TRUSTEE & BOARD GOVERNANCE BRIEFING

Cybersecurity for Care Charity Trustees

Five questions every board should ask to protect the people you support, the information you hold, and the services you provide.

Trends4You

Resource-Aware Cybersecurity (RACF-CC)

Why cybersecurity matters to your care charity

A cyber incident is not just an IT problem. It directly affects the safety, dignity, and continuity of care - preventing care workers from accessing digital care plans, interrupting medication administration records (eMAR where used), halting staff rotas, or exposing sensitive personal safeguarding notes. Care charities face the same threats as enterprise organisations, but operate with small generalist teams, constrained budgets, and legacy infrastructure. **Trustees do not need to be cybersecurity experts.** They do need to understand their organisation's risks, ask the right questions, and ensure proportionate, evidence-led action is taken.

1 What are our three biggest cybersecurity risks?

Could a cyber incident interrupt care delivery, expose personal safeguarding records, or prevent frontline staff from working?

Evidence to ask for: A concise, prioritised risk register identifying the top operational risks, their potential consequences on care delivery, named accountable owners, and current mitigations.

RACF-CC Prioritisation Tool

2 Could we continue providing care if our systems stopped working tomorrow?

What happens if electronic care records, medication systems (eMAR), staff rotas, or internet connectivity become unavailable during a shift?

Evidence to ask for: A practical business continuity plan, documented manual alternatives, such as paper MAR charts and emergency care notes where applicable, and results from a recent backup restoration drill.

RACF-CC Domain 5: Backup

3 Are we protecting the information entrusted to us?

Who can access sensitive care records? Are former employees and agency staff accounts promptly revoked? Are staff using protected accounts and devices?

Evidence to ask for: Joiner, mover, and leaver procedures, access review records, Multi-Factor Authentication (MFA) enforcement on email and cloud systems, and basic endpoint security checks.

RACF-CC Domains 1 & 2: Identity & Endpoints

4 Does everyone know what to do during a cyber incident?

Who should frontline care staff contact? Who decides whether systems must be isolated? Who manages safeguarding, family communications, and ICO notification within 72 hours where required?

Evidence to ask for: A clear, 1-page incident response plan, named operational responsibilities, out-of-band emergency contacts, and evidence that the procedure has been rehearsed.

RACF-CC Domain 7: Incident Response

5 How do we know our cybersecurity is improving?

Are we reducing meaningful operational risks to care delivery, or simply introducing more unread policies and vendor software subscriptions?

Evidence to ask for: A short, regular progress report showing improvements completed, outstanding high-priority risks, results of routine security checks, and decisions requiring board approval.

RACF-CC Control Assurance Tracker

What should the board do next?

- ✓ **Agree the three most significant cyber risks** to care delivery and operations.
- ✓ **Confirm who is accountable** for managing each agreed risk.
- ✓ **Record actions, owners, and realistic completion dates** in board minutes.
- ✓ **Request an assurance update** at the next scheduled board meeting.

"The goal is not perfect security. It is informed decisions, proportionate protection, and demonstrable improvement."

About RACF-CC

The Resource-Aware Cybersecurity Framework for Care Charities helps non-profits translate enterprise security into prioritised actions.

Risk over compliance	**Feasibility** over completeness
Containment over perfection	**Measurement** over assumption

Scan for resources

Free tools: trends4you.co.uk/racf-cc.html

This briefing supports governance discussions and does not replace legal or regulatory advice.