

CYBER RISKS EXPLAINED

WHAT THEY ARE, WHAT THEY COULD COST AND HOW TO PROTECT AGAINST THEM



WHAT THIS BRIEFING COVERS

▶ Introduction

▶ Section 1: What are the risks and the impacts?

- Cyber crime and cyber terrorism
- Accidental loss of your own or someone else's data
- Liability for your online activities or comments made in emails
- Physical loss of systems

▶ Section 2: What can be done to mitigate the risks?

- Where to start
- Risk control mechanisms

▶ Section 3: What is the insurance position?

- Gaps in traditional insurance policies
- Specialist insurance options

▶ Our offices across UK and Ireland

INTRODUCTION

In the modern business environment, use of and interaction with electronic data and the internet is a normal - even critical - business activity. It can bring significant business efficiencies and growth opportunities, but also a range of particular risks that need to be understood and mitigated. For the purposes of this guide we are defining these as cyber risks, i.e. the specific risks that relate to the use of computers, information technology and virtual reality.

The costs and impacts can be considerable. For example:

- The government has recently published figures highlighting that the cost of cyber crime in the UK is £27 billion a year, of which £21 billion is cost to businesses. Nearly half of this relates to theft of intellectual property – a critical asset for many firms.
- The recently published National Security Strategy places cyber attack (including by other states, by organised crime and by terrorists) as one of the four highest priority risks for the UK currently and over the next five years.

HELP IS AT HAND

As with any risk, there is much that can be done to mitigate your position and protect yourself against costs, litigation and damage to reputation.

As the world's leading risk and insurance services firm, Marsh has a 140 year history of helping organisations respond to new and emerging risks. This document explains the risks, the risk management actions that can be taken and the insurance options available.

FOR FURTHER INFORMATION AND ASSISTANCE, PLEASE
CONTACT YOUR USUAL MARSH REPRESENTATIVE OR E MAIL
NATIONAL.ENQUIRIES@MARSH.COM

SECTION 1: WHAT ARE THE RISKS AND THE IMPACTS?

The cyber risks to the business can be split into the following broad areas:

- losses due to cyber crime and cyber terrorism
- accidental loss of your own or someone else's data
- physical loss of systems
- liability for your online activities or comments made in emails.

We explore each of the areas in the following paragraphs.

CYBER CRIME AND CYBER TERRORISM

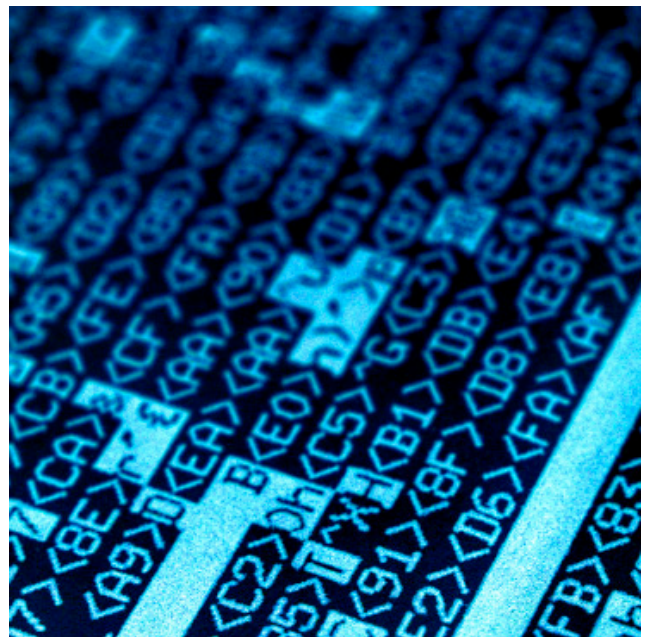
A lot of financially motivated crime has now gone digital. Criminals are increasingly seeking to exploit vulnerabilities in the internet and electronic systems for financial gain. And the bad news is, it is businesses that are suffering the most.

A recent study estimates the economic cost of cyber crime to UK businesses is £21bn per annum. This estimate includes:

- £9.2bn per annum from theft of intellectual property (copyright, ideas, designs, methodologies and trade secrets).
- £7.6bn per annum from industrial espionage (stealing of competition sensitive information which could impact a company's chances of winning open tenders and the loss of information which could enable cyber criminals to gain advantage from share price movements).
- £2.2bn per annum from extortion (cyber criminals hold a company to ransom, e.g. through the deliberate crashing or hacking of systems, or by manipulating company website links, which can lead to extensive brand damage).

- £1.3bn per annum from direct online theft (e.g. fraudulently obtaining access and looting company accounts and monetary reserves).
- £1bn per annum from the theft of sensitive customer data from cyber attacks.

Source: *The cost of cyber crime*: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office. February 2011. <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>



SECTION 1: WHAT ARE THE RISKS AND THE IMPACTS?

“ THE RESULTS OF THIS STUDY SUGGEST THAT BUSINESSES NEED TO LOOK AGAIN AT THEIR DEFENCES TO DETERMINE WHETHER THEIR INFORMATION IS INDEED WELL PROTECTED. ENCOURAGING COMPANIES IN ALL SECTORS TO MAKE INVESTMENTS IN IMPROVED CYBER SECURITY, BASED ON IMPROVED RISK ASSESSMENTS, IS LIKELY TO CONSIDERABLY REDUCE THE ECONOMIC IMPACT OF CYBER CRIME ON THE UK.”

QUOTE FROM THE COST OF CYBER CRIME REPORT

The government’s recently published National Security Strategy puts cyber attack in the four highest priority risks for the UK currently and over the next five years.

You can find out more at http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

The report includes consideration of cyber terrorism – that is, acts directed towards the overthrowing or influencing of the government. Cyber terrorism could be a concern to businesses operating in sectors linked to the government or infrastructure, for example transport, communications, health; as they may form part of the target for a cyber terrorism attack.

SECTION 1: WHAT ARE THE RISKS AND THE IMPACTS?

ACCIDENTAL LOSS OF YOUR OWN OR SOMEONE ELSE'S DATA

Crime is not the only way that data can be lost or compromised. Regular press articles about lost laptops, memory sticks and CDs are a reminder of the vulnerability of data held electronically. Other causes of data loss include viruses, natural disasters, fires, accidental or deliberate deletion, system crashes, corruption and hardware failure.

BUSINESS IMPACTS OF DATA LOSS INCLUDE CLAIMS FROM CUSTOMERS AND SUPPLIERS FOR BREACH OF CONFIDENTIALITY, BREACH OF CONTRACT AND NEGLIGENCE, DIRECT REVENUE LOSS, INTERRUPTION TO BUSINESS AND DAMAGE TO REPUTATION. THERE CAN ALSO BE ADDITIONAL WORK AND EXPENSE IN CRISIS CONTAINMENT AND MANAGING ADVERSE PUBLICITY.

RESEARCH BY THE PONEMON INSTITUTE FOUND THAT, IN 2009, THE AVERAGE COST TO A UK ORGANISATION OF A DATA BREACH WAS £1.68 MILLION. MUCH OF THE COSTS RELATED TO LOST BUSINESS OR MEASURES TO PREVENT A LOSS OF CUSTOMER TRUST.

(SOURCE: ANNUAL STUDY: COST OF A DATA BREACH, PONOMON INSTITUTE JANUARY 2010).

[HTTP://WWW.ASA.ORG.UK/MEDIA-CENTRE/2010/ASA-DIGITAL-REMIT-EXTENSION.ASPX](http://www.asa.org.uk/media-centre/2010/asa-digital-remit-extension.aspx)

Data losses resulting from outsourcing data to third parties were found to be common, as were breaches resulting from lost laptops and other mobile devices.

