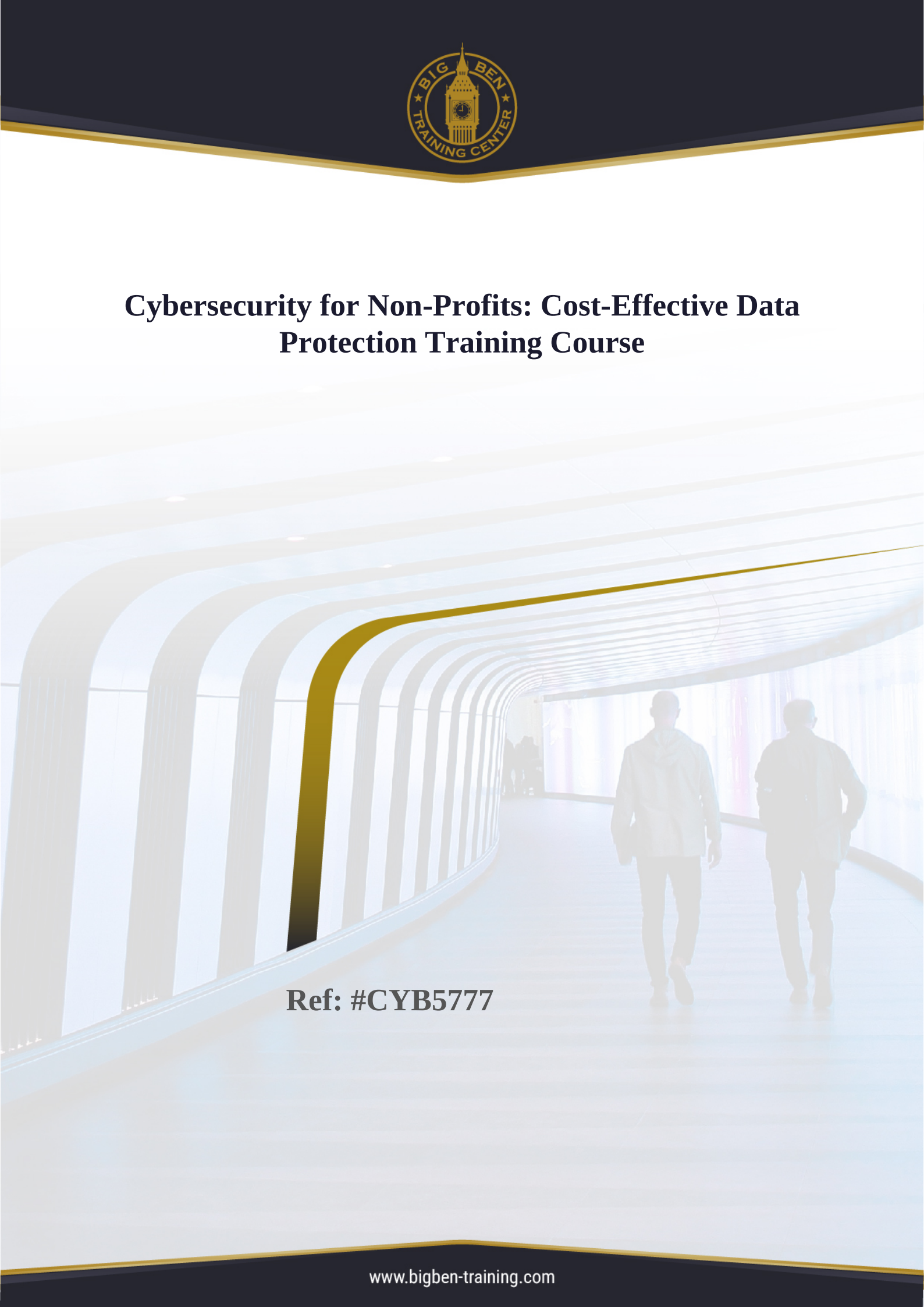
Cybersecurity for Non-Profits: Cost-Effective Data Protection Training Course



Ref: #CYB5777

Course Introduction / Overview:

This comprehensive training course is designed to provide non-profit leaders and staff with the essential knowledge and practical skills required to protect their organizations from cyber threats. Non-profits often handle sensitive donor and beneficiary data, but they operate with limited budgets and IT resources. This program goes beyond a general overview of cybersecurity and focuses on the unique challenges and cost-effective solutions for the non-profit sector. Participants will learn how to implement robust data protection strategies, manage privacy risks, and ensure the integrity of their digital assets without a large IT budget. We will cover key topics like phishing defense, secure cloud practices, and the development of an incident response plan. Drawing from the academic research of renowned authors like Gene Kim and his work on DevOps and organizational efficiency in his book "The Phoenix Project," this program provides a strategic and practical framework for leveraging limited resources for maximum security impact. His work highlights that security is not a separate function but an integrated part of a streamlined process. This course at BIG BEN Training Center will empower you to build a resilient and trustworthy organization that can continue its vital work without interruption.

