Cyber

Protection against cyber-attack and data breach

ansvar
Insuring the heart of your community

Cyber

Protection against cyber-attack and data breach

These guidance notes are intended to help you understand the common risks and responsibilities you are likely to face. The information provided in this guide is by no means exhaustive.

We would encourage you to be proactive in the management of cyber risks to which your organisation may be exposed to.

The information in these guidance notes is given in good faith and is based on our understanding of current law and best practice. Ecclesiastical Insurance Group plc, including Ansvar Insurance, cannot accept any responsibility for action taken as a result of information provided in this publication. It is your responsibility to ensure that your organisation complies with its legal responsibilities and any interpretation or implementation of this guidance is at the sole discretion of your organisation or other party who may read these notes.

Contents

What are cyber risks?

Organisations have become increasingly reliant on technology to carry out their activities. Almost all organisations use or have access to the internet in some way.

Technology and the internet are revolutionising the way organisations communicate with others and how they handle and manage data. However, this has increased the risk of data being compromised by criminals, who can make large sums of money from accessing and stealing data. In addition, legislation can impose penalties on an organisation for not taking appropriate steps to secure or prevent access to data relating to individuals. All of which could result in significant financial loss, disruption to your activities, or damage to your reputation.

These risks aren't just a problem for large organisations; small and medium-sized organisations with fewer data security resources are particularly vulnerable.

Common cyber exposures

Liability

Organisations have certain responsibilities when managing, securing and using data. Failure to adhere to these responsibilities could result in enforcement action by the regulator and the imposition of fines. At the same time, if the person or organisation to which the data relates suffered a financial loss, or harm to their reputation because of your failure to adhere to these responsibilities, a civil liability could be created. This could result in you having to pay:

a) compensation (damages) to the affected party,
b) their legal costs (in the event you were unsuccessful in defending a legal action),
c) your own legal defence costs.

Public liability insurance normally covers the above costs that you may have to pay for third party property damage or bodily injury that arises from your negligence. However, a loss of data will not necessarily involve damage to property (or injury) and as such, standard public liability insurance will not offer protection against the costs arising from a 'cyber liability' (although some cover may be provided as an extension to a policy). Professional indemnity (PI) insurance may offer some protection, but cover can vary and this will be dependent on you having PI cover.

Claims example

Property management firm's email system became corrupted. IT investigation needed to confirm a virus was the cause. Former customer sued for damages after being infected via an email.

Claim £45,000

Common cyber exposures

Expenses following a data-breach

The costs to you following an unauthorised or inadvertent loss of data are not limited solely to legal costs and any amounts of compensation you may have to pay. You may incur further costs:

a) investigating the extent of the issue, which may include hiring professional persons to undertake this for you,
b) informing affected parties that their data has been lost or illegally accessed,
c) providing support to affected parties, which may include providing helplines and specialist help because of the effects of identity theft, and
d) reducing the impact of a loss of data on your reputation, which may include hiring public relations specialists.

Civil law is compensatory in nature. The law compensates victims of a civil wrong, but (with the exception of injunctions) it makes no provision for limiting or reducing the after effects of a civil wrong. Public liability insurance works on a similar basis by indemnifying you for the costs arising from you being legally liable to compensate another. Cover to reduce or limit the effects of an incident may exist by extension to a public liability policy, but cover varies by insurer. However, specialist cover to reduce or limit the after effects of a loss of data is also available.

Claims example

Accountant's laptop stolen containing 800 customer tax records. Cost to investigate breach, take legal advice and notify clients.

Claim circa £35,000

Damage to computer systems and business interruption

You may also incur additional expense in repairing damage to your computer systems (including your websites) following an incident of hacking, a computer virus or corruption of data.

Insurance policies covering damage to material property ordinarily only respond if there has been *physical* damage to your property (for example, a fire damages your laptop). Insurance cover for *non-physical* damage to property (including damage by a virus) is normally catered for by specialist insurance policies.

