Cyber Essentials for Cathedrals: The Cost of Protection vs. Cost of a Breach?

Brief: Cathedrals are called to deliver the mission of God through worship, community, and outreach. To do this effectively, they depend on secure systems for communication, safeguarding, administration, and stewardship of resources. Cyber threats can undermine this mission by disrupting ministry, eroding trust, and draining finances.

What is Cyber Essentials

Cyber Essentials (CE) is a government-backed certification that protects against the majority of common cyber attacks. This paper compares the costs of implementing and maintaining Cyber Essentials (CE) with the financial, operational, and reputational risks of leaving cathedral IT systems unprotected.

Why Cyber Essentials Matters for Mission

- Ensures ministry and outreach can continue without disruption from cyber attacks.
- Protects sensitive data relating to safeguarding, volunteers, staff, and donors.
- Demonstrates stewardship of cathedral resources and accountability to donors.
- Shows leadership in governance, aligning with Charity Commission expectations.

Beyond Compliance — Stewardship & Mission

Cyber Essentials is more than an IT standard. For cathedrals, it is an act of stewardship: safeguarding the resources entrusted to them so they can be devoted to worship, community service, and outreach.

It reassures staff, volunteers, congregations, and donors that their data is respected and protected. And it ensures the mission of God can continue without unnecessary interruption or loss.

Real-World Examples

Ransomware at a UK Diocese IT supplier (2023): Parish communications were down for over a week, with recovery costs exceeding £50,000.

Phishing scam against a church treasurer (2022): Fraudulent emails led to unauthorised payments of nearly £20,000 before being detected.

Safeguarding data leak (charity, 2021): Personal details of volunteers and vulnerable individuals were exposed online, leading to an ICO fine and a long-term loss of donor trust.

Suite 1, 1 Cardale Park, Harrogate, North Yorkshire, HG3 1RY

supportdesk@andisa.net | 01423 290029 | www.andisa.net

Implementation Costs

- **Certification fee**:
  £300–£500 (self-assessment)
  or £1,500–£2,500 (guided).
- **Consultancy support** (if required):
  £2,000–£5,000.
- **Technical upgrades:**
  £2,000–£10,000 one-off
  (MFA, antivirus, patching, secure backup).
- **Staff training:**
  £500–£1,500.

  Year 1 total: typically £5,000–£15,000

Costs of not acting

- **ICO fines:**
  £10,000–£250,000 depending on breach severity.
- **Incident response (IT, legal, PR. increased premiums):**
  £5,000–£25,000 per event.
- **Ransomware/data recovery:**
  £10,000–£50,000+.
- **Downtime:**
  Weeks without systems, loss of fundraising and donor confidence.
- **Reputation:**
  loss of trust can reduce donations by 5–15% for years.

Conclusion

For a cathedral or similar organisation, the cost of Cyber Essentials implementation and maintenance is modest when compared to the potentially devastating consequences of a breach. Choosing CE is a practical step in stewarding resources faithfully, protecting trust, and ensuring that nothing hinders the mission of God.

If you are concerned about cyber security and want guidance then why not arrange a discovery call with one of our senior members of staff. We have atrack record in helping organisations implent secure protection and certification for Cyber Essentials.

Scan the barcode to arrange your free call.

Suite 1, 1 Cardale Park, Harrogate, North Yorkshire, HG3 1RY

supportdesk@andisa.net | 01423 290029 | www.andisa.net