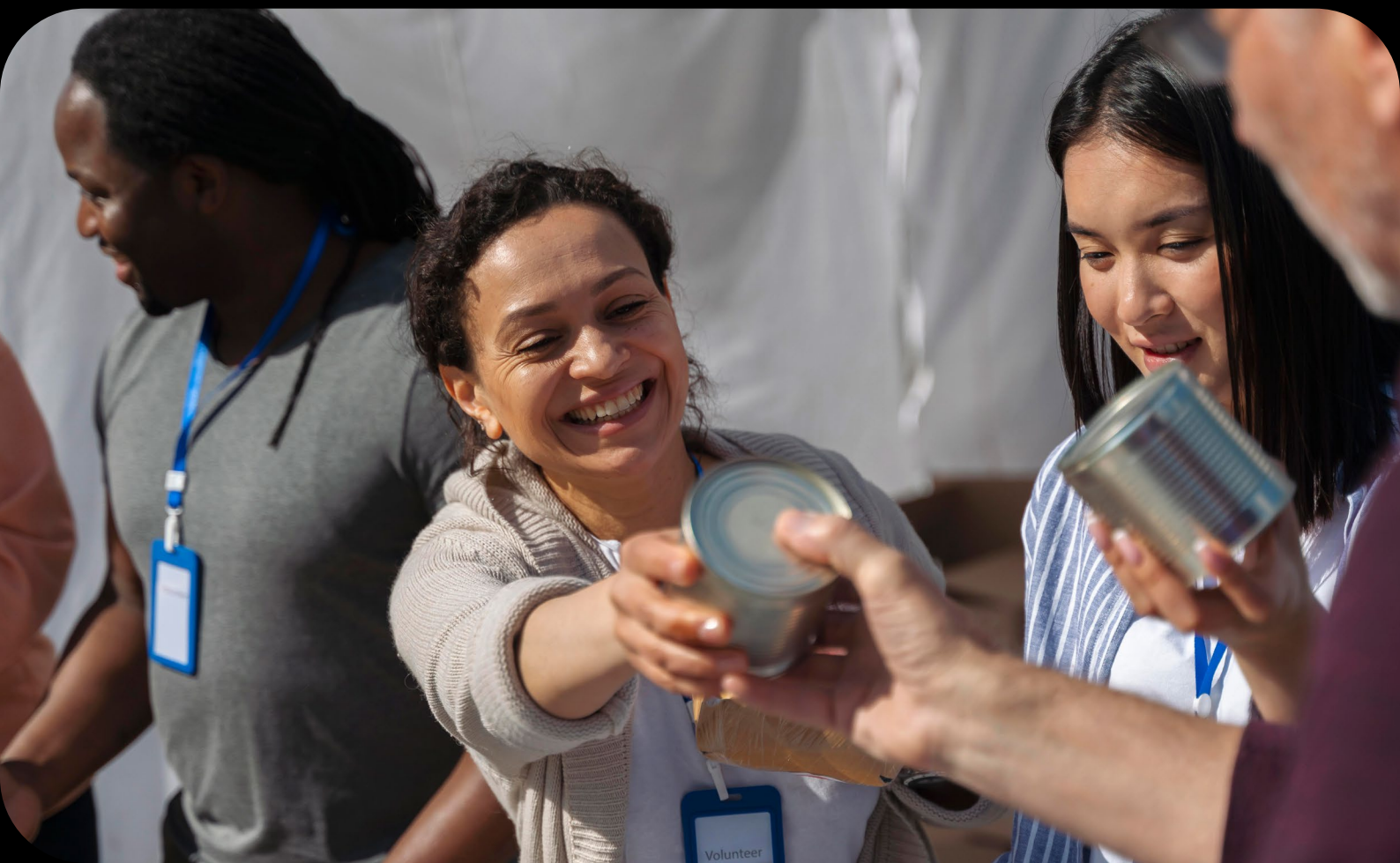
SERKET-TECH SECURITY

www.serkettech.com

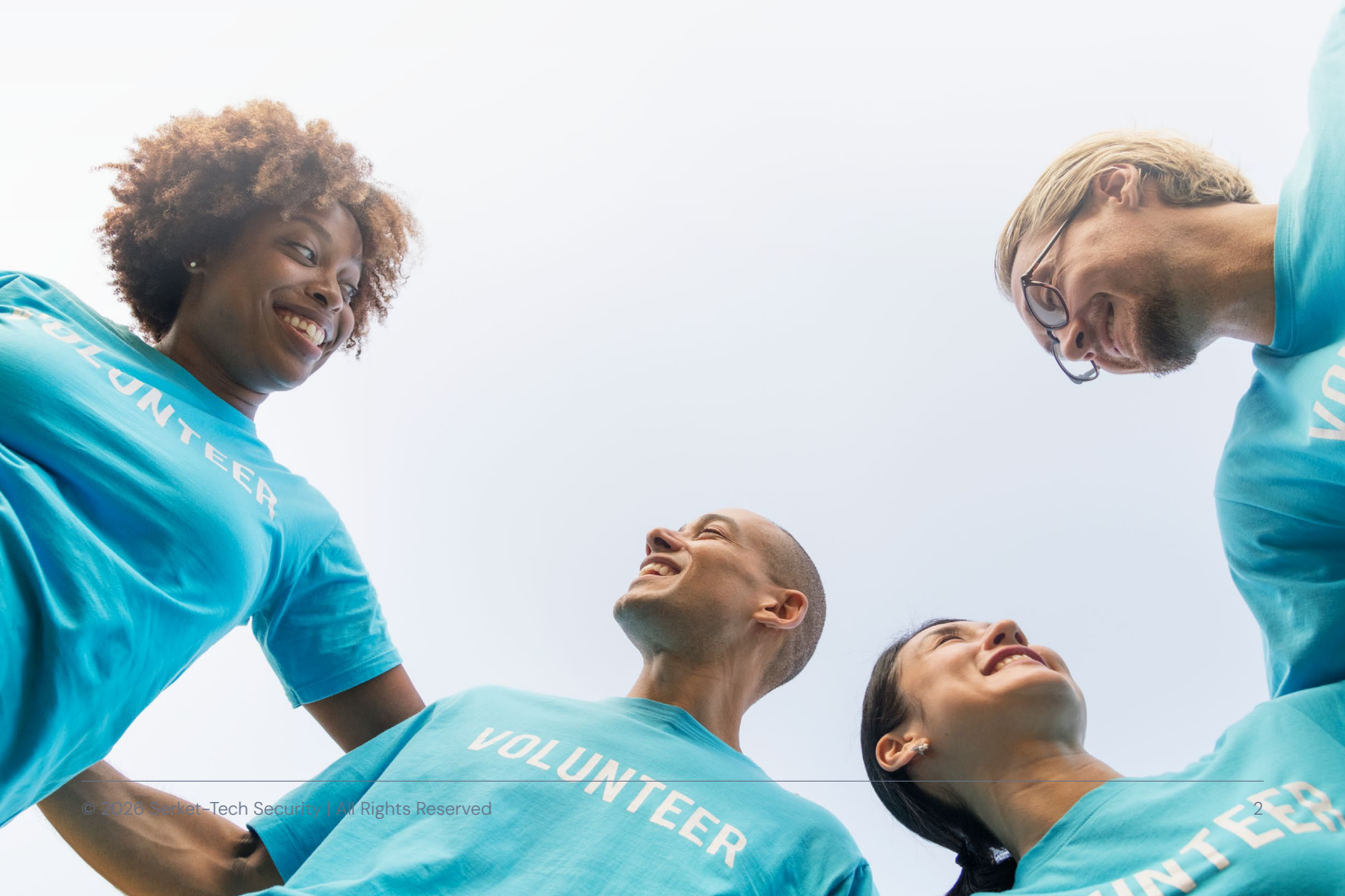
Serket-Tech Security: Securing the Mission



Nonprofit organizations are on the front lines of some of society's most important work helping to feed and shelter families, providing legal services to those in need, and empowering underserved communities.

Behind the scenes though, many nonprofits are operating with a critical vulnerability, inadequate cybersecurity. They face increasingly sophisticated cybersecurity threats making it imperative for them to prioritize and adopt proactive cybersecurity solutions.

Historically, cybercriminals have focused their efforts on financial institutions and large enterprises but that is changing, and nonprofits have emerged as high-value, low-resistance targets. Why? Because nonprofits hold a combination of sensitive donor data, financial records, and personally identifiable information, yet they are only able to allocate a fraction of their budget to modern cybersecurity solutions. This imbalance makes them attractive and ransomware groups, phishing operators, and state-sponsored actors alike have taken notice.