There is also the regulatory position to consider. The Information Commissioner has a range of sanctions available, including the ability to levy a fine of up to £500,000 for loss of sensitive personal data. See http://www.ico.gov.uk/for_organisations.aspx

PHYSICAL LOSS OF SYSTEMS

Cyber activity often requires a physical information technology system. Therefore it is important to consider the risk of loss or damage to physical equipment. It can be damaged by anything from a fire to a temperature change in a server room, from a flood to an electrical surge.

LIABILITY FOR YOUR ONLINE ACTIVITIES OR COMMENTS MADE IN EMAILS

Electronic communication can be of great benefit to businesses. However, it can also produce threats. An incorrect, misleading, libellous or even illegal statement on a website, or in an email, can lead to compensation claims and damage to reputation. Social networking by employees can result in liabilities for employers and is more difficult to control than official business email.

For businesses engaged in online trading (selling goods and services via a website) there are additional risks. For example, failure to keep customer login or payment card data secure can lead to a large volume of compensation claims. Incorrect pricing of a product can lead to financial shortfalls.

Marketing communications on websites are now covered by the The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP code). This includes rules relating to misleading advertising, social responsibility and the protection of children.

SECTION 2: WHAT CAN BE DONE TO MITIGATE THE RISKS?

WHERE TO START

The starting point is to identify and assess the specific risks and impacts to your business.

Create an inventory of the critical business data and information you hold in electronic format (customer and supplier data, employee records, financial information, designs, product specifications, plans, etc.) Then ask yourself what the impact would be if you lost any of it. What controls do you have in place? Could they be improved?

A similar process can be followed in respect of your online content. Create an inventory of your websites, intranets, any mobile sites and applications. What is the process for adding, removing or changing content on them and how is it controlled?

Find out how much you and your employees are engaged with social networking sites and how much they are identified with you, their employer. Do you have a policy regarding use of social networking, and has this been communicated effectively to employees?

What is your dependency on third parties? (For example, in respect of data outsourcing, website management, equipment and networks.) How much do you know about them and their competencies? What legal and contractual controls do you have in place?

What business critical information and data technology systems do you have and how is the equipment that runs them protected?

What plans do you have in place for manual workarounds for critical functions such as payroll, finance, manufacturing, etc. if you lost your IT systems?

SECTION 2: WHAT CAN BE DONE TO MITIGATE THE RISKS?

RISK CONTROL MECHANISMS

Once you understand the extent of the risks, you can consider control mechanisms, which should then be recognised in the organisation's formal cyber risk policy and procedures. While the specific controls will be unique to each business, we have shared some examples below, split into six broad areas:

Security: We recommend you look at:

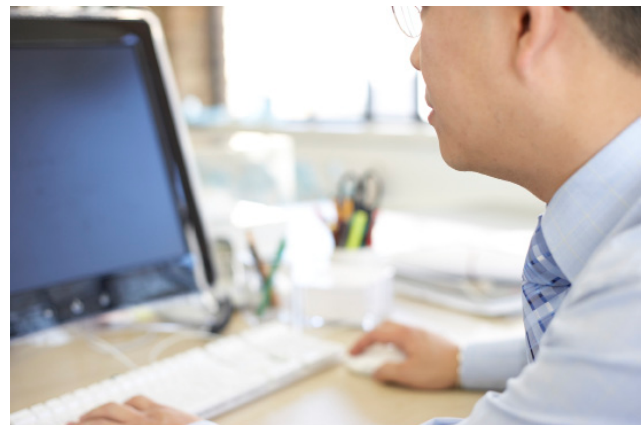
- Physical security at operating locations (intruder detection, access restrictions, locks, etc).
- IT system security (segregated networks, with isolation of business critical information and data, system intruder detection, identity and access management, anti malware tools, etc).
- Data security, e.g. encryption especially of mobile equipment, anti spyware, etc.

IT security management should be centralised, so it can be uniformly enforced across the entire IT network in the business.

Legal controls: Work with your legal advisers to ensure you have robust legal protections in place where possible. These include:

- Patents
- Copyrights
- Secrecy and confidentiality clauses in contracts, including employment contracts.

Whilst these will not protect against criminal acts, they could at least give you a level of protection against an accidental breach and may serve to focus the minds of contractors and outsourcing parties as to their own responsibilities and the controls that they should maintain.