Target Audience / This training course is suitable for:

- Non-profit executive directors.
- IT managers and staff.
- Fundraising and development managers.
- Volunteer coordinators.
- Board members.
- Program managers.
- Staff responsible for donor or client data.

Target Sectors and Industries:

- Non-profit organizations.
- Charitable and social services.
- Advocacy and human rights groups.
- Educational institutions.
- Religious organizations.
- Government agencies and equivalents.
- Foundations and trust.

Target Organizations Departments:

- IT.
- Development and Fundraising.
- Finance.
- Human Resources.
- Program Management.
- Volunteer Management.
- Communications.

Course Offerings:

By the end of this course, the participants will have able to:

- Implement cost-effective cybersecurity controls.
- Develop a data protection strategy for a non-profit.
- Protect sensitive donors and client data.
- Create a plan to respond to a cyber incident.
- Educate staff on cybersecurity best practices.
- Secure cloud applications and remote work.
- Identify and mitigate common threats like phishing.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, scenario-based methodology that focuses on the unique constraints of non-profit organizations. The program includes workshops where participants will develop a low-cost security plan for a fictional non-profit. You will learn to prioritize risks and allocate resources effectively, proving that security is possible without a massive budget. The course emphasizes a collaborative approach, encouraging participants to share their challenges and successes. The instructor will provide expert guidance on how to leverage free and low-cost tools and how to build a security-conscious culture from the ground up. This approach ensures the knowledge and skills gained are directly applicable to building a resilient organization that can continue its mission without interruption.

Course Agenda (Course Units):

Unit One: The Non-Profit Threat Landscape

- Common cyber threats to non-profits.
- The value of donor and client data.
- Understanding your organization's risk.
- The importance of a security mindset.
- Social engineering and phishing attacks.
- Case study: a ransomware attack on a non-profit.
- The ethical responsibility of data protection.

Unit Two: Foundational Security for Low Budgets

- Risk assessment with limited resources.
- Implementing strong passwords and multi-factor authentication.
- The use of free security tools.
- Securing email and communications.
- Best practices for data backup and recovery.
- Securing remote work.
- Practical lab: a risk prioritization exercise.

Unit Three: Data Protection and Privacy

- Data inventory and mapping.
- Protecting sensitive client and donor data.
- Privacy policies and compliance.
- Secure data handling and storage.
- Data privacy and legal requirements.
- Secure volunteer and staff onboarding.
- Case study: a data privacy incident.

Unit Four: Incident Response and Recovery

- Developing a simple incident response plan.
- Steps to take during a cyber incident.
- Crisis communication.
- Notifying stakeholders and authorities.
- Post-incident review.
- Tabletop exercise: a simulated cyberattack.
- Lessons learned from past incidents.

Unit Five: Building a Culture of Security

- The role of leadership.
- Creating a security-conscious culture.
- Effective security awareness training for staff and volunteers.
- Measuring program effectiveness.
- Long-term security planning.
- The future of cybersecurity for non-profits.
- Final project: a security roadmap.
- Frequently Asked Questions:

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In a non-profit environment where resources are scarce and every dollar must go toward the mission, how can a leader justify the investment of time and money in cybersecurity when the benefits are often invisible until a catastrophic incident occurs?

What unique qualities does this course offer compared to other courses?

This course stands out by providing a unique and vital focus on cybersecurity specifically for the non-profit sector. Unlike general security training that assumes a large budget, this program is designed for organizations that must be resourceful. The curriculum is built around a practical, cost-effective approach. It teaches you how to leverage free and low-cost tools, prioritize the most critical risks, and build a culture of security without significant financial investment. The emphasis on real-world scenarios and on creating a security plan that is both effective and financially feasible distinguishes this course from others. It is for non-profit professionals who are ready to protect their organization's mission and its beneficiaries' data.