501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

NONPROFIT CYBERSECURITY TALKING POINTS FOR BOARDS OF DIRECTORS

Prepared by

Brian Scott

NONPROFIT CYBERSECURITY TALKING POINTS FOR BOARDS OF DIRECTORS

1. Cybersecurity Protects Our Mission

- **Key Message**: "A cyberattack could disrupt our ability to deliver programs and services to the communities we serve. Protecting our systems is directly linked to protecting our mission."
- **Why It Resonates**: Emphasizes that cybersecurity is a mission-critical investment, not just an IT expense.
- **Supporting Fact**: The *National Council of Nonprofits* (2023) reports that ransomware attacks can shut down nonprofit operations for weeks, delaying mission-critical work.

---

2. We Are a Target

- **Key Message**: "Hackers increasingly see nonprofits as soft targets because of limited cybersecurity resources. We are just as vulnerable as corporations, and the risks are growing."
- **Why It Resonates**: Frames cybersecurity as a proactive defense against real threats rather than a hypothetical scenario.
- **Supporting Fact**: IBM's *Cost of a Data Breach Report* (2023) highlights that nonprofit breaches have increased by 9% in recent years, with hackers targeting sensitive donor and program data.

---

3. Cybersecurity Is a Governance Priority

- **Key Message**: "Good cybersecurity practices are part of good governance. Donors, regulators, and partners expect us to protect the data entrusted to us."
- **Why It Resonates**: Aligns cybersecurity with the board's fiduciary, risk management and ethical responsibilities.
- **Supporting Fact**: According to the *Charity Digital Skills Report* (2023), 65% of funders prioritize nonprofits that demonstrate strong cybersecurity practices.

4. A Breach Could Cost Us More Than Money

- **Key Message**: "A data breach can harm our reputation and erode member, donor and partner trust, which could take years to rebuild. The financial impact is only part of the cost."
- **Why It Resonates**: Reinforces that reputation and trust are critical for long-term sustainability.
- **Supporting Fact**: *Blackbaud* (2023) found that 82% of donors would reconsider giving to a nonprofit that experienced a major data breach.

---

5. Proactive Measures Save Money

- **Key Message**: "Investing in cybersecurity now is far less expensive than responding to a breach later. Prevention is cost-effective and protects us from operational downtime."
- **Why It Resonates**: Focuses on cybersecurity as a financial safeguard and risk management strategy.
- **Supporting Fact**: The *Ponemon Institute* (2022) found that the average cost to remediate a breach is $4.35 million globally, significantly more than the cost of preventative measures.

---

6. Regulatory and Legal Risks Are Real

- **Key Message**: "We are subject to data privacy laws like GDPR, CCPA, and others. Noncompliance could result in legal penalties or fines, adding to the cost of a breach."
- **Why It Resonates**: Frames cybersecurity as necessary for legal and regulatory compliance, which is a board-level concern.
- **Supporting Fact**: *TechSoup* (2023) highlights that many nonprofits are underprepared for the compliance requirements of modern data privacy laws.

7. Donor Expectations Are Changing

- **Key Message**: "Today's donors expect transparency and security. Strengthening our cybersecurity shows that we're serious about protecting their contributions and data."
- **Why It Resonates**: Appeals to the board's understanding of donor expectations and stewardship.
- **Supporting Fact**: *Nonprofit Hub* (2023) states that digital trust is now a deciding factor for donor engagement and retention.

---

8. Cybersecurity Strengthens Organizational Resilience

- **Key Message**: "Strong cybersecurity practices make us more resilient, ensuring that we can continue operating even if we face an attack."
- **Why It Resonates**: Emphasizes long-term organizational stability and continuity.
- **Supporting Fact**: *NTEN* (2023) stresses that having a cybersecurity plan in place reduces downtime and speeds recovery after an incident.

---

9. Cybersecurity Is a Team Effort

- **Key Message**: "Cybersecurity isn't just an IT issue—it's a leadership issue. Our board has a role in setting the tone and ensuring that we prioritize these investments."
- **Why It Resonates**: Invites the board to take ownership and see cybersecurity as a strategic, organization-wide priority.
- **Supporting Fact**: The Nonprofit Alliance (2024) advocates that "An organization's [leadership] needs to view cybersecurity in the same manner they think of a financial or tax audit: part of the regular duties addressed each year."

---

10. Proposed Actions for the Board

- **Approve a cybersecurity budget**: “We recommend allocating [X]% of our annual budget to cybersecurity improvements.”
- **Support cybersecurity training**: “Investing in staff training is essential to reduce risks caused by human error.”
- **Establish board oversight**: “Consider forming a cybersecurity subcommittee to ensure regular updates and alignment with best practices.”
- **Adopt a cybersecurity policy**: “We need a formal cybersecurity policy that outlines our approach to protecting data and responding to incidents.”

Final Thought

Reassure the board: "Cybersecurity is a manageable risk if we address it proactively. By taking action today, we’re protecting our mission, our reputation, and the trust of our stakeholders for years to come."