WRS insurance brokers

Cyber Insurance and Fraud Protection for Charities

Proudly part of the BENEFACT GROUP

As more charities operate in a digital world, they face growing risks from **cybercrime** and **fraud**. From **phishing scams** to **financial mismanagement**, these threats can compromise sensitive data, disrupt operations, and damage reputations.

This guide, from our Charity Cyber Insurance specialists, outlines **practical steps** that charities, social enterprises and Community Interest Companies can take to **protect themselves** through insurance and fraud prevention strategies.

Contents

About WRS Insurance Brokers 3
Understanding cyber risks for charities 4
Can you afford a breach? 5
Strengthening cyber security 6
Why Cyber Insurance matters for charities 7
Fraud Prevention for Charities 8
Steps for charities to take if a cyber attack is suspected 9
Steps for charities to take if fraud is suspected 10

About WRS Insurance Brokers

WRS is part of the Benefact Group, a charity-owned, international family of financial services companies that gives all available profits to charity and good causes.

With over 50 years of experience, WRS Insurance Brokers specialise in providing tailored insurance solutions for the third sector, including **Cyber Insurance.**

Why Choose WRS?

- Expertise in charity insurance and an understanding of sector-specific challenges
- Comprehensive policies covering cyber risks, fraud, and reputational damage
- Access to cybersecurity experts, legal advisors, and recovery teams

Protect Your Charity Today Contact WRS Insurance Brokers for expert advice and comprehensive cover to secure your charity's digital future.

Get a quote

Our products, policies and advice

help protect and grow what matters most to our clients

and because we give all available profits to charity

they make the lives of others a little brighter too.

BENEFACT GROUP

WRS Insurance Brokers are proudly part of the Benefact Group, which is owned by one of the UK's leading grant-making charities the Benefact Trust. Benefact Group are a diverse family of specialist financial services businesses, driven by our shared ambition to do right by our customers and united by a common purpose to give all available profits to charity and good causes.

We have donated over £200 million since 2014. Giving our profits to good causes means we are motivated by something far greater than the need to satisfy shareholders' returns, allowing a focus on the highest levels of customer service and satisfaction.

01206 760 780
hello@wrsinsurance.co.uk

Understanding cyber risks for charities

What is a cyber attack?

Simply using email or maintaining a website puts your organisation at risk. A cyber attack is any attempt to gain unauthorised access to an organisation's systems or data, disrupt operations, or steal sensitive information. Common types of cyber-attacks include:

Phishing scams

Phishing is the most common type of cyber attack. Fraudulent emails can be sent tricking users into sharing personal information

Example: A type of online fraud where attackers impersonate a legitimate organisation or a Trustee to trick victims into sharing sensitive information like passwords, bank details, or personal data.

Ransomware

Malicious software encrypts (locks) data until a ransom is paid

Example: A hacker encrypts your charity's files and asks for money to provide the decryption key.

Malware

Malicious software designed to damage, disrupt, or gain unauthorised access to systems. Includes viruses, worms, Trojans, and spyware.

Example: Downloading a file that infects your computer and steals login credentials.

Click here to read the Government's definition on the most common types of cyber attacks

The National Cyber Security Centre defines cyber security as **helping individuals and organisations reduce the risk of cyber-attack** by "protecting the devices we all use and the services we access from theft or damage" and "...preventing unauthorised access to the vast amounts of personal information we store online."

32% of charities experienced cyber breaches in 2024, *rising to* **66%** for high-income charities.

83% were impacted by phishing attacks.

30% of charities have board-level cybersecurity responsibility, *rising to* **47%** in high-income charities.

37% were impacted by impersonation scams.

Source: Gov Cyber breaches survey 2024

Can you afford a breach?

The real costs of cyber attacks

When it comes to the cost of cyber attacks, the question isn't just whether your charity can recover—but whether it can afford the financial and reputational costs of a breach in the first place. These may include:

Financial losses

Cyberattacks often come with significant financial repercussions.

- ***Restoration Costs:*** Paying for IT specialists to recover lost data or rebuild systems.
- ***Ransom Payments:*** In cases of ransomware, organisations may feel pressured to pay to regain access.
- ***Legal Fees:*** Addressing legal claims or meeting regulatory obligations.

Operational disruption

Cyberattacks can bring operations to a standstill, particularly for charities that rely on digital platforms to deliver services.

- Critical services may go offline, delaying aid and support to those who depend on them
- Systems downtime could prevent access to donor platforms, halting fundraising efforts

Reputational damage

A data breach or attack can erode trust among donors, beneficiaries, and stakeholders.

- Donors may hesitate to contribute if they believe their information isn't safe.
- Long-standing partnerships with other organisations may suffer, leading to reduced collaboration opportunities.

Regulatory penalties

Non-compliance with data protection laws, such as GDPR, can result in:

- Substantial fines imposed by regulatory bodies
- Mandatory reporting requirements, which could expose vulnerabilities publicly

Strengthening cyber security

A Charity Cyber Insurance policy will help protect your charity from the moment a breach is identified.

Click here to find out more about Charity Cyber Insurance from WRS.

Create strong cybersecurity policies

Password management: Use strong, unique passwords for all accounts and systems, and enforce regular updates. Encourage the use of multi-factor authentication (MFA).

Click here to find out more about multi-factor authentication

Restrict administrative privileges: Limit access to sensitive systems and data to only those who need it.

Train staff and volunteers to recognise and report cybersecurity threats

Recognise phishing: Teach staff how to spot fraudulent emails and websites attempting to steal information

Follow Safe Data Practices: Provide guidance on safely handling sensitive data

Frequently back up data and test recovery plans

Prevent data loss: Back up critical data regularly to avoid losing it to cyber-attacks like ransomware

Cloud and offline backups: Use a combination of cloud storage and external drives to back up data automatically

Test your backups: Periodically check that backups can be restored in emergencies

Secure online donations and payment systems

SSL Encryption: Ensure your website has SSL encryption (look for "https://" in the URL) to protect donor data.

Trusted Payment Processors: Use reputable third-party payment processors for online donations.

Develop an incident response plan

Incident response team: Assign roles for handling breaches, including waho to notify and what steps to take

Adopt international standards for information security

ISO 27001 Certification: This certification provides a framework for improving your charity's **Information Security Management System (ISMS)** and helps prevent cyber incidents

Regularly update software

Install security updates: Cybercriminals often exploit vulnerabilities in outdated software. Regularly install updates to protect against risks

Stay updated

Subscribe to email alerts from organisations like the **National Cyber Security Centre (NCSC)** or use a threat intelligence platform to receive updates about current cyber risks that may affect your charity

Perform regular security audits

Review systems: Conduct comprehensive audits of your charity's digital systems and procedures to evaluate security effectiveness

Why Cyber Insurance matters for charities

Charities often handle sensitive data such as donor records, financial information, and beneficiary details. Charity Cyber Insurance protects by providing the following cover:

Data breach response

Supports investigation, containment, and notifying affected individuals to manage breaches effectively.

Business interruption

Provides compensation for income loss caused by cyber incidents disrupting operations.

Legal & regulatory support

Covers legal expenses and potential fines related to data protection breaches.

Cyber extortion & ransomware

Addresses costs for ransom payments and system restoration after ransomware attacks.

Crisis management

Includes public relations support and reputation management services to restore trust.

Things to consider when choosing a policy for your charity:

1. Assess risks
Identify potential threats, such as phishing or ransomware

2. Check your cover
Ensure the policy covers data recovery, legal costs, and business interruptions

3. Review exclusions
Be aware of exclusions, such as cover for outdated software vulnerabilities

A Cyber Insurance policy will help protect your charity from the moment a breach is identified. With over 50 years' experience in the Charity Insurance sector, we can help you find the best policy for your charity's needs.

Click here to find out more about Charity Cyber Insurance

Fraud Prevention for Charities

Fraud can come from both internal and external sources. Internally, this may involve employees or volunteers; externally, it could include false funding requests or scams targeting the charity.

Fraud can devastate charities by:

Draining financial resources

Damaging reputations

Undermining trust among stakeholders

Fraud can manifest in various ways, including:

Banking Fraud

Unauthorised access to or misuse of charity accounts

Fundraising Fraud

Misappropriation or false representation of donations

Identity Fraud

Misuse of the charity's name or reputation.

Tax & Gift Aid Fraud

Incorrect claims or misuse of tax benefits

Property & Investment Fraud

Mismanagement or theft of assets

Fraud Prevention Tips

The following tips have been compiled from best practices in fraud prevention and guidance from industry experts, Small Charities Finance.

1.

Implement robust financial controls

Segregate duties: Ensure different people manage authorising, processing, and reconciling financial transactions.

Monitor transactions: Regularly review bank statements for unusual activity

Clear authorisation processes: Set guidelines on who can approve payments and access financial records.

2.

Encourage whistle-blowing & transparency

Whistle-blowing policy: Develop a policy to protect individuals who report fraud

Transparency: Ensure financial information and audits are accessible and reviewed regularly by trustees and senior staff.

3.

Conduct regular audits

Internal and external audits: Regularly carry out audits to ensure accurate financial records.

Review procurement: Check that all purchases are legitimate and properly recorded.

4.

Protect sensitive data

Data encryption: Encrypt sensitive data both in transit and at rest.

Access controls: Limit access to sensitive data to those who need it.

5.

Secure cash handling and fundraising processes

Cash handling: Assign different individuals to handle donations, count money, and bank the funds.

Event controls: Ensure clear guidelines for handling funds raised at events and document all transactions.

6.

Establish Strong Governance

Trustee oversight: Trustees should regularly review financial statements and audits to ensure proper controls are in place.

Clear roles and responsibilities: Ensure staff and trustees understand their duties regarding fraud prevention.

Regular staff training: Ensure staff are aware of fraud risks and trained to spot potential fraud.

Find out more about Small Charities Finance **here**

Steps for charities to take if a cyber attack is suspected

A suspected cyber attack is identified.

Step 1.

Identify indicators

Look for unusual activity, such as unauthorised logins, unexpected system behaviour, or missing data

Step 2.

Isolate affected systems

Disconnect compromised systems and devices from the network to prevent further spread

Step 3.

Notify leadership

Inform key personnel, including board members, IT staff, and leadership teams

Step 4.

Preserve evidence

Avoid shutting down systems; instead, place affected devices in hibernation mode

Secure logs and other records for forensic analysis

Step 5.

Engage cyber insurance

Contact your cyber insurance provider for guidance on investigation and recovery

Step 6.

Report the incident

Notify relevant authorities, such as Action Fraud, and the Information Commissioner's Office (ICO) if personal data is involved

Step 7.

Investigate internally

Work with IT or cybersecurity experts to assess the scope and impact of the breach

Identify compromised data or systems

Step 8.

Mitigate the threat

Apply fixes, such as patching vulnerabilities and resetting passwords.

Update and secure software and systems.

Step 9.

Restore operations

Use backups to recover lost data or restore affected systems

Test systems to ensure the threat has been neutralised

Step 10.

Communicate transparently

Notify stakeholders, including donors, beneficiaries, and partners, if they may be affected

Step 11.

Review and strengthen security

Conduct a post-attack audit to understand what went wrong.

Update cybersecurity policies, improve staff training, and enhance security measures.

The attack is resolved, and preventative measures are in place to reduce future risks.

Steps for charities to take if fraud is suspected

A potential fraud incident is identified.

Step 1.

Recognise red flags

Look for unusual transactions, missing funds, altered documents, or discrepancies in financial records

Step 2.

Preserve evidence

Secure all records, logs, and data related to the suspected fraud

Avoid making changes to financial or digital records that could compromise the evidence

Step 3.

Notify leadership

Inform key personnel, including trustees, board members, or senior management

Ensure that only necessary individuals are informed to maintain confidentiality

Step 4.

Report the fraud

Internal Reporting:
Follow your charity's internal fraud policy or reporting procedures

External Reporting:
Notify relevant authorities, such as:

Action Fraud:
For suspected criminal activity

Charity Commission:
If the fraud impacts the charity's ability to operate or breaches regulatory requirements

Step 5.

Engage insurance

Contact your fraud insurance provider to initiate the claims process and seek guidance on next steps

Step 6.

Conduct an internal review

Assemble a response team to investigate the scope and impact of the fraud

Identify vulnerabilities that allowed the fraud to occur

Step 7.

Mitigate the impact

Take immediate steps to minimise further losses, such as freezing accounts or revoking access to affected systems.

Step 8.

Communicate transparently

Inform stakeholders, including donors, staff, and beneficiaries, if they may be affected

Be transparent while protecting sensitive details and preserving trust

Step 9.

Education

Implement measures to prevent future fraud, such as:

Enhancing financial controls.

Conducting fraud awareness training for staff and volunteers.

Establishing or updating whistleblowing procedures.

Step 10.

Monitor and review

Conduct regular audits and risk assessments to identify and address vulnerabilities

Update policies and procedures based on lessons learned

Fraud is addressed, and preventative measures are in place to reduce future risks.

Useful links:

NCSC - Cyber Aware Programme

NCSC - Small Charity Guide

Charity Digital

Protect your charity from cyber crime

"I have always found everyone at WRS Insurance **extremely helpful** and I am delighted with the service they provide. They are **very knowledgeable** about the third sector generally and took the time to come and **understand our business** to make sure we got the policy which best suited our particular, diverse needs.

They are very good at getting claims **resolved quickly** and are **all-round nice people** to deal with – very **friendly** and very **enthusiastic**. WRS always seem to be looking out for **our best interests.**"

Richard Beard
Chief Executive, The Jericho Foundation

Jericho

WRS insurance brokers

Contact us:

01206 760780
hello@wrsinsurance.co.uk

Cadman House, Maurice Way,
Stanway, Colchester, Essex, CO3 0BA
www.wrsinsurance.co.uk

Proudly part of the BENEFACT GROUP

WRS Insurance Brokers is a trading name of SEIB Insurance Brokers Ltd who are authorised and regulated by the Financial Conduct Authority. Registration number: 479477.