CYBERSECURITY READINESS

A Quick Self-Assessment for Nonprofit Leaders, Finance Teams & Boards

As nonprofit operations go more digital, cybersecurity increasingly affects access to donations and funds, recurring payments and donor trust. A strong cybersecurity plan is not about eliminating risk entirely. It's about actively managing and mitigating risk so your organization can continue operating and making financial decisions if a disruption occurs.

This checklist is designed to help you assess your cybersecurity readiness through both an operational and financial lens.

- [ ] **Identify critical systems, data and financial risk**
  Know which systems support donations, payroll and vendor payments, as well as determine where sensitive donor and financial data is stored. Consider which disruptions would have the greatest impact on daily operations.
- [ ] **Clarify who has access and approval authority**
  Review which team members, volunteers and vendors can access financial systems, approve transactions or change donor payment instructions, especially where roles overlap.

Huntington Bank

- [ ] **Protect access to critical systems**
  Enable multi-factor authentication (MFA) for email, banking and donor platforms. Limit administrative privileges to essential users and review access regularly when staff or volunteer roles change.

- [ ] **Safeguard the ability to make and receive payments**
  Verify more than one trusted team member can securely access payment systems and confirm that backup processes are in place if primary access is disrupted.

- [ ] **Establish governance and board visibility around cyber risk**
  Ensure cybersecurity risk is discussed with leadership and the board as part of financial oversight, including how an incident could affect donor funds, operations and organizational reputation.

- [ ] **Have a documented cybersecurity response policy**
  Confirm your organization has a written policy outlining prevention and response, and that leadership and board members understand their roles if a cyber incident occurs.

- [ ] **Prepare for response and continuity**
  Define decision-makers, communication responsibilities and how programs and services will continue if systems are temporarily unavailable during a cyber incident.

- [ ] **Practice and review response readiness**
  Periodically test response plans through tabletop or discussion-based exercises. Update plans based on lessons learned.

- [ ] **Address third-party and vendor risk**
  Understand the cybersecurity posture of key vendors that handle donor data, payments or payroll.

- [ ] **Consider risk transfer as part of your strategy**
  Evaluate whether cyber liability insurance plays a role in your broader approach to financial risk management and recovery planning.

CYBERSECURITY READINESS IS ABOUT BALANCE

Cybersecurity readiness is not about adding complexity. It's about making sure leaders and boards can protect access to funds, maintain operational continuity and respond decisively when systems or donor trust are at risk.

Have questions? Your Huntington Business Banker can help you think through financial preparedness and risk management in support of your nonprofit's goals.