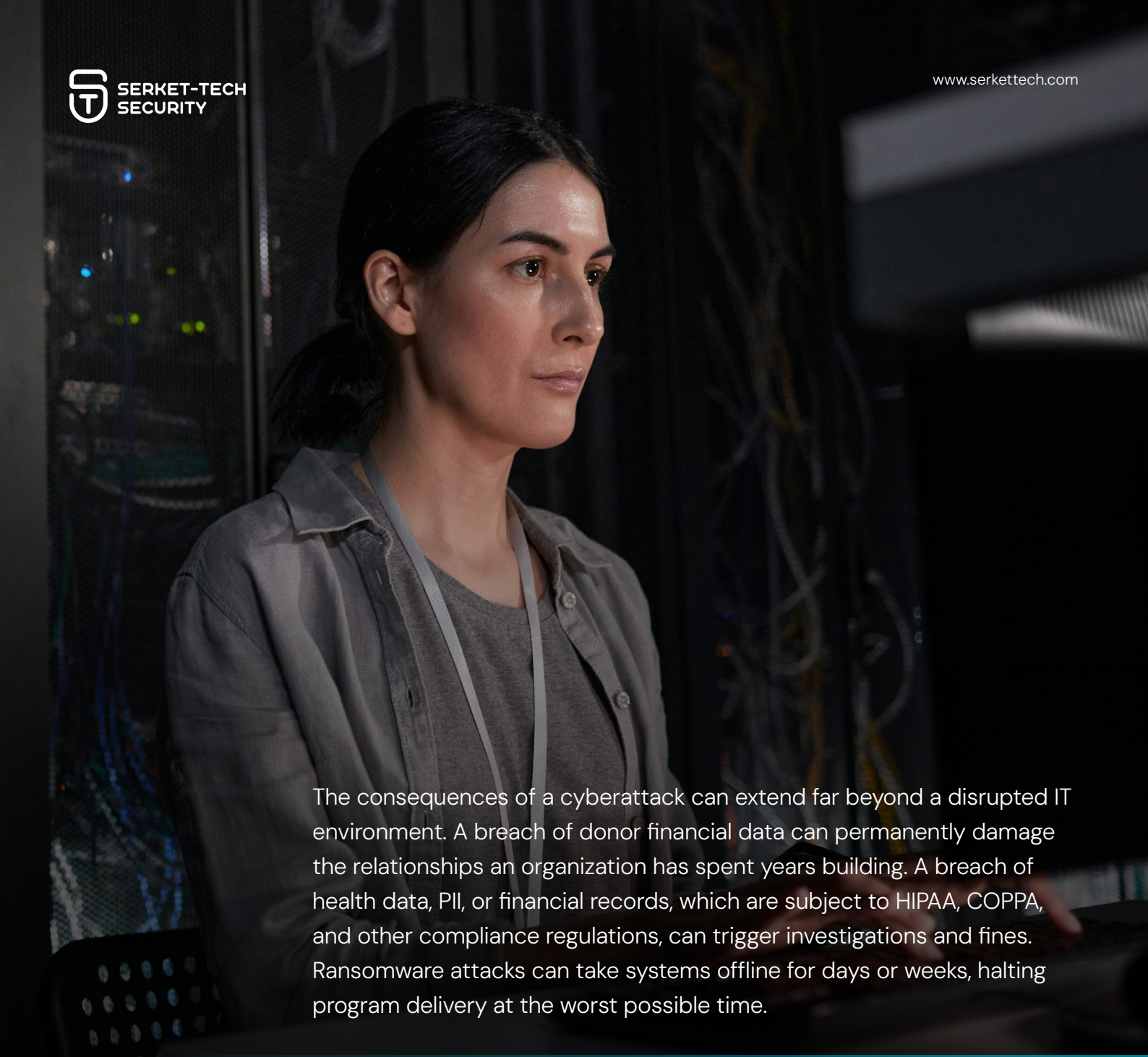
According to industry research,

over
60%
of nonprofits report experiencing at least one cyberattack or security incident.

In
2025
ransomware attacks against nonprofits continued to rise

with a reported average of
2,550
cyberattacks per week. Many more go unreported due to reputational concerns or a simple lack of detection capability.

Understanding why nonprofits are at risk requires looking into the challenges that make cybersecurity difficult to prioritize. Limited budgets impact funding for modern cybersecurity tools and training. Many nonprofits rely on rotating volunteers and part-time staff who may have access to sensitive information with little to no security training. Misconfigured grant management platforms, donor CRMs, cloud storage, and communication tools each introduce potential vulnerabilities and exposure.



The consequences of a cyberattack can extend far beyond a disrupted IT environment. A breach of donor financial data can permanently damage the relationships an organization has spent years building. A breach of health data, PII, or financial records, which are subject to HIPAA, COPPA, and other compliance regulations, can trigger investigations and fines. Ransomware attacks can take systems offline for days or weeks, halting program delivery at the worst possible time.

Cybersecurity should be a **mission-critical priority** and can no longer be treated as a back-office IT concern. The organizations doing the most important work in our communities deserve the protection to keep doing it. Organizations that lose donor trust, face regulatory penalties, or suffer prolonged operational disruption cannot fulfill their purpose.

The average data breach can cost a small organization over $150,000 and can be potentially catastrophic for most nonprofits.

The question is not whether your nonprofit can afford to invest in cybersecurity. The question is whether it can afford not to.

Serket-Tech Security is on a mission to help nonprofit organizations build resilient, secure technology environments that protect their data, their donors, and their core mission.

Contact us today to schedule a free cybersecurity consultation and risk assessment.

SERKET-TECH SECURITY

www.serkettech.com
(678) 989-7941
info@serkettech.com