Cyber risk and resilience: what recent incidents mean for charities

IS CYBER RESILIENCE ON YOUR AGENDA?

Recent incidents involving a popular fundraising CRM and a charity bank have provided the charity sector with two very different reminders of how organisations are dependent on technology and external providers.

One involved the potential loss of information. The other involved the loss of access to an essential service.

Together they demonstrate an important point: **a charity does not have to directly be the victim of a cyber incident to experience the consequences of interruption via third party providers.**

For many small and medium sized charities, cyber risk can still feel unfamiliar or difficult to understand. If your organisation has never experienced a serious cyber incident, it can be easy to assume that the greatest risks sit somewhere else; perhaps with larger charities, financial institutions or organisations holding huge quantities of sensitive information. Recent events might have challenged you to reconsider that assumption.

A charity may be affected through the bank it uses, the CRM holding its supporter information, its payroll provider, fundraising platforms, cloud services or other technology on which its everyday work depends.

That is why cyber resilience deserves to sit firmly on the agenda for trustees and senior leaders, including within smaller organisations.

TWO INCIDENTS, TWO DIFFERENT RISKS

FUNDRAISING CRM BREACH: WHEN INFORMATION HELD BY A SUPPLIER IS COMPROMISED

In August 2026 the Charity Commission issued specific guidance following a cyber security incident affecting a popular fundraising CRM and the charities using its CRM service to manage information about donors, supporters, volunteers and other contacts. The Commission advised affected organisations to consider the potential impact on their charity, their obligations to the Information Commissioner's Office and whether the circumstances required a serious incident report to the Charity Commission.

The incident highlights one of the realities of modern charity operations - significant amounts of organisational and personal information are often held in third-party systems.

Outsourcing is necessary and frequently provides better technology and security than an organisation could build for itself. It does not, however, remove the charity's responsibility to understand what information is being shared, how important that information is, and what would happen if it were compromised.

The lesson is not that charities should avoid using external technology providers. It is that **outsourcing a system does not outsource the risk associated with relying upon it.**

BANKING OUTAGE: WHEN AN ESSENTIAL SERVICE BECOMES UNAVAILABLE

The difficulties experienced recently by a charity bank's customers provides a different example.

The bank experienced issues affecting access to online banking. For organisations reliant on online banking for everyday finance administration, disruption to an important service can quickly become an operational problem. The bank itself identifies online banking incidents as potentially major operational or security events where customers are prevented from using payment services.

The important lesson here for charities is slightly different from the fundraising CRM example.

An organisation's own systems may be working correctly. Its information may not have been compromised. Yet if an important external service suddenly becomes unavailable, the charity may still struggle to carry out essential activities.

That could include paying staff or suppliers, accessing financial information or performing other activities.

The question therefore becomes:

What would happen to our organisation if a critical supplier or Digital service was unavailable tomorrow?

This is particularly important for smaller charities.

Large organisations may have dedicated IT teams, information security specialists or risk professionals. Smaller and medium-sized charities are more likely to rely on a combination of staff, trustees and external providers.

Cyber terminology itself can also be a barrier. Discussions about ransomware, APIs, encryption, access keys, malware or vulnerabilities can become technical.

Trustees don't need to become cyber security experts.

They do, however, need to understand the potential consequences for their organisation and be capable of asking sensible questions about controls and contingency arrangements.

For an organisation that has never experienced a serious cyber incident, it may be tempting to conclude that existing arrangements must be working well, which isn't necessarily the case. It may simply not have had an incident that exposes a vulnerability yet.

These examples provide a useful opportunity for boards to discuss these risks so they can be prepared if an incident does occur.

THE RISK ENVIRONMENT IS CHANGING

The Charity Commission's 2026 Charity Sector Risk Assessment reinforces the importance of that discussion.

The Commission reports that 30% of charities experienced a cyber attack during the previous year. Phishing remains the most common and disruptive type of attack with ransomware also increasing. The assessment warns that the misuse of AI could create additional risks for charity beneficiaries and employees.

Cyber risk also sits within a much wider picture.

The Commission reports increasingly sophisticated attempts to exploit charities for private benefit and other improper purposes. Cases involving suspected private benefit increased by 29% during 2025/26 following an increase of 38% the previous year.

AI may further change that environment by making some forms of fraud, impersonation and deception easier to produce and potentially more convincing.

At the same time many charities continue to operate under significant financial pressure.

An organisation with limited staff, tight finances and little specialist expertise may have less capacity to absorb a prolonged interruption, investigate a breach or respond quickly to the effects of an incident.

Cyber should therefore be considered as part of the charity's wider approach to **governance, financial resilience and business continuity**, rather than as a standalone technology issue.

DEPENDENCY ON THIRD-PARTY SUPPLIERS SHOULD BE PART OF A CHARITY'S RISK MANAGEMENT

Charities increasingly rely on external organisations for services such as:

- banking
- payroll
- donor and supporter databases
- fundraising platforms
- email and cloud storage
- accounting systems
- website hosting
- payment processing
- beneficiary or case management systems.

Outsourcing these vital functions provides access to expertise, infrastructure and technology which would otherwise be beyond the reach of a smaller charity, but the important issue is whether there is a risk of being dependent on a particular provider for a critical function.

A useful exercise for trustees and senior managers is to identify the services the organisation could not easily operate without.

For each one, ask:

- What do we rely on this supplier for?
- What information do they hold?
- How long could we operate without the service?
- What alternative arrangements would we have?
- Who would take responsibility if something went wrong?

WHAT SHOULD TRUSTEES AND SENIOR LEADERS CONSIDER?

Cyber resilience does not have to begin with an expensive technology project.

For many charities the starting point is simply understanding the organisation's exposure and making sure sensible controls exist.

UNDERSTAND YOUR CRITICAL SUPPLIERS

Maintain a simple record of the external providers on which the charity relies.

Consider both the information they hold and the importance of their service (A CRM provider holding thousands of supporter records presents one type of risk. A payroll provider or bank whose service becomes unavailable presents another.). Consider a disaster recovery plan for the temporary or permanent sudden loss of that provider.

UNDERSTAND YOUR DATA

Know broadly what personal and sensitive information the charity holds and where it is stored.

Avoid retaining information simply because it may one day be useful. The less unnecessary information an organisation holds, the less information there is to lose.

THINK ABOUT WHAT HAPPENS WHEN A SERVICE IS UNAVAILABLE

Business continuity planning should consider digital suppliers as well as more traditional risks.

- Could payroll still be processed?
- Could key people be contacted?
- Could donations still be received?
- Could services to beneficiaries continue?
- Could essential financial transactions be authorised another way?

The answer will vary considerably depending on the charity.

REVIEW ACCESS CONTROLS

Basic controls remain important.

Multi-factor authentication should be used wherever appropriate. Access to systems should reflect what individual staff and volunteers genuinely need and old accounts should be removed promptly when people leave.

Government research published in 2026 found that cyber security was considered a high priority by senior management in 60% of charities. However, only 30% reported board-level responsibility for cyber security.

That suggests there remains an opportunity for more trustee boards to engage directly with the issue.

ASK QUESTIONS OF SUPPLIERS

Charities cannot independently audit every technology company they use, but they can ask questions about:

- Whether the supplier has any recognised cyber security certifications
- How information is backed up
- How quickly customers will be informed following an incident and what arrangements exist for restoring services

No certification or security standard can guarantee that an incident will never occur, but good due diligence reduces risk.

HAVE AN INCIDENT PLAN

Resilience means also preparing for the possibility that controls fail.

One of the worst times to decide who is responsible for responding to a cyber incident is while one is taking place.

Even a simple plan can identify:

- who coordinates the response
- who communicates with the affected supplier
- who informs trustees
- who considers regulatory reporting
- who handles communications with staff, beneficiaries, supporters or the media
- who contacts insurers or specialist advisers

The plan should be accessible even if normal IT systems are unavailable.

REPORTING AND REGULATORY RESPONSIBILITIES

A supplier experiencing a cyber incident does not necessarily mean every charity using that supplier must make the same regulatory reports.

Each organisation needs to assess its own circumstances.

Following the Beacon incident the Charity Commission reminded affected charities to consider whether the incident caused or risked significant harm to the charity, its beneficiaries, assets, services or reputation. Where that threshold is met trustees may need to make a serious incident report.

Separate responsibilities can arise under data protection legislation where personal information has been compromised.

The important practical point is to understand these responsibilities before an incident wherever possible and to know where specialist advice can be obtained if required.

THE SECONDARY RISK: FRAUD AFTER THE INCIDENT

The immediate disruption caused by a cyber incident may not be the end of the problem.

Information obtained through a breach can potentially make subsequent fraud or phishing attempts more convincing.

An email that appears to know the name of a colleague, donor, supplier or project can be much easier to trust than a generic scam.

AI is likely to make some forms of impersonation increasingly sophisticated.

That means staff and volunteers should be particularly alert following a known security incident involving an organisation or supplier with which the charity works.

Good financial controls remain an important defence but human defence should also be a priority for any organisation.

Unusual payment requests, changes to bank details or requests for sensitive information should be secondarily verified rather than relying solely on an email or message.

WHERE INSURANCE FITS IN THE PICTURE

Cyber insurance should not be viewed as an alternative to good security or effective business continuity planning. It can, however, form part of the resilience conversation.

Some insurance policies may contain limited protection relating to data or privacy liabilities. Specialist cyber insurance can potentially provide a broader response depending on the cover purchased.

Importantly, the value of cyber insurance may not simply be the financial limit shown on the policy.

Depending on the policy, cover can provide access to specialist expertise following an incident, potentially including legal advice, forensic investigation, regulatory support, communications assistance and crisis management as well as protection against certain financial losses.

For a smaller charity without internal cyber, legal or communications specialists, access to that expertise at the point an incident occurs can be particularly valuable.

Charities should understand:

- whether they have cyber insurance
- what the policy actually covers
- what significant exclusions or conditions apply
- whether important third-party suppliers are appropriately considered
- who should be contacted if an incident occurs

A PRACTICAL CONVERSATION FOR YOUR NEXT TRUSTEE MEETING

Cyber security can become intimidating when the discussion starts with technical terminology.

A more useful starting point may be five simple questions:

1. **Which digital services could we not operate without?**
2. **Where is our important or sensitive information held?**
3. **What would we do if one of those systems was unavailable for several days?**
4. **Who would lead our response if information was compromised?**
5. **What alternatives and specialist support would we have available?**

THE WIDER LESSON

The recent breach and service interruption examples are important not because every charity will experience exactly the same circumstances.

They are important because they make an often abstract risk much easier to understand.

Technology enables charities to operate more efficiently, reach supporters, process donations, manage finances and deliver services in ways that would previously have been impossible.

That reliance also needs to be part of risk and resilience conversations.

A vulnerability within a supplier can become your problem. A service being taken offline can affect you. Information being compromised can become your regulatory and reputational issue.

For smaller charities in particular, cyber risk may still feel like something belonging to larger and more technically sophisticated organisations.

These 2 examples should change our understanding of those risks.

Trustees do not need to understand every technical threat.

They do need to understand **what their charity depends upon, what could go wrong and how the organisation would respond if it did.**

That is ultimately what cyber resilience means.

Example incident information checked on 14 August 2026. This guide provides general information only and does not constitute advice. Professional advice should be obtained before applying any information contained within particular circumstances.

AUTHORS

AUTHOR PROFILE:

Tim Larden

Group Sales & Marketing Director

Tim Larden is a Director at Access Insurance. He has 25+ years experience in the insurance sector, with 20 years specialising in the charity sector. In 2015 he took up the running of charity-specialists Ladbrook Insurance, which was acquired by Access Insurance in 2025. Access is an ethically driven, charity-specialist, Chartered Insurance Broker that advises 18,000 charities, community and not-for-profit organisations.

COMPANY PROFILE:

Access Insurance

Access is an ethically driven, charity-specialist, Chartered Insurance Broker that advises 18,000 charities, community and not-for-profit organisations. Access Insurance is part of the Benefact Group, which means all available profits are given to charities and good causes.

accessinsurance.co.uk/charity | charity@accessinsurance.co.uk | 0333 344 7420