct trade electronically may also be covered. Reputation protection may be available, including the cost of public relations advice to help limit any damage to your company's public standing.

Third party cover may meet losses resulting from a range of different claims that could be made against your company. For example it may pay for liabilities arising from libel contained in emails or website content, breaches of intellectual property rights and contravention of data protection legislation. If your company is held liable for forwarding an Internet virus or failing to deliver agreed systems support to a trading partner, an appropriate insurance policy may pay for any legal costs and damages you incur.

Risk mitigation policies and risk transfer through the use of insurance are two equally important elements of any successful digital risk management strategy. Neither will be completely effective in isolation. Together, however, they can form a comprehensive defence for businesses looking to ensure the security and integrity of their information technology systems. Certainly the cost of any insurance cover will be significantly reduced and its availability greatly enhanced for any company that has already properly conducted and acted upon its own risk assessment process.

Sources of best practice and further advice

ISO/IEC 17799

'Code of practice for information security management'

The international standard ISO/IEC 17799 (previously the UK standard BS 7799 Part 1) provides best practice on information security management. The aims of this best practice are to:

- minimise the risks and impacts to your business information systems,
- maximise your business investment and opportunities,
- ensure the continued availability of your business information systems, services and processes

The best practice found in ISO/IEC 17799 can be applied to an organisation's information systems to ensure that appropriate protection is given to the integrity, availability and confidentiality of its information. It covers best practice for managing risks across different areas of the business, for example:

- Organisational
- Human resources
- Third party services
- Business operations and communications
- Legal and regulatory compliance

Another standard, BS 7799 Part 2, defines a set of security processes (including risk assessment, treatment and reviews) for implementing a management system for managing information security risks and the best practice found in ISO/IEC 17799. This standard is used for third party audits of an organisation's management system for information security. It should be noted that ISO/IEC 17799 can be used without the use of BS 7799 Part 2.

BSI British Standards produces the PD3000 series of guides on implementing BS 7799 (available from www.bsi-global.com, tel 020 8996 9000).

The DTI acts as Secretariat for the UK ISO/IEC 17799 Users' Group which is free to join for any UK company using, or interested in using, the standards. Membership includes invitations to workshops as well as regular newsletters and updates on the standards. Please see the DTI Information Security website (details below) for a leaflet explaining about the Group and how to join.

The DTI produces a full range of Information Security publications as well as CD ROMs and workplace posters. These are available to download or order from the DTI's website at www.dti.gov.uk/industries/information_security. This home page also links to the DTI's infosec business advice web pages as well as to sources of advice about ISO/IEC 17799/BS 7799.

For further information from the
Department of Trade and Industry:

Tel: +44 (0)20 7215 1962
Email: InfosecPolicyTeam@dti.gsi.gov.uk
Address: Information Security Policy Team
Department of Trade and Industry
Bay 251
151 Buckingham Palace Road
London SW1W 9SS

For further information from the
International Underwriting Association:

Tel: +44 (0)20 7617 4449
Email: info@iua.co.uk
Address: London Underwriting Centre
3 Minster Court
Mincing Lane
London EC3R 7DD

Members of the IUA's Digital Risk Working Party

Member

Ben Maidment
Tim Humphries
David Walsh
Paul Skinner (Chairman)
Andrew Shefford
Barrie Razzell
Scott Farley
Deborah Finch (Secretary)
John Cross
Bob Donovan
Andrew Taylor
Chris Cotterell

Company

ACE Global Markets
Association of British Insurers
CFC Underwriting Ltd
Chubb Insurance Company of Europe
Ernst & Young LLP
International Underwriting Association
International Underwriting Association
International Underwriting Association
Limit Underwriting Ltd
Norwich Union
QBE International Insurance Ltd
Safeonline Ltd

Assessing and managing digital risks, Project Advisor: Ted Humphreys