Continued...

Continued...

Any incident of hacking, a computer virus or corruption of data that means you are unable to use your computer systems may also have an effect on your activities and could leave you potentially unable to trade. This may result in a loss of income, or additional expense to minimise the impact of this interruption to your organisation (for example, temporary hire of replacement computer equipment). In the event a fire damaged your property and left you unable to trade, a normal 'business interruption' insurance would pay for this loss of income and also the additional expenses you incur in reducing the effect of the interruption. However, as noted above, cover for business interruption following *non-physical* damage is normally catered for by specialist insurance policies.

Claims example

Ransomware encrypted the files of a computer system. Costs incurred to clean the system and restore data.

Claim circa £31,300

Crime

Illegal access to your computer system or those of businesses that you hire to provide services for you could result in money being taken from a bank account or credit arrangements (such as loans or overdrafts) being arranged in your name for the benefit of a fraudster. There is also the possibility that someone could attempt to extort money from you by threatening to damage your computer system or steal data. Protection against such risks can be catered for by specialist insurance policies.

Claims example

Employee fraudulently modified information which resulted in a transfer of funds.

Claim circa £12,800

Risk management

There are practical steps you can take to reduce the:
a) likelihood of a 'cyber event' occurring
b) impact a cyber event has on your organisation.

These include, but are not limited to, the following:

- Data back-up. You should back-up your data regularly and at least once a week. In the event your computer systems have to be restored or rebuilt this will make the process quicker and reduce the impact on your organisation. It is important that any device used to back-up data is removed from your computers when not in use, this will reduce the risk of a virus spreading and corrupting the backed-up data.
- Anti-virus software. Free software should not be used. Your anti-virus software should be updated at least once a week. Where possible you should enable automatic updates. This will reduce the likelihood of you being infected with a computer virus.
- Firewalls. You should have in place maintained firewalls to control access, and prevent unauthorised access, to your computer system. Ensure that security precautions on devices are enabled, disabling security precautions may be convenient but it will also increase the risk of infection.
- Email and internet usage. You should have in place an email and internet usage policy that all staff (including volunteers) should adhere to. Computers should only be used for your business or charitable purposes and users should not be permitted to download software or apps from untrusted sources. This will reduce the risk of employees accessing inappropriate or potentially damaging websites.
- Background checks. For new members of staff (including volunteers) you should undertake credit checks and where appropriate, checks with the Disclosure and Barring (DBS) service. Cyber events are not always attributable to external sources and can arise from rogue or disgruntled employees stealing data or sabotaging the system.
- Transferring money. You should have in place documented procedures that requires staff to ensure payment requests are genuine and can be verified prior to making any payment. Staff should be vigilant and treat any unexpected emails requesting bank details or the transfer of funds with suspicion.
- Data service providers. Anyone providing data storage or data services for you should be located in the UK, Channel Islands or the Isle of Man. This will ensure adequate levels of protection for your data, in line with statutory requirements, are in place.
- Password security. Passwords should be unique, strong and changed regularly to reduce the risk of unauthorised access to your system.
- Limiting access. Access to systems and functions should be limited to only those staff or volunteers who need access to that system or function to carry out their role. Access should be revoked for staff or volunteers who leave the organisation, or who change roles within the organisation and no longer require access to a particular system or function.
- Data privacy and information security policies. You should have in place comprehensive data privacy and information security policies. This should include training, so all staff and volunteers are aware of their responsibilities. These policies should be updated regularly and after any incident.
- Crisis management. A crisis management policy will ensure your organisation can:
  a) respond quickly to, and
  b) mitigate the impact of
  an actual, or alleged, data breach or a cyber event. Being prepared in advance will reduce the impact any incident has on your organisation.

