GUIDANCE

Cyber insurance guidance

Cyber security considerations for organisations thinking about taking out cyber insurance.

Introduction

This guidance is for organisations of all sizes who are considering purchasing cyber insurance.

It is **not** intended to be a comprehensive cyber insurance buyers guide, but instead focuses on the cyber security aspects of cyber insurance. If you are considering cyber insurance, these questions can be used to frame your discussions. This guidance focuses on standalone cyber insurance policies, but many of these questions may be relevant to cyber insurance where it is included in other policies.

> **Note:**
> In the first instance, it's worth checking if your organisation already has cyber insurance in place as part of existing policies, such as business interruption or property insurance. These may provide some level of coverage for cyber-related losses (or they may specifically exclude certain cyber-related incidents). Check your policy document, or speak to your insurance provider or broker for advice.

About cyber insurance

In a world where cyber threats are varied (and constantly changing), cyber insurance can help your organisation to get back on its feet, should something cyber-related go wrong. Managing cyber incidents (such as ransomware, data breaches) may require in-depth technical knowledge. As well as minimising business disruption and providing financial protection **during** an incident, cyber insurance may help with any legal and regulatory actions **after** an incident.

However, before considering any cyber insurance, you can help protect your organisation by ensuring you have fundamental cyber security safeguards in place, such as those certified by Cyber Essentials, or Cyber Essentials Plus.

> **Note:**
> Cyber insurance will **not** instantly solve all of your cyber security issues, and it will **not** prevent a cyber breach/attack. Just as homeowners with household insurance are expected to have adequate security measures in place, organisations must continue to put measures in place to protect what they care about.

What existing cyber security defences do you already have in place?

Purchasing an insurance policy might require providing information about your security controls. This may include technical, procedural, and human controls. Gathering this information may require the input of a number of people in your organisation, or from outsourced providers to your business (e.g. IT).

It is important for you to identify what within your organisation needs protecting the most (your 'crown jewels'), and to also identify any scenarios that must **not** happen. Do not limit yourself to meeting the minimum cyber security requirements specified by an insurer; these might not adequately protect the things your organisation cares about. To help you do this, the NCSC has provided further guidance on understanding and managing cyber risk.

Some insurers offer discounts if your organisation already has recognised cyber security defences in place (such as those certified by Cyber Essentials, or Cyber Essentials Plus) so ensure your broker is aware of these. As well as potentially lowering your premiums, completing schemes like these demonstrate to your customers, partners and suppliers that you take cyber security seriously, and for this reason should be considered even if you don't intend to take out cyber insurance.

Some organisations who achieve Cyber Essentials are provided with cyber liability insurance offered as part of this certification through the IASME Consortium. This won't be suitable for all organisations and the questions in this guide are still relevant to check that any cyber insurance offered meets your needs. If you have any questions about this type of cyber insurance, please refer to the information published by IASME.

How do you bring expertise together to assess a policy?

Cyber insurance policies often contain detailed technical information, which can include cyber security jargon. If you don't fully understand the policy, you may need

to identify people in your organisation who can help. This may include people who:

- deal with contracts (lawyers/commercial managers)
- manage and run your IT and security systems (technical experts)
- are responsible for the organisation's processes and procedures (such as human resources)

If you don't have direct access to technical expertise, you may want to use an NCSC-assured cyber security consultancy. For smaller organisations, your broker may be able to give advice and guidance on how to assess potential policies.

Do you fully understand the potential impacts of a cyber incident?

A cyber incident can impact a business in a variety of ways. For example, ransomware could mean your systems or devices are unavailable, or you may lose data (or your customers' data) due to virus or malware infection. It is important to build up a full understanding of how you're impacted, and the effects this will have on your organisation. This includes the financial impact of business interruption, and the associated costs of response and recovery. Of course, if you've done some sensible things (like ensuring the backup is kept separate from your network, or in a cloud service designed for this purpose), then ransomware attacks will have a smaller impact.

Unlike incidents such as a fire or theft, cyber incidents are often not restricted to a single location. Understanding how your organisation operates and the inter-dependencies between different parts is vital to determining the extent of an incident, which may have global implications.

What does the cyber insurance policy cover (or not cover)?

Before purchasing cover, it is important that you understand how important your organisation's data, systems and devices are to operations, so that an appropriate level of cover can be set.

Make sure you understand in detail what the policy covers, and equally important, what is excluded. For example, some insurance policies will not cover monies lost through business email compromise fraud. This is just one instance where a relatively common incident may not be covered by a standard cyber security policy. If business email compromise (for example) is an issue for you, you'll need to check that your policy covers this.

Remember, cyber attacks are evolving all of the time, and you might fall victim to a new type that may not have existed at the time the policy was taken out. You'll need to find out from your broker if you'd be covered if affected by a new type of cyber attack that's not consistent with your current policy.

Other questions it would be worth asking are:

- whether the cyber insurance policy you are looking at covers claims for compensation by third parties in the event of a cyber attack, or if personal data is lost as a result of a data breach at your organisation (for example, if a customer's personal data is lost)
- what the limits of the policy are, and whether they are appropriate for your organisation
- what services the insurer provides in the immediate response to an incident to help manage recovery and improve resilience; if the worst happens, you want to ensure that your organisation can learn from what went wrong and adapt to be stronger in the future.

What cyber security services are included in the policy, and do you need them?

Many insurers will offer cyber security consultancy services and risk management support once you have taken out their policy. This may include providing resiliency planning in addition to financial protection. Making use of these services and the expertise that come with them, especially if you don't have access to these skills in-house, may help reduce the chance and impact of a cyber incident or breach.

However, you need to consider how these meet your cyber security needs, and support your overall approach to cyber risk management.

Does the policy include support during (or after) a cyber security incident?

Some insurers will supply services that are useful during (or immediately after) a cyber security incident, such as IT forensic services, legal assistance or public relations support. They may put your organisation in touch with a Cyber Incident Response (CIR) organisation or their own in-house cyber incident response team. You may also find the NCSC's Incident Management guidance useful in thinking about how to plan, build, develop and maintain an effective cyber incident response capability.

Most cover responds to the immediate effects on the organisation by working to quickly restore network systems and data, while seeking to minimise losses from business interruption. For data breaches, there may be legal action from customers or other affected parties. The defence and settlement of such claims would normally be covered. Certain cyber insurance policies will go further and cover other cyber-related incidents such as computer-enabled fraud.

What must be in place to claim against (or renew) your cyber insurance policy?

Most cyber insurance policies are re-assessed every 12 months. The onus is on you to ensure that your organisation's cyber security details are accurate and up to date. It is important for insurers to understand what cyber security measures you have in place, and provide any other details they require. As with other insurance policies, you should also let your insurers know when your circumstances change so that you're still covered. If you're claiming that security measures are in place when they're not, the insurer may not be obliged to pay any claims.

Further reading: Cyber Security guidance from the NCSC

There's a selection of detailed cyber security advice and guidance available from the NCSC website.

Cyber Essentials

Helps you to guard against the most common cyber threats, and demonstrates your commitment to cyber security.

Small Business Guide

How to improve cyber security within your organisation - quickly, easily and at low cost.

Small Business Guide: Response and Recovery

How small to medium sized organisations can prepare their response to (and plan their recovery from) a cyber incident.

Board Toolkit

A selection of resources designed to encourage essential cyber security discussions between board members and their technical experts.

10 Steps to Cyber Security

Detailed guidance on how larger organisations can protect themselves in cyberspace.

Cyber Assessment Framework

The Cyber Assessment Framework (CAF) provides guidance for organisations responsible for vitally important services and activities. The organisations likely to find the CAF collection most useful fall into three broad categories, namely

- organisations within the UK Critical National Infrastructure (CNI)
- organisations subject to NIS Directive cyber regulation
- organisations managing cyber-related risks to public safety

Exercise in a Box

A free online tool which helps organisations find out how resilient they are to cyber attacks, and to practise their response in a safe environment.

NCSC's Incident Management guidance

Guidance on how to effectively detect, respond to and resolve cyber incidents

Cyber Incident Response (CIR) certified companies

Organisations who have networks of national significance can use Cyber Incident Response (CIR) certified companies to help them deal with targeted attacks.

Mitigating ransomware & malware attacks

How to defend organisations against malware or ransomware attacks

PUBLISHED

6 August 2020

REVIEWED

6 August 2020

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations