Charity Council

Cybersecurity Guide for Charities in Singapore

(Adapted from SID's Cyber Resilience Guide for Boards in Singapore)

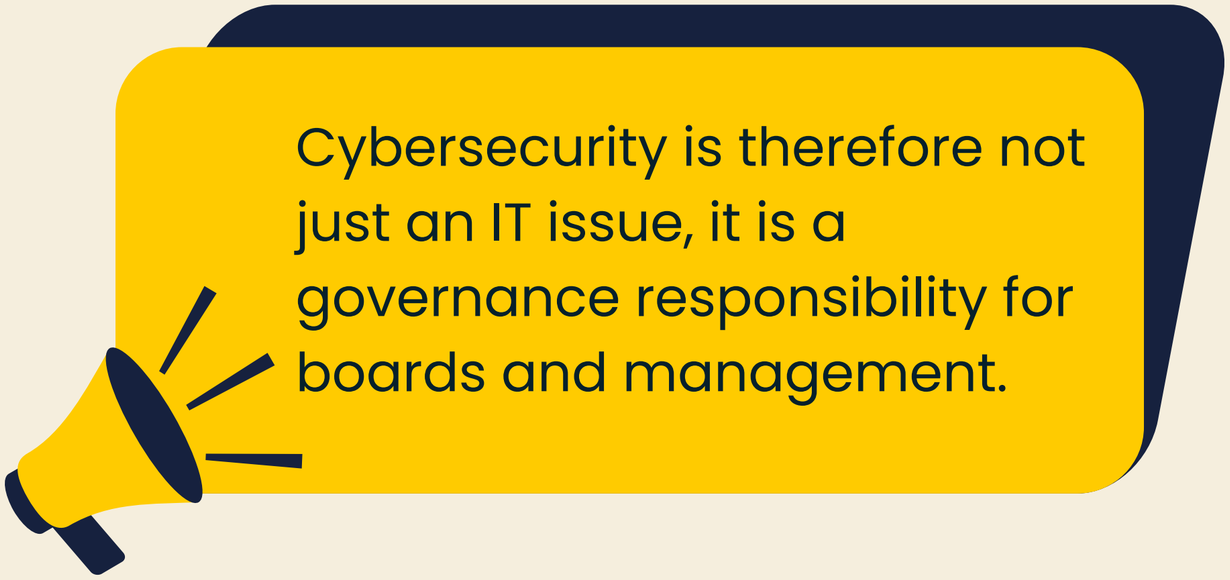
Introduction

Charities in Singapore rely heavily on digital tools to manage donor information, beneficiary data, and daily operations.

This makes them potential targets for cyber threats even if they believe they are “too small” to be attacked.

Cyber incidents can:

- Disrupt critical services to beneficiaries
- Expose sensitive personal and financial data
- Damage public trust and reputation



THIS GUIDE PROVIDES SIMPLE, PRACTICAL STEPS THAT ANY CHARITY REGARDLESS OF SIZE OR RESOURCES, CAN TAKE TO PROTECT ITSELF AND RESPOND EFFECTIVELY TO CYBER INCIDENTS.

If You Can't Do Everything, Do These 5 Things

1. Enable Multi-Factor Authentication (MFA) on email and key systems
2. Back up critical data regularly
3. Train staff and volunteers to spot phishing emails
4. Assign one person responsible for cybersecurity
5. Use only trusted vendors and systems

Section 1: Cyber Protection
(prevent attacks and reduce risk)

1. Implement Basic Cyber Hygiene (Most Important)

These are the minimum controls every charity should have:

- MFA enabled for email, banking, and cloud systems
- Strong passwords or passphrases (no reuse)
- Automatic software updates turned on
- Antivirus/anti-malware installed and updated
- Secure Wi-Fi (strong password, proper encryption)

Key priority is to enable MFA.

2. Know What You Must Protect

Focus on what matters most:

- Donor data
- Beneficiary data
- Financial/payment systems
- Email accounts

Limit access to only those who need it.

Protecting these key areas reduces most of your risk.

3. Train Staff and Volunteers

People are the first line of defence.

Ensure everyone knows:

- Do not click suspicious links or attachments
- Do not share passwords
- Report anything unusual immediately

Common threat: phishing emails pretending to be banks, government agencies, or senior staff.

Most cyber incidents happen because of human error.

Section 1: Cyber Protection
(prevent attacks and reduce risk)

4. Assign Ownership and Leadership
Cybersecurity must have clear ownership.

- Assign one responsible person (staff, volunteer, or board member)
- Include cybersecurity in board or management discussions at least annually
- Treat cyber risks as part of overall risk management

If no one owns cybersecurity, no one will manage it.

5. Manage Third-Party and Technology Risk
Charities often rely on vendors and digital tools.
Take simple precautions:

- Use trusted vendors with basic security practices
- Limit vendor access to only necessary data
- Include data protection and breach notification clauses in contracts
- Remove access when vendors are no longer engaged

Use of AI Tools

- Do not input confidential or personal data into public AI tools
- Ensure human review of AI-generated outputs

You can outsource services, but not responsibility.

Section 2: Cyber Resilience
(Respond, recover, and continue operations)

6. Detect Issues Early

Early detection reduces damage.

- Enable security alerts (e.g. unusual login notifications)
- Use antivirus tools that flag threats
- Watch for unusual system behaviour
- Ensure staff know who to report issues to

The faster you detect a problem, the smaller the impact.

7. Have a Simple Incident Response Plan

Every charity should have a basic plan.

3-Step Response:

1. **Contain** – Disconnect affected systems to stop spread
2. **Report** – Inform internal lead; assess if PDPC or stakeholders must be notified
3. **Recover** – Restore systems and fix vulnerabilities

Include:

- Key contacts (internal and external support)
- Clear roles and responsibilitie

A simple plan is better than no plan!

Section 2: Cyber Resilience
(Respond, recover, and continue operations)

8. Back Up Data and Ensure Continuity

Backups are critical.

- Back up important data (donor, financial, operational) regularly
- Store backups securely (cloud or offline)
- Test recovery periodically

Plan for disruptions:

- Identify critical operations
- Have temporary workarounds (manual processes if needed)

Backups are your last line of defence against ransomware.

9. Review and Improve Regularly

Cybersecurity is an ongoing process.

- Review practices at least once a year
- Update controls when systems or risks change
- Learn from incidents or near misses

Use available, free resources such as:

- CSA's SG Cyber Safe Programme
- Government advisories and toolkits

Small improvements over time make a big difference.

Quick Self-assessment Checklist

A) Critical (Do Immediately)

- ☐ MFA enabled for email and key systems
- ☐ Regular data backups in place
- ☐ Someone responsible for cybersecurity

B) Important

- ☐ Staff trained to recognise phishing
- ☐ Sensitive data identified and access controlled
- ☐ Vendors assessed for basic security
- ☐ Strong passwords or passphrases (no reuse)
- ☐ Antivirus/anti-malware installed and updated

C) Good to Have

- ☐ Incident response plan documented
- ☐ Periodic cybersecurity review conducted
- ☐ AI usage guidelines established

Quick Self-assessment Checklist

What This Means

Implemented “Critical“ & mostly “Yes” for others
→ Maintain and review annually

Some gaps
→ Prioritise “Critical” actions and staff awareness

Many gaps
→ Treat cybersecurity as an urgent governance priority

Conclusion

Cybersecurity may seem complex, but most risks can be reduced through simple, practical steps

For charities, strong cybersecurity:

- Protects donors and beneficiaries
- Ensures continuity of services
- Preserves trust and reputation

Ultimately, cybersecurity is about protecting YOUR mission and the community YOU serve.

Resources

Charities Capabilities Fund

For exempt, registered charities and IPCs

- Consultancy Grant: Consultancy projects by external consultants to review and draft policies and standard operating procedures for the charity.
- Info-Comm Technology Grant: For basic IT infrastructure and digital solutions.
- Shared Services Grant: Outsource of Informational Technology Management
- Training Grant: Courses on data protection/cyber security

Contact: NCSS_Grants@ncss.gov.sg

Transformation Sustainability Scheme Grant

For NCSS Members and MSF-funded agencies

- Consultancies relating to cybersecurity and data protection
- Digital solutions relating to data/cybersecurity under PSG solutions list

Contact: sector_capability@ncss.gov.sg