Cyber insurance: protect your organisation in the digital age

The worldwide web and smart technologies have created an incredibly well-connected society in which we can do almost anything at the touch of a button. But our dependence on digital devices at home and at work expose us all to the potentially devastating costs of system failures, data losses, and cyberattacks.

At Unity, we understand the risks our customers face, and know that the right cyber insurance – along with some good security practices – can help protect your organisation online. This information sheet highlights some of the major risks and what you can do to reduce them.

Are you at risk?

News headlines would suggest that cybercrime only affects big businesses and banks, but charities, not-for-profit organisations and small businesses are far from immune. In fact:

- Cybercrime on small and medium-sized enterprises (SMEs) is increasing.
- SMEs and charities are seen as easier targets as they often have fewer security measures.

Your charity or Scout group is at risk if it:

- uses IT systems and the internet;
- holds sensitive information electronically;
- has a website;
- uses social media; or
- accepts payments online or by card.

What are the risks?

The three main types of cyber risks are:

1. Direct, malicious cyber-attacks
2. Accidental information loss or misuse
3. Physical system failures

Cybercrime is evolving as quickly as the technology itself and hackers are using increasingly sophisticated methods. Many people and organisations may be unaware of an attack until it is too late. Cyber criminals can, for example:

- encrypt your data so you cannot access it.
- steal sensitive data and threaten to publish it unless you pay a ransom.
- access your electronic banking and steal money directly.

Besides malicious attacks, IT systems do sometimes fail by themselves and vital information can be lost, leaked or accidentally deleted by human error.

How big are the risks?

In the first half of 2021, individuals and organisations in the UK reported losing £1.3 billion to fraud and cybercrime. Cyberattacks and system outages can disrupt your activities, which could temporarily reduce your charity's income, but if personal data is lost you could face huge fines (up to £17.5 million or 4% of your annual turnover) under UK data protection laws.

Besides the direct financial losses from theft and fines, the hidden costs of cybercrime and system failures can also quickly mount up. These include:

- Legal fees
- Forensic investigations
- Ransom payments
- Software and website repairs
- Reputational damage

What can you do about it?

Manage the risks:

Besides the obvious firewalls, encryption, anti-virus software and data backups, everyone within your organisation, whether it's a nationwide charity or local Scout group, plays an important part in reducing your cyber risks. It is now more vital than ever to train your staff and volunteers in cyber security and good online practice.

As a basic measure you should:

- Encrypt all portable devices
- Use multi-factor authentication for accessing your network, banking or social media accounts remotely
- Regularly change your passwords
- Use long, random passwords with a mix of letters, numbers, and symbols
- Check the security of your cloud computing and service providers
- Never access confidential information or make card payments on public Wi-Fi
- Regularly back up your documents and data offline
- Keep your software updated
- Include threats of data breaches and service disruption in your Business Continuity Plan

Malicious attacks are the hardest to defend yourself against, but there are some common traps that everyone can learn to recognise and avoid:

- **Phishing emails** – messages disguised as being from recognised companies such as Amazon and PayPal, but are trying to get your passwords or bank details.
- **Spam emails** – messages containing links to fake online shops or competition websites that, once clicked, install malware (viruses, spyware) onto your computer.

If an email looks suspicious, has spelling errors, or has been sent from a strange address, do not click on any links. Report it as spam and delete it immediately. Fortunately, most reputable email providers automatically scan for malicious attachments and links and send them straight into spam.

Buy cyber insurance:

Not all cyber risks can be predicted or prevented, but an effective insurance policy can help you respond and recover from an unavoidable incident. Products like Cyber Liability Insurance and Data Protection Insurance can safeguard your organisation against cybercrime, data losses, and system failures. Most importantly, it enables experts to bring the crisis under control, allowing you to continue your good work.

What does cyber insurance cover?

A comprehensive cyber insurance policy can cover the cost of system failures and security breaches, whether malicious or accidental, as well as providing practical support to guide you through a difficult situation.

Here is a thorough, but not exhaustive, list of things that cyber insurance can provide cover for:

Data breaches: If confidential data is lost, stolen or compromised; the cost of notifying customers, legal advice on data compliance, forensic investigations into how the breach occurred, cleaning up your computer systems, and restoring lost data.

Cyber extortion: If a hacker steals data or locks down the computer system and demands money to restore it; the ransom and the costs of bringing in a risk consultancy firm to manage the situation.

Repair costs: This covers the restoration of programmes and data that were damaged or lost during a security breach or virus attack.

Business interruption: This covers loss of income resulting from a cyberattack or network failure.

Cyber liability: This covers legal costs for if someone was to sue you for a data breach (privacy liability) or for publishing libellous, plagiarised, copyrighted or slanderous content on your website and social channels (multimedia liability).

Payment card industry (PCI) penalties: This covers the potential fines and penalties for if your organisation failed to follow PCI data security standards.

Please note that not all cyber insurance policies are the same and very few cover the full range of cyber threats, so we recommend you take time to ensure you are correctly covered.

We're here to help

As a specialist insurance broker that understands the technology and data risks faced by charities, voluntary organisations and businesses, we can arrange the right cyber liability cover for you.

Call us to chat through your needs on:

0345 040 7702

unityins.co.uk