ZURICH®

Security & Privacy Current cover and Risk Management Services

Introduction

Technological advancement has enabled greater working flexibility and increased methods of communications. However, new technology brings about new risks with one of the most commonly reported thefts being that of personal data.

Information risk management is recognised as being one of the fastest emerging risks facing all organisations today. Unlike IT (hardware, systems etc.) this most commonly relates to the platforms in which information is held and exchanged. Exposure to Information Risk will vary depending on an organisation's business. Some of the potential costs incurred are tangible, such as fines or penalties whilst others are reputational, both of which can result in considerable financial costs:

- The Information Commissioner's Office (ICO) confirmed that public sector authorities have now paid over £4m in fines for breaches of the Data Protection Act since they have had the ability to levy fines from April 2011 (V3.co.uk 2nd September 2013)

And;

- The average cost of a data breach for a UK organisation is in excess of £2m (source: Ponemon Institute).

Added to this is the cost of mitigation, which can be approximately three times the cost of the original fine.

But where is the greatest risk coming from?

One of the greatest risks is the lack of clarity and understanding of the term, 'information risk'. There is a misconception that it is purely an IT issue with organisations trusting in technology to mitigate this risk, when in fact, in broad terms, over 70% of an organisation's information risk exposure comes from their own employees, be it by negligence or malice.

The purpose of this document is to provide you with a variety of scenarios where a loss can happen. It highlights what consequences it could lead to and the remedies that are currently available under your Zurich policy wording and the Risk Management solutions that we can also provide.

The impact from a data loss incident or a data breach can lead to serious repercussions for an organisation, whether it is the fines levied by the Information Commissioner's Office or the damage to reputation that it will inevitably bring within the media. As pending EU legislation is designed to supersede the existing Data Protection Act, organisations should make themselves even more aware and have solutions in place to try to mitigate data losses and breaches.

As detailed within this document Zurich already provides cover for the key concerns related to information risk and public sector information.

What is Information Risk Management?

We think of Information Risk Management as being:

"…an organisation's ability to identify business critical data, its inherent value to the business and others and to subsequently protect the confidentiality, integrity and availability of that information proportional to the risk to customers, the business and the extended enterprise."

Information Risk Management enables organisations to inform and prioritise decisions on the deployment of valuable resources and direct improvements in the protection of that critical information.

Information risks can be broadly categorised into three overarching themes:

1. Accidental data loss, source organisation, customer and partner/supplier
2. Physical system failures, which also includes infrastructure failures and breaches
3. Direct malicious cyber-attacks

In mitigating these, an organisation needs to know its information flows, understanding **what** the information is to be used for; **how** and **when** is it to be shared; having assurance that its retention and disposal procedures are effective and compliant with regulatory and industry standards.

"…once risks are classified they can be measured, once risks are measured they can be managed…"

(Jorion, P. 2002)

The following sections provide examples of scenarios where a loss could happen as well as highlighting what consequences it could lead to, as well as identifying the remedies that are currently available under your Zurich policy.

Data Breach

INTRODUCTION

Private information you hold about a Third Party is made public. Examples of how this can occur include: a lost laptop or hard copies of data, an attack from hackers or malicious persons and information sent to the incorrect recipient

CONSEQUENCES

Affected people suffer a loss and a Claim is bought against you for a **breach of the Human Rights Act**

Affected people suffer a loss and a Claim is bought against you for a **breach of confidence**

Affected people suffer a loss and a Claim is bought against you for **breach of the Data Protection Act**

ZURICH POLICY RESPONSE

If the Claim relates to **bodily injury**, **illness** or **financial loss** suffered by a member of the public, Public Liability cover will protect against legal costs and damages awarded against you. If the Claim relates to injury to an employee then your Employers' Liability cover will apply

If the Claim relates to **compensation** under Section 13 of the Data Protection Act, Legal Expenses will protect against this

Business Interruption

INTRODUCTION

Your ability to trade online is disrupted as a result of computer equipment being damaged or breaking down

CONSEQUENCES

Your **revenue streams are reduced** (no hacker/malware/virus involvement)

You incur **additional costs** to maintain your computer systems and services until normal functioning is restored (no hacker/malware/virus involvement)

ZURICH POLICY RESPONSE

An extension under Business Interruption cover will protect against both **lost revenue** and **increases in operating costs** during a disruption to your computer networks

Wrongful Publishing

INTRODUCTION

Content that is published on your website infringes the rights of a Third Party. The content may be libellous or may represent a breach of intellectual property such as plagiarism, breach of copyright or trademark

CONSEQUENCES

Content published on your website is accused of being **libellous** and a Third Party sues for damages

Content published on your website is accused of **breaching a Third Party's intellectual property** (plagiarism, breach of copyright or trademark) and a **Third Party suffers a financial loss and sues for damages** which they claim against you

ZURICH POLICY RESPONSE

Our Libel and Slander section will cover defence costs and indemnify against legal costs and damages awarded as a result of **libellous publications on the organisation's website**

Claims made against you for **financial losses** arising from breaches of intellectual property will be covered under our Public Liability section under the financial loss extension

Damage to Computer Records

INTRODUCTION

Your computer systems suffer a breakdown or physical damage which causes computer records and data to be damaged, or your data or software is erased, destroyed or distorted

CONSEQUENCES

Your **computer systems break down** or suffer physical damage

Data or Software **is erased**, **destroyed**, **corrupted** or **distorted**

ZURICH POLICY RESPONSE

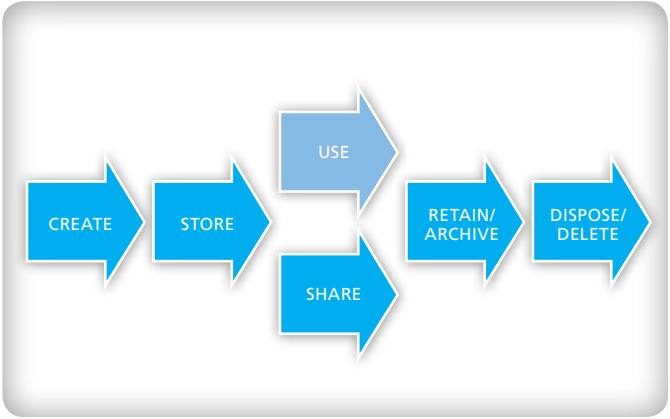
Our All Risks section includes £5,000 cover for computer equipment which **breaks or burns out from mechanical or electrical defect**. Our Material Damage section includes £10,000 cover for damage to computer records

Our Business Interruption section includes cover up to £5,000 for **loss or damage to data or information** which isn't accompanied by visible and identifiable damage to the data carrying media

Risk Management Services

How can Zurich support you?

As this diagram illustrates, the key is for organisations to take a holistic approach to the management of information-related risk.



We understand that information management consists of both physical and electronic forms. To be able to mitigate the risks associated with the use of these modes an organisation must understand the information lifecycle, irrespective of the information source.

The end-to-end information lifecycle consists of six interlinked components, visually represented in the diagram, all of which need to be understood and given the appropriate level of ownership. An organisation needs to risk assess each element to:

- Determine the correct strategy and approach, ensuring its information management approach supports the attainment of organisational objectives
- Understand the value of the information in the lifecycle and any one time
- Know the sequence and interaction of the information flow, ensuring that all of the six elements effectively operate from end to end
- Respond to regulatory and customer requirements
- Determine budget allocation, being able to optimise information security investments in support of business objectives
- Assess and respond to incidents, being able to share understanding of the risk profile and what needs to be done

Furthermore, employees and where applicable Board and Committee Members, must understand the risks associated with each phase of the information flow, being held accountable to why they create, store, use and share information. They need to understand and adhere to their organisation's archive and disposal procedures. They must appreciate that they are not passive recipients to this risk and that they share ownership and responsibility with their organisations IT department to protect both their organisations and their customers information.

Whatever your concern, Zurich is dedicated to working directly with you, to produce organisation-wide benefits. Some of our services in helping you improve your security & privacy precautions are outlined below:

Corporate Diagnostic	This process acts as a health check of existing data security strategy and processes against the organisation's core objectives, business plans, regulatory environment and industry best practice

The results of the Corporate Diagnostic will help us work with you to draw up an action plan for future development, consisting of the following elements:

Service-specific Diagnostic	A tool to enable a deep-dive diagnostic into an identified service area, partnership, contract etc.
Information Governance Assurance Framework	A pragmatic framework developed using insight from Zurich's wide sector knowledge, and their own experience of information risk management
Third Party Assessment and Mapping	Exploring information management and communication supply chain across key partners and suppliers, such as IT providers, contractors etc. to gain assurance that information is being managed, shared and disposed of properly
Awareness and Training	Addressing cultural and behavioural issues to mitigate the threat of negligence and error and to increase the level of information risk awareness across employees, Board, Members etc.
Resilience Review	"Critical friend" review of business continuity and disaster recovery arrangements, to ensure that recovery plans adequately reflect actual and planned outage, and that IT arrangements can support recovery requirements

Why Zurich?

Because we speak from experience. As a wider organisation we faced an incident which incurred a large penalty, leading to us greatly improving and refining our internal information security arrangements. This, combined with our in-depth knowledge of our customers' issues and experiences, gives us unique insight into information risk and we have developed bespoke tools to mitigate it.

For more information on how we can help you, or to arrange for a free consultation, please contact your Risk & Insurance Consultant.


F9
F8
F7
Enter
Shift
Ctrl
Alt

Zurich Insurance plc
A public limited company incorporated in Ireland. Registration No. 13460.
Registered Office: Zurich House, Ballsbridge Park, Dublin 4, Ireland.
UK Branch registered in England and Wales Registration No. BR7985.
UK Branch Head Office: The Zurich Centre, 3000 Parkway, Whiteley, Fareham, Hampshire PO15 7JZ.

The pulp used in the manufacture of this paper is from renewable timber produced on a fully sustainable basis. The pulp used in the manufacture of this paper is bleached without the use of chlorine gas (ECF – Elemental Chlorine Free). The paper is suitable for recycling.

ZURICH®

716401001 (03/14) RRD