Contractor and partner vetting: When a procurement exercise is undertaken, an assessment of the candidates' risk management controls should be an important part of the selection criteria. If they are interacting with your information technology systems or data, you should ask to see their cyber risk management policy and procedures.

- Make sure you are comfortable with their proposed physical and management controls.
- Do you consider their employee training and communication around data protection to be adequate?
- Obtain details of any previous incidents and losses and any remedial action taken.
- Do they have employee vetting and monitoring processes in place (especially if they are to handle sensitive data)?
- Do they have any insurance in place which could provide some protection?

SECTION 2: WHAT CAN BE DONE TO MITIGATE THE RISKS?

Employee training, communication and vetting:

Dealing with electronic data and messaging is now such a routine part of daily working and personal life that employees may not be alert to the risks stemming from inadvertent or malicious actions. Therefore we recommend the following:

- Develop a robust policy and procedures, backed up with the potential for disciplinary action if a breach occurs.
- Develop and deliver a training course to communicate the issues and procedures to employees, followed up with regular reminders about data security and messaging policies.
- For those staff handling sensitive data, more detailed and specific training should also take place.
- You should consider background screening and vetting to employees handling sensitive, confidential information.

Post event plans: In addition to the preventative measures profiled earlier, we recommend you consider how you would react if an incident did occur.

- This involves formulating plans to deal with the crisis and recovery of the business/business systems.
- Media and public relations strategies to manage crisis communications need to be part of the plan, as some incidents could become high profile and public.
- So too do communications to individuals and/or organisations whose data has been lost or compromised.

HOW MARSH CAN HELP YOU

MARSH CAN FACILITATE AN IT AND DATA SECURITY WORKSHOP TO HELP YOU IDENTIFY AND ASSESS THE SPECIFIC RISKS TO YOUR BUSINESS. WE CAN THEN WORK WITH YOU TO DEVELOP A COSTED AND TIMED ACTION PLAN TO ENHANCE CONTROLS.

Insurance: This is an important part of a cyber risk management strategy. It is a complex subject and in the next section we explain what cover is typically available under standard insurance policies and go on to profile the protection provided by specialist cyber risk insurance policies.

SECTION 3: WHAT IS THE INSURANCE POSITION?

GAPS IN TRADITIONAL INSURANCE POLICIES

Property and business interruption policies: these typically limit cover to loss or damage to tangible physical property, and resulting loss of revenue, resulting from an insured physical peril (fire, flood, etc.) Computers and the data contained on them are susceptible to some specialist causes of damage, which will not be covered if you are insured on this basis. For example, damage resulting from a change in temperature in your server room, loss of power supply, software corruption or breakdown, are not covered by a standard property or business interruption policy. Neither is accidental loss or theft of data and the resulting financial impact.

Theft insurance policies: These often limit cover to theft of tangible assets following forcible or violent entry to/exit from the premises. They would therefore not pick up theft of data, which is an intangible asset and one which is often stolen remotely. Even if 'full theft' cover is in force, i.e. without the need for forcible or violent entry to/exit from the premises, arguments regarding cover for data, as an intangible asset, remain.

Terrorism insurance policies: These work on the basis of physical damage, so a cyber attack designed to compromise the information technology infrastructure - but usually without physical damage - would not be covered.

Fidelity guarantee/crime policies: These generally limit cover to direct loss resulting from theft by employees of money, securities or other tangible property. Even broadened coverage under a computer crime extension limits cover to the cost of recollecting or restoring the damaged or corrupted data. These policies will often specifically exclude cover for the actual theft of data or information.

General liability and errors and omissions policies: These usually only respond where there has been negligence on the part of the insured. They usually exclude cover for criminal or deliberate acts of the insured or its employees, and expenses associated with a privacy breach (such as notification costs and regulatory defence). Some policies also specifically exclude any liability for electronic data.

SECTION 3: WHAT IS THE INSURANCE POSITION?

SPECIALIST INSURANCE OPTIONS

Marsh's specialist computer insurance facility: This widens cover for information technology risks to include:

- Damage or business interruption due to hacking, virus or misuse of data.
- Publicity costs directly relating to the protection of brand image (i.e. to counter the impact of negative press coverage flowing from damage and/or loss of information).
- Full theft cover on computer equipment and data, without security requirements.
- Cover whilst in transit or located outside the UK.
- Loss of information (loss, distortion, corruption or erasure of programmes and data).
- Breakdown cover (without the need for a maintenance agreement), in respect of desktop PCs and portable computer equipment.
- Residual breakdown cover on all other computer equipment.
- Additional expenditure incurred following unexpected failure or impairment of external IT or power supply.
- Cost of replacement licence agreements.
- Damage to computer equipment following a change in temperature, including resultant reinstatement of data and/or additional expenditure.

Specialist cyber insurance (available through Marsh with a range of insurers): This can provide even wider protection including:

- Legal liability to others for computer security breaches.
- Legal liability to others for privacy breaches (including breaches by the insured's third party contractors).
- Legal liability for online media content.
- Costs associated with regulatory actions and scrutiny.
- Loss or damage to data/information.
- Loss of revenue due to a computer attack.
- Extra expense to recover/respond to a computer attack.
- Loss or damage to reputation.
- Privacy notification costs.
- Identity theft.
- Cyber extortion (e.g. ransom costs or investigative expenses).
- Cyber terrorism.

Note: the descriptions of insurance covers contained in this section are outlines only. Terms, conditions and limits apply. Full details are available on request.

HOW MARSH CAN HELP YOU

MARSH CAN CARRY OUT AN INSURANCE GAP ANALYSIS TO ESTABLISH THE EXTENT AND LIMITATIONS OF YOUR EXISTING INSURANCE PROTECTION FOR CYBER RISKS. THEN WE CAN OBTAIN QUOTATIONS FOR SPECIALIST COMPUTER, OR WIDER CYBER RISK, INSURANCE COVER, TAILORED TO THE PROFILE AND REQUIREMENTS OF YOUR BUSINESS.

OUR OFFICES ACROSS THE UK AND IRELAND

For details of the nearest and most appropriate Marsh claims expertise that is available to you, please contact your Marsh Client Executive.

ABERDEEN	+44 (0) 1224 577 800	HAYWARDS HEATH	+44 (0) 1444 335 267
BELFAST	+44 (0) 2890 556 100	ISLE OF MAN	+44 (0) 1624 691 900
BIRMINGHAM	+44 (0) 121 452 1200	LEEDS	+44 (0) 113 209 5800
BRISTOL	+44 (0) 117 906 5300	LEICESTER	+44 (0) 1162 542 321
CARDIFF	+44 (0) 292 043 1000	LIMERICK	+353 (0) 61 319 155
CARLISLE	+44 (0) 122 856 4470	LONDON	+44 (0) 20 7357 1000
CORK	+353 (0) 21 490 7400	MIADSTONE	+44 (0) 1732 877 500
DERRY	+44 (0) 2871 343 121	MANCHESTER	+44 (0) 161 954 7200
DUBLIN	+353 (0) 1 604 8100	MILTON KEYNES	+44 (0) 1908 846 000
EDINBURGH	+44 (0) 131 311 4200	NEWCASTLE	+44 (0) 191 222 3200
GALWAY	+353 (0) 91 596 200	READING	+44 (0) 118 958 5235
GLASGOW	+44 (0) 141 304 4300	SOUTHAMPTON	+44 (0) 2380 218 700



For further information, please contact your local Marsh office
or visit our web site at: marsh.com

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Services Authority for insurance mediation activities only.

Marsh Ltd, trading as Marsh Ireland is authorised by the Financial Services Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules only.

Registered number: 1507274 Registered office: 1 Tower Place West, Tower Place, London, EC3R 5BU

© Copyright 2011 Marsh Ltd All rights reserved Ref: 802579430040460F_Exp Apr 2013