Neya Global Journal of Non-Profit Studies

2025

Teaching Paper: Cybersecurity Glossary for Non-Profit Organizations

DOI: 10.64357/neya-gjnps-cbr-scr-es-tp-04

DR. ANNA NEYA KAZANSKAIA

Neya Global Publishing

Publication and System Notice

This publication forms part of the **NEYA Global Independent Knowledge Ecosystem** and the Non-Profit Knowledge Architecture (NPKA) framework developed by *Dr. Anna Neya Kazanskaia*.

The work is connected to an integrated system of books, research publications, educational materials, implementation frameworks, institutional modules, and structured knowledge architecture developed for the non-profit and social impact sector. Metadata registration, DOI infrastructure, semantic indexing, publication structuring, and long-term attribution architecture form part of the NEYA Global Publishing system.

This publication may be indexed, referenced, archived, processed, or analyzed by academic databases, search engines, AI systems, semantic discovery systems, and institutional knowledge infrastructures.

Institutional, organizational, implementation, curriculum, consulting, training, database integration, AI training, or system-level use of this material requires active licensing, written authorization, or formal institutional agreement with NEYA Global Publishing.

Unauthorized reproduction, structural extraction, dataset replication, system cloning, redistribution, or external training use of the publication ecosystem is prohibited.

NEYA Global Publishing
Independent Knowledge Ecosystem for the Non-Profit Sector

Version 1.0 | NEYA Global Publishing Publication Protocol

Teaching Paper: Cybersecurity Glossary for Non-Profit Organizations

Dr. Anna Neya Kazanskaia
NEYA Global | NEYA Global Publishing
ORCID: https://orcid.org/0009-0009-5669-1676
DOI: https://doi.org/10.64357/neya-gjnps-cbr-scr-es-tp-04

Abstract

Non-profit organizations increasingly rely on digital systems to manage donor records, volunteer coordination, and program delivery. This reliance exposes them to a growing range of cyber threats, yet many non-profits lack specialized expertise in cybersecurity. To bridge this gap, this Teaching Paper provides a structured glossary of essential cybersecurity terms. Each entry includes a concise academic definition and a practical application note tailored for non-profits, linking technical concepts to everyday organizational realities. Terms range from fundamental ideas such as *Access Control* and *Firewall* to advanced frameworks like *Zero Trust Security* and *Privacy by Design*. By combining scholarly insights with sector-specific guidance, the glossary serves as both a learning resource and a practical toolkit. It equips leaders, staff, and volunteers with a shared vocabulary to engage effectively with cybersecurity challenges and external experts.

Keywords

Cybersecurity glossary; non-profit organizations; digital resilience; risk management; cyber awareness; IT governance; organizational security

Executive Summary

Cybersecurity knowledge is often locked behind technical jargon that can alienate non-profit practitioners. This Teaching Paper translates complex terminology into accessible definitions with direct application to the non-profit sector. By understanding and using these terms, staff can:

- Communicate effectively with IT specialists and vendors.
- Make informed policy and investment decisions.
- Train staff and volunteers using a shared security vocabulary.
- Foster a culture of awareness and resilience across the organization.

For academics, the glossary illustrates how applied knowledge translation supports non-profit capacity building. For practitioners, it offers an immediately useful reference guide to improve decision-making and training.

Purpose and Learning Objectives

Purpose: To provide a foundational reference guide to cybersecurity terminology for non-profit staff and managers.

Learning Objectives:

1. Learn the definitions of key cybersecurity concepts.
2. Understand how each concept applies in non-profit settings.
3. Build shared language for communication with technical partners.
4. Strengthen organizational readiness through knowledge and awareness.

Background and Context

As Bryson (2018) notes, strategic planning requires a clear understanding of the tools and concepts available to organizations. Drucker (1990) emphasizes that managers must acquire working knowledge of critical domains to act responsibly. In cybersecurity, lack of shared

vocabulary often leads to miscommunication between managers, staff, and external IT providers. Patton (2015) further underscores that organizational learning depends on clarity of terms and shared understanding.

