access INSURANCE

incorporating clients of

Ladbrook insurance

Understanding cyber insurance for NAVCA members

A short guide to common cyber risks, charity vulnerabilities, the associated recovery costs and what cyber insurance covers.

30% of charities said they identified a cyber attack in the last 12 months (Cyber Security Breaches Survey 2025). Cyber threats and crimes are becoming more common and more sophisticated as criminals use ever-evolving tactics to exploit charities (as well as other organisations).

1 THE COMMON CYBER THREATS

Not-for-profits hold sensitive information such as volunteer records, donor data, financials, and beneficiaries' personal information. This, combined with less frequently reviewed cyber security, makes them attractive targets for cyber-criminals. The following are some of the most common cyber threats for charities:

- **Phishing** is a form of social engineering where cybercriminals attempt to steal sensitive information by posing as a trustworthy entity in emails, texts, social media messages, or calls.
- **Ransomware** is malware that encrypts files on a computer system and demands payment for the decryption key. It can cause significant disruption and financial losses for individuals and organisations.
- **Viruses** are malware that can replicate themselves and spread to other computers. They could cause damage to computer systems, corrupt files, and steal personal information.
- **Data breaches** occur when an unauthorised party accesses personal or sensitive data. They could result in identity theft, financial fraud, fines, extortion and reputational damage.
- **Identity theft/impersonation** is the unauthorised use of someone's personal information and is often combined with phishing attacks.
- **Website hacking/takedowns** refer to making a website unavailable to its intended users, often through distributed denial-of-service (DDoS) attacks. Hackers could also edit some code or redirect the site to harmful sites and make your web visitors targets of cybercrime.
- **Online financial fraud** can occur through phishing attacks, extortion in ransom demands or stealing donor payment information.

2 VULNERABILITIES TO LOOK OUT FOR

Staff and volunteers

Phishing is a significant risk for charities as volunteers may not have the necessary training or systems to identify these fraudulent emails. Phishing emails have become more sophisticated with AI, and even with robust security measures in place, an external email with a malicious link or attachment can lead to cybercrime such as malware or tricking individuals into divulging sensitive information.

Access issues

Although outsourcing IT maintenance or setup to experts can be beneficial, it can also create vulnerabilities. For example, if the IT vendor is attacked or infiltrated, they could potentially compromise all of their clients through remote connections. Data shows that only 5% of charities review potential cyber security risks their suppliers pose. Therefore, it is vital to ensure IT vendors have implemented appropriate cybersecurity measures to mitigate this risk. These include strong access controls, regularly reviewing their security protocols, and prioritising employee cybersecurity awareness training.

Weak passwords pose another vulnerability. Attackers can use various methods to guess passwords, including brute-force attacks or social engineering techniques. To avoid this, don't use easily guessable, simple or reused passwords and implement two-factor authentication.

Insider threats from the mishandling of personal data also present a vulnerability. Even leaving hard copies of sensitive information lying around on public display is a potential cyber risk, so it is important to have strong policies for accessing and storing personal data.

Whilst backups enable you to restore lost data, if they are connected to the same network then they are vulnerable to the same attacks. Therefore, creating an offline backup (not connected to the main system) is vital to mitigate this vulnerability.

3 THE SCALE OF DAMAGE AND RECOVERY

If criminals manage to exploit any of these vulnerabilities, the damage could be severe and can include the following:

Financial losses

- Ransom payments.
- Forensic and computer expert costs.
- Data recovery and clean-up costs.
- Legal fees, such as e-discovery and notification costs (including credit monitoring and identity protection services).

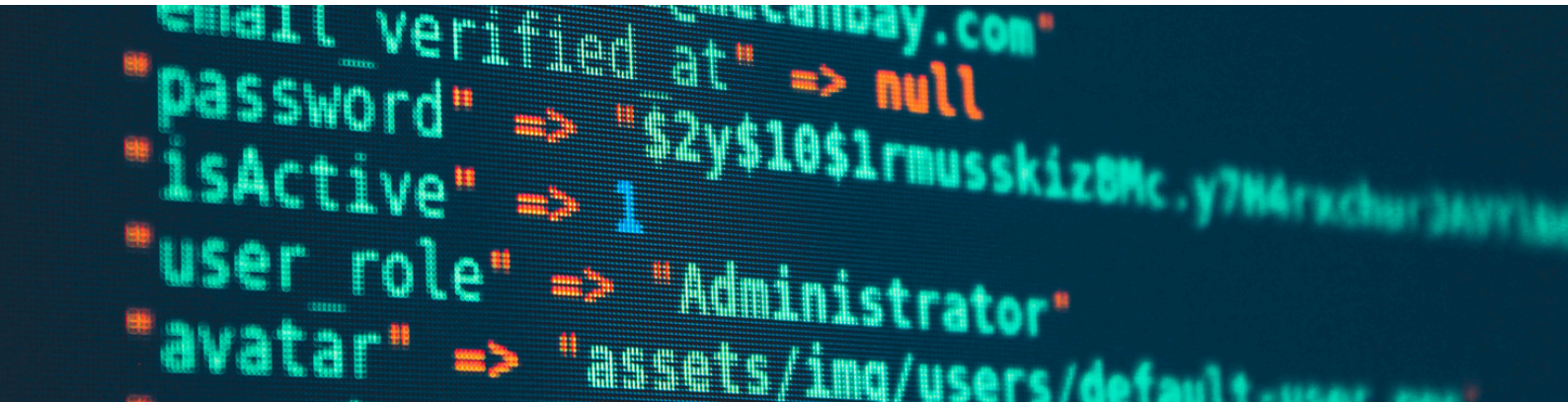
Reputational damage

- Damage caused by unauthorised access and use of personal, sensitive and payment information.
- The loss of website control.
- Negative PR and communications.

Disruption

- Recovery takes not only money but time. Criminals may have compromised your systems or data in multiple ways to extort you again. This is why a forensic investigator must perform a thorough check of your system.
- Your normal operations may be disrupted through the downtime of systems and while you get back up and running.

For these reasons, the costs associated with cyber incident recovery can be substantial, on average for charities it can be £8,690, but can exceed £350k in the most disruptive cases for a larger charity.



4 CYBER INSURANCE

Cyber insurance policies typically cover the expenses associated with recovery efforts, including consulting, legal, and advisory services. Such services can be invaluable, especially when it comes to making critical decisions regarding the handling of ransomware payments. They can offer expert advice and guidance on whether or not to negotiate with cybercriminals, taking into consideration the specific circumstances and potential risks.

Policy wordings change regularly due to the evolving and emerging nature of cyber risks, but insurers typically offer cover for the following:

- **Privacy Breach Response**: This covers the costs associated with a data breach, including notification and credit monitoring for affected individuals as well as forensic investigations and services.
- **Business Interruption**: This covers the losses incurred as a result of a cyber attack that disrupts your operations.
- **Cyber Extortion**: This covers the costs associated with responding to a ransomware attack.
- **Liability**: This covers the costs associated with legal action taken against your organisation due to a data breach. ICO issues penalties and fines for data protection failures.
- **Crisis Management**: This covers the costs associated with managing the fallout from a cyber attack, including public relations and crisis management.

5 IMPLEMENTING GOOD RISK MANAGEMENT

Implementing robust cyber risk management before considering cyber cover is essential. Insurers will often impose specific conditions that must be met before purchasing cyber insurance.

We recommend that you at least take advantage of the Cyber Essentials training for charities, designed by the National Cyber Security Centre.

Some of the standards that insurers will often impose before offering cyber cover:

- **Enabling multi-factor authentication** for cloud-based services (e.g. email providers).
- **Only using a Virtual Private Network (VPN)** to access your environment.
- **Taking offline backups** that will be unaffected by issues with the live environment.
- **Regular training** on awareness of cyber threats and preventative measures for staff and volunteers (see Cyber Essentials).

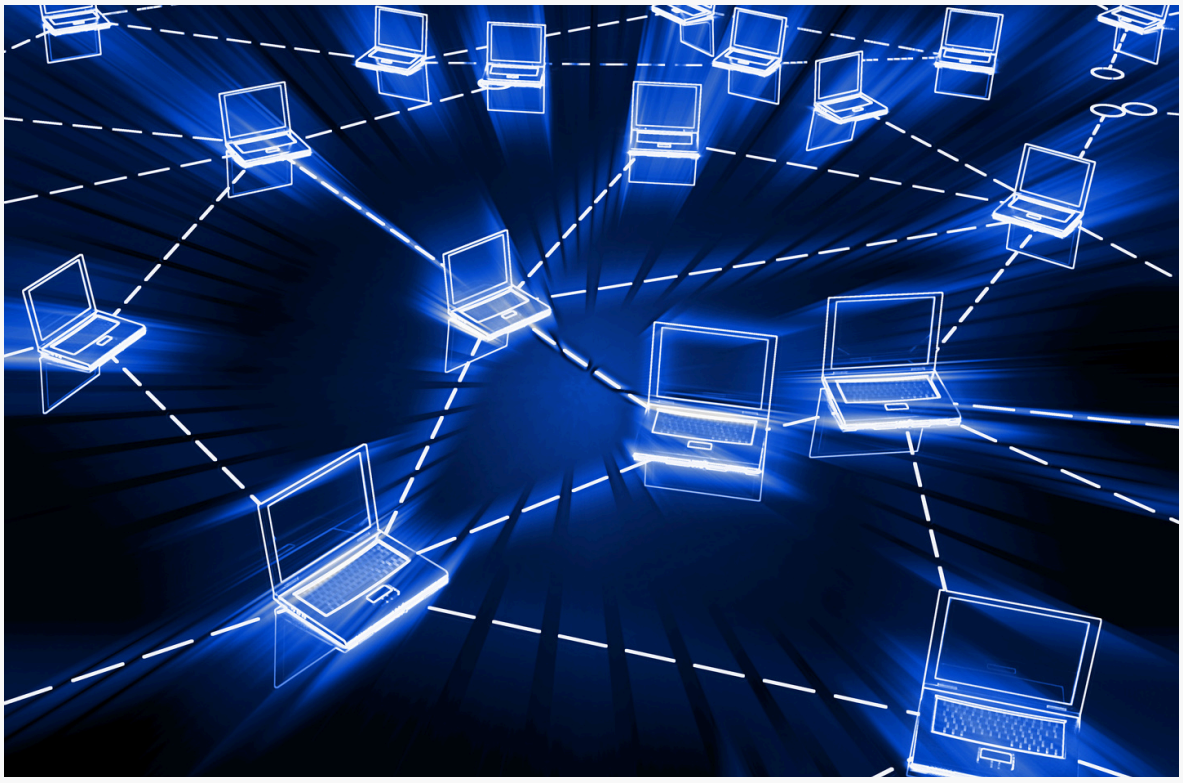
HOW ACCESS INSURANCE CAN HELP YOU?

Our service is often described as bespoke, as we build insurance policies based on your unique risks. Here's why charities choose to work with us:

You only pay for the cover you need
As an independent Chartered broker, we recommend the most suitable cover for your risks to protect you properly. We work in your interests rather than insurers. We compare multiple insurers on your behalf, and you can be confident that we provide you with a competitive quote.

We're charity specialists, owned by a charity
Charity is at the heart of what we do, from our vision, our specialist advice to our internal culture. Over 18,000 charities, community groups and social enterprises trust us to advise on and arrange their insurance each year. We're also proud to be part of the Benefact Group, a family of financial service businesses that gives all available profits to charity, and is ultimately owned by a charity, the Benefact Trust. Over £1m is given annually through the Group's giving programme, Movement for Good, which anyone can get involved in.

Understanding cyber insurance for NAVCA members



If you have questions about anything in this guide, or would value advice on improving your risk management and insurance programme, please contact one of our specialist advisers at **charity@accessinsurance.co.uk** / **020 8651 7420**.