Cyber Resilience Safeguards Mission, People, and Impact

The Reality: Nonprofit organizations are increasingly targeted due to sensitive constituent and donor data, limited security resources, and interconnected systems.
A cyber incident can directly disrupt program delivery, community impact, and organizational credibility.

The Cost of Inaction

- Operational disruption to programs. Fundraising, and service delivery
- Loses of donor and stakeholder trust
- Financial impact from downtime, recovery costs, and potential loss of funding grants

What Proactive Resilience Looks Like

- Ongoing visibility into cyber risk across the organization
- Clear prioritization aligned to mission impact and organizational risk
- Measurable risk reduction over time

What Good Cyber Hygiene Really Means

(Not tools — habits and visibility)

- Knowing **where your highest business risks are today**
- Reducing **avoidable exposure** across people, process, and technology
- Prioritizing fixes based on **financial and operational impact**, not checklists
- Maintaining **continuous awareness**, not point-in-time assessments

Cyber resilience is mission stewardship

Get Started Here