- Hardware destruction policy. When documents are disposed of, or any hardware is disposed of or sold, all information and personal data should be removed to reduce the risk of a third party accessing this data.
- Data encryption. Any sensitive data sent to third parties or stored or transferred onto portable devices (such as USB sticks) should be encrypted.
- Update systems. Systems, software and devices should be kept up to date with the latest updates. Computer viruses are often designed to exploit known flaws in older software and devices, keeping your systems, software and devices up to date will reduce the risk of being infected by a virus or hacked.

Compliance with a recognised standard, such as ISO/IEC 27001:2013, can help you implement some of the above steps. Obtaining ISO 27001 accreditation can be a complex process but it will demonstrate to your customers and service users that you take data security seriously. Alternatively, the government has introduced the 'Cyber Essentials' scheme to help organisations implement basic controls to address cyber threats and certification with this will likewise demonstrate to others that you have taken essential precautions against these threats (see https://www.gov.uk/government/publications/cyber-essentials-scheme-overview for more details).

It is important that in the event of someone attempting to extort money from you, or holding your data or systems to ransom that you do not pay any ransom demand without first seeking specialist advice. Paying even a small sum can result in you being more likely to be targeted again in the future.

Provision of insurance cover may be dependent on you adopting some, or all, of the measures outlined above. However, whether you take out specialist cover to protect yourself from the financial consequences of a cyber-attack or not, you should consider if any additional security measures are appropriate for your organisation.

Cyber summary of cover

This summary shows the main features and exclusions of the cyber cover we can offer – it does not provide all the terms, conditions and exclusions of the cyber section of cover or those of the policy wording. You can ask us for a copy of this. A significant exclusion is something that may affect your decision as to whether the cyber section of cover or the policy is suitable for you or is unusual compared to other policies that are available.

Our cyber cover is provided by Ecclesiastical Insurance Office plc.

Cover under our policies applies within the United Kingdom, the Channel Islands and the Isle of Man only unless we say otherwise.

See your policy wording for full details of cover, exclusions, and the general conditions and general exclusions.

Cyber

Cover	Significant exclusions and limits
Damages, costs and expenses agreed by us for the insured incidents as shown	£500 excess Section limit: £25,000 any one period of insurance For all insured events: Acts of terrorism Any loss of income during the time excess period Claims brought against you by a company in which you are a director, officer, partner or employee or have a financial interest Cost of correcting any failings in procedures, systems or security Cost of normal computer system maintenance Deliberate act or failure to act Fines or penalties other than what is covered by the Fines and Penalties extension Infringement of any patent Wear and tear Your insolvency or bankruptcy
Cyber – insured events	
Cyber liability – claims made in any one period of insurance for damages, costs and expenses as a result of: • failure to secure or prevent unauthorised use or access to data • unintentionally transmitting a computer virus • the content of your website, emails or anything else distributed by your computer system damaging the reputation of others or infringing intellectual property rights	

Cyber

Cover	Significant exclusions and limits
Data breach expense – if you failed to keep to your data privacy obligations, costs for: • hiring information-technology specialists to investigate the cause of the failure and advise you how to respond • informing customers and the data privacy regulator • credit file monitoring and identity theft assistance to customers or others who have been affected and provide a helpline to respond to queries where the failure relates to personal data (these services provided for up to 12 months) • public relations and crisis management expertise	
Computer system – cost of investigating and rectifying computer system damage and restoring data following loss or corruption of data, damage to websites, damage caused by viruses or hacking, including: • damage to a computer system of a provider under a contract to perform a service on your behalf • additional costs to prevent or reduce the disruption to your computer system • loss of income up to a 12 month period	Failure or interruption of any electrical power supply network or telecommunication network not owned and operated by you Value of the data to you
Cyber crime – financial loss: • following hacking that results in fraudulent input of, damage to or change of data in your computer system or to that of a provider under a contract to perform a service on your behalf leading to: - money being taken from your accounts or, - goods, services or property being transferred or, - credit being taken out in your name, • if you transfer money to a third party as a result of a fraudulent email Including costs: • of proving such transactions, contracts or agreements were entered into fraudulently • added to your telephone bill following hacking of your computer system • of specialist support to prove a threat is genuine • to help you respond to (including if we agree in writing, payment of a ransom demand) a threat of cyber extortion provided you can demonstrate that it is not a hoax and you have reported it to the Police	Any financial loss resulting from: • actual or alleged fraudulent use of credit or debit cards • a fraudulent application for credit or someone providing false details to apply for credit with you Any hacking by an employee

Cyber extensions

Specified extension limits form part of, and are not in addition to, the section limits unless we tell you otherwise.

Cover	Significant exclusions and limits
Costs we agree for removing viruses from your computer system whether they have caused damage to your computer system or not and hiring professional consultants to advise you how to prevent viruses or hacking	£15,000 any one period of insurance
Costs to carry out a security audit of your computer system following a valid cyber data breach claim	£15,000 any one period of insurance
Investigation costs for the repair, replacement or restoration of damage to your computer equipment following a valid cyber event claim	£15,000 any one period of insurance
Costs we agree to prevent or reduce actual or expected damage to computer systems or loss of income	£15,000 any one period of insurance Costs greater than the amount of damage and loss of income
Costs of temporary repairs, fast-tracking a permanent repair, replacement or restoration if we have accepted a claim for damage to your computer system	£15,000 any one period of insurance
Extra staffing costs and auditors or accountants fees incurred by you to verify any claim	£15,000 any one period of insurance
Following a claim against you, resulting from your failure to keep to your data privacy obligations, we will pay: • fines, penalties and • agreed damages you have to pay under a contract	£15,000 any one period of insurance Any fines or penalties which you cannot insure against by law

Special conditions for cyber

- These are aimed at reducing the risk of loss, damage or liability.
- We may refuse to pay part or all of your claim if you fail to keep to a special condition.
- See your policy wording for full details of the special conditions.

Special conditions	Summary of special conditions
Reporting a claim	What you must do in the event of a claim, or an incident that may give rise to a claim
Protecting data	You must have procedures in place for disposing of computers or files
Controlling defence	What we can do, and you must allow us to do, to defend a claim
Recoveries	What you must do, and we will do, if any money is recovered from a third party
Reasonable care	What you must do to maintain your equipment and protect data
Defence software	Protections you must have for your computer system
Data back-up	How often you must back-up and secure data
Right to survey	Allowing us to survey your premises
Data protection authority	You must be registered with the appropriate authority

Answers to some questions about the policy

How long does the policy provide cover for?

The policy normally runs for 12 months. About four weeks before it ends, we will send a renewal notice telling you our terms for the next 12 months.

What if you want to cancel the policy?

a) If you are an individual person and you want any part of the insurance for purposes which are outside your trade, business or profession, the following cooling-off conditions apply.

- If at the start of cover or when you renew the policy, you change your mind and no longer need the cover, you have 14 days (cooling-off period) from either the date you received the policy wording and the schedule or the date the cover began (whichever is later) to write to us, or your insurance advisor, to say you want to cancel the policy. In these circumstances we will make a full refund of your premium as long as you have not made a claim.
- You may cancel the policy after the cooling-off period but the following conditions then apply.

b) For all other insured people, companies or organisations and for an individual person cancelling outside the cooling-off period, the following conditions apply.

- We will refund the premium for the rest of the period of insurance, which we will adjust if you pay your premium by instalments. We will not give you a refund if it is less than £25.
- If you have made a claim in the current period of insurance, the full annual premium is due and we will not make a refund. If you pay the premium in instalments, you will have to pay any premium you owe for the rest of the period of insurance or we will take it from any claim payment due.

Can Ansvar cancel the policy?

We also have the right to cancel the policy by giving 14 days' notice sent by special delivery to your last-known address. If we cancel the policy, we will refund the premium for the rest of the period of insurance.

What is different about cover arranged on a 'claims made' basis?

Trustees' and directors' indemnity, fidelity guarantee (cover for your loss of money or property following the dishonest or fraudulent behaviour of an employee or volunteer), professional indemnity, libel and slander, misappropriation of money and cyber (cover for legal liability for loss of data or transmitting a virus and cybercrime) are all types of cover which insurers normally provide on a 'claims made' basis. This means we only provide cover for claims which are discovered and we are told about during a current period of insurance.

If you cancel the cover, you will no longer have protection for losses or actions before you cancelled. This can leave a possible gap in cover if you do not replace it with another insurance policy from the cancellation date. Ideally, before you cancel, you should get written agreement from anyone who will lose their protection of cover.

What if you need to make a claim?

You can find detailed guidance on making a claim in the policy wording and on our website.

Our 24-hour claims number is 0345 606 0431.

Our address is Ansvar Insurance, Ansvar House, 31 St Leonards Road, Eastbourne, East Sussex, BN21 3UR.

What governing law and language apply?

Our policies are governed by English law unless your legally registered address is in Scotland, in which case Scottish law will apply.

We will communicate with you in English at all times.

Complaints procedure

If you are unhappy with our products or service, please contact us as soon as possible.

You can complain in writing or by phone at any time to:

For all complaints

Ansvar Insurance

Ansvar House, 31 St Leonards Road, Eastbourne, East Sussex, BN21 3UR

Phone: **0345 60 20 999** or **01323 737541**

Email: **ansvar.complaints@ansvar.co.uk**

Our promise to you

We will aim to resolve your complaint within one business day.

To resolve your complaint we will:

- investigate your complaint thoroughly and impartially;
- keep you informed of the progress of the investigation; and
- respond in writing to your complaint as soon as possible.

For more complicated issues, we may need a little longer to investigate and we may ask you for more information to help us reach a decision.

If you are not satisfied with our response, or if we have not completed our investigation within eight weeks, we will tell you about your right to take the complaint to:

Financial Ombudsman Service

Exchange Tower, London, E14 9SR

Phone: **0800 023 4567**

Email: **complaint.info@financial-ombudsman.org.uk**

Website: **www.financial-ombudsman.org.uk**

This complaints procedure does not affect your right to take legal proceedings.

The Financial Services Compensation Scheme (FSCS)

The FSCS is an independent organisation set up by the Government. They give you your money back if an authorised financial-services provider cannot pay you because they do not have enough money.

The FSCS can only pay compensation for customers of financial-services firms authorised by the Prudential Regulation Authority or the Financial Conduct Authority.

The FSCS protects a range of products for both individuals and small businesses. Limits apply depending on the product you have bought.

The FSCS does not charge individual consumers for using their service.

The FSCS cannot help you if the firm you have done business with is still trading.

You can write to:

Financial Services Compensation Scheme

10th Floor, Beaufort House, 15 St Botolph Street, London, EC3A 7QU

Visit the website: **www.fscs.org.uk**

Phone FSCS helpline on **0207 741 4100** or **0800 678 1100**

Email: **enquiries@fscs.org.uk**

Useful links

https://www.actionfraud.police.uk/

(The National Fraud & Cyber Crime Reporting Centre. Cyber crimes committed or attempted against you can be reported here. Also contains useful information on how to protect your organisation against fraud, scam emails and the like)

https://www.ncsc.gov.uk/cyberessentials/overview

(overview of the government's 'cyber essentials' scheme)

https://www.ncsc.gov.uk/guidance

(Website for the National Cyber Security Centre, useful information on how to protect your organisation against common cyber threats)

Insurance advisor

Ansvar Insurance
Ansvar House, 31 St Leonards Road
Eastbourne, East Sussex BN21 3UR

Phone: **0345 60 20 999** or **01323 737541**
Email: **ansvar.insurance@ansvar.co.uk**
www.ansvar.co.uk

ansvar
Insuring the heart of your community