"90% of large and 74% of small businesses had a security breach over the previous year"
Hiscox

Guide: Cyber Insurance

Charities and Cyber Risks

Disclaimer

This guide does not provide a detailed analysis of your needs. It is intended purely as introductory information into the subject matter, and does not offer information on risk management, or advice (whether legal or financial) on insurance on which you can rely. You should always seek professional advice specific to your requirements.

What is cyber insurance?

Technology and data are fundamental to doing business today. With the digital landscape changing so quickly it can be difficult to know where the next risk is coming from. External threats and internal errors pose risks and if your data or network was compromised, your charity could quickly grind to a halt.

This could be an employee or volunteer losing or stealing your sensitive customer data, a virus in your network or even a hacker closing down your website. The press is increasingly highlighting examples of criminal or malicious attacks including those that effect charities.

Whilst there are elements of your existing insurances which may be applicable to some electronic exposures, standard charity policies are not designed to focus specifically on cyber risk and as such you should not rely on them to meet some of the risks now emerging.

Ultimately, there is no policy which offers absolute protection against all risks which are emerging as a result of digital progress.. But by considering the cover under a specialist Cyber Liability policy, you can perhaps draw some conclusions about what your charity is not covered for and consider whether your potential risks merit exploring the scope and cost of such policies.

Is your charity at high cyber risk?

Ultimately the management committee (and trustees) are responsible for identifying the extent to which your organisation is at risk. We can provide some food for thought when you are considering your exposure.

Your charity could be particularly vulnerable to a data breach or loss of vital services if you hold sensitive service user details such as names and addresses or banking information. You might also consider whether you hold sensitive health information or if the data you hold relates to vulnerable individuals too.

Another consideration would be whether you are particularly reliant on digital systems to conduct your activities. If your website is an essential part of your operation then this would heighten your organisational vulnerability.

If your charity takes card payments then you are subject to PCI compliance which gives you additional risk. According to the PCI Compliance Guide, compliance applies to all organisations that accept, transmit, or store any cardholder data. Using a third party payments company, may cut, but will not exempt your group from PCI compliance risks.

Does a sophisticated IT team or using a cloud for data help?

Many large corporations (such as Talk Talk with their infamous breach) have large sophisticated IT departments devoted to data security. Sometimes, a simple error such as failing to update software, or losing an unencrypted laptop, or even a malicious employee, can all lead to a breach.

If you store data with a cloud provider, you should carefully consider the legal contract you enter. Even if the risk of a data breach is reduced, the liability may still fall on your shoulders. You can outsource the service but not the responsibility.

What cover is provided?

Cyber products vary from provider to provider but a good policy will ensure that the following cover is in place.

Your charity will be financially protected from costs you incur in responding to a data breach. This would include IT forensic support and legal fees

If your charity activities are interrupted following a breach, then an element of financial protection will cover income you lose and additional costs you incur to get back trading.

A hacker may cause you costs as you have to restore or replace IT systems and programmes.

As astonishing as it seems cyber extortion is occurring in the UK (see the incredible claims examples below) and the ransoms incurred are covered under a good cyber policy. as are fees for professionals to handle negotiations on your behalf

A loss of data can lead to a media storm, a good cyber product not only covers the professional fees but will also provide experienced communications experts to help your organisation.

There are other costs that might be incurred by other parties that they seek to reclaim from your charity.

Individuals or groups (even employees or volunteers) might litigate against you for a breach of their privacy, a good cyber product will cover the costs of any legal awards and the legal defence costs.

If a data breach has occurred, you are likely to incur the attention of the regulator. The ICO has fined several charities in recent years and your cyber cover needs to cover defence costs and the settlement of fines (as long as the regulator does not make a condition of fine that it cannot be covered by insurance). Similar comments apply to charities who are processing payments and therefore subject to PCI compliance.

A good policy includes protection if your charity mistakenly infringe someone's copyright by using a picture online for

example, or inadvertently libel a third party in an email or other electronic communication.

A third party organisation might also sue if you unwittingly transmit to them a virus which causes them a loss. This will be covered under a good cyber product.

If your charity suffers theft (for example money) following a hack into your systems, this is not traditionally insured under a standard cyber policy wording. Some insurers allow you to extend cover to include such cover. Similar comments apply to the dishonesty of employees, trustees or volunteers.

Can I add cyber cover to an existing policy?

Cyber Insurance can be provided as part of a combined charity insurance product with some insurers, although many do not provide cover at all. Alternatively, cover can be organised as a stand alone product with some specialist insurers such as Markel and Hiscox.

The benefit of an insurer in your corner when the worst happens

Time, experience and confidence in the way forward is all of the essence when it comes to responding to a cyber incident.

By having specialist cyber cover, your charity will benefit from an expert response to a difficult situation. This might enable you to get on with the business of your charity more quickly.

Following a cyber breach, a good cyber product will provide the immediate legal support to support you. If the regulator is involved, specialist data lawyers will lead interactions with the Information Commissioner.

To support reducing cost and disruption to the charity, IT forensics might be deployed to understand quickly what has happened and how. This support will extent to remedying against any further damage.

If you work in a high volume organisation, a data breach can lead to increased phone traffic, for example, your service users contacting you to understand if their data has been effected. A good cyber policy will provide call centre support in this instance to help you manage the volume.

A PR team of experts will help you communicate to affected service users and suppliers, helping explain the steps you have taken to remedy your situation. If there is a risk of fraud to

your service users, this process will include a credit monitoring option to alert them to any unusual activity and provide more peace of mind.

Some real claims from Hiscox

Example Claims

One of our key insurer partners, Hiscox have dealt successfully with many cyber and data related claims.

From a client held to ransom by a Russian hacker, to a customer being tipped-off by 'white hat hackers' that their information was for sale on the dark web, here are some recent examples.

The technology business and malware claim:
Cost £250,000

Our client was advised that government security services had detected an intrusion on its systems. IT forensic experts were deployed to investigate and assess the extent to which the network had been compromised. A significant amount of malware was discovered on our client's servers so a containment plan was executed to remove all malware. Our client was also able to take legal and PR advice under their insurance cover to help them decide how and when to communicate this incident to their clients.

The optician held to ransom:
Cost: £60,000

An employee from a chain of opticians – received an email to say that she had been caught speeding and clicked the button. Shortly afterwards our client received an email from someone in Russia to say that they had infected their systems with the Cryptolocker virus and that all files on its servers were encrypted. The encrypted files included patient records and software used to run the business.

The Russians asked for £400 in Bitcoins for a decryption key. We approved the payment of the ransom. Unfortunately this only recovered 90% of the files and an IT contractor helped them recover the remainder. Their insurance policy covered this business interruption as well as the costs of being unable to trade for a couple of days and not being fully up-to-speed for a couple of weeks.

The publisher's lost passwords:
Cost £10,000

Contacted by a 'white hat hacker', our client was told that user names and passwords for two of their websites had been stolen. We called in IT forensic experts to investigate, who confirmed there had been a hack and set about plugging the security breach. Legal advice was also taken to confirm whether or not our client was required to notify the individuals whose user names had been compromised.