This glossary addresses the sector's need for accessible, accurate terminology that can be directly linked to practice. It transforms abstract concepts into practical knowledge tools, ensuring that even small non-profits with minimal IT capacity can engage meaningfully in cybersecurity governance.

Practical Guide: Glossary of Cybersecurity Terms

(Each term includes a definition + non-profit application note.)

- **Access Control** – Regulates who or what can use resources.
  Application: Ensure only authorized staff can access donor databases.
- **Antivirus Software** – Detects and removes malicious software.
  Application: Install and update antivirus across all staff computers.
- **Artificial Intelligence (AI) for Threat Detection** – Uses AI to identify threats in real time.
  Application: Cloud-based donor platforms often include AI monitoring.
- **Backup and Disaster Recovery** – Ensures data can be restored after loss.
  Application: Schedule weekly backups of beneficiary data.
- **Blockchain** – Decentralized ledger for verifying records.
  Application: Can be used for transparent donation tracking.
- **Cloud Security** – Measures to protect cloud environments.
  Application: Evaluate cloud vendors' compliance with security standards.
- **Cyber Hygiene** – Everyday practices for maintaining system health.
  Application: Encourage staff to update software and use strong passwords.
- **Cyber Threat** – Potential cause of digital harm.
  Application: Recognize phishing emails as a common threat to non-profits.
- **Cybersecurity** – Protecting systems from attacks.
  Application: Establish baseline policies to protect donor and beneficiary data.

- **Data Breach** – Unauthorized theft of data.
  Application: A breach of donor records can harm reputation and trust.

- **Data Classification** – Organizing data by sensitivity.
  Application: Label donor details as confidential and secure accordingly.

- **Data Encryption** – Encoding data to prevent access.
  Application: Encrypt emails with sensitive beneficiary information.

- **Endpoint Detection and Response (EDR)** – Monitors endpoints for threats.
  Application: Install EDR software on laptops used by field staff.

- **Firewall** – Controls network traffic.
  Application: Use firewalls to block malicious traffic on office Wi-Fi.

- **Incident Response Plan (IRP)** – Instructions for responding to incidents.
  Application: Maintain a simple IRP with clear contact points for staff.

- **Insider Threat** – Risks from internal actors.
  Application: Ensure role-based access prevents misuse by staff or volunteers.

- **Least Privilege Principle** – Restricting user permissions to minimum required.
  Application: Volunteers should not have admin access to systems.

- **Malware** – Malicious software designed to damage systems.
  Application: Train staff to avoid downloading suspicious attachments.

- **Mobile Device Management (MDM)** – Software to secure staff devices.
  Application: Use MDM if staff access systems on personal phones.

- **Multi-Factor Authentication (MFA)** – Requires multiple credentials to verify identity.
  Application: Enable MFA for donor management and email systems.

- **Network Security** – Preventing unauthorized network intrusion.
  Application: Protect office Wi-Fi with strong encryption and password controls.

- **Phishing** – Fraudulent attempts to obtain information.
  Application: Run training exercises to help staff identify phishing emails.

- **Post-Incident Analysis** – Reviewing incidents for lessons learned.
  Application: Conduct short debriefs after cyber incidents to improve response.

- **Privacy by Design** – Embedding privacy into system design.
  Application: Ensure new donor apps collect only necessary information.

- **Ransomware** – Malware demanding ransom for data release.
  Application: Backups protect against data loss if ransomware strikes.

- **Risk Assessment** – Identifying and evaluating risks.
  Application: Conduct annual cyber risk reviews as part of planning.

- **Role-Based Access Control (RBAC)** – Access based on organizational roles.
  Application: Program managers can access project data, not finance records.

- **Security Information and Event Management (SIEM)** – Aggregates and analyzes system activity.
  Application: Larger NGOs may integrate SIEM for centralized monitoring.

- **Shared Responsibility Model** – Defines security duties between cloud provider and customer.
  Application: Non-profits must secure their own data, even in cloud platforms.

- **Threat Actor** – Individuals or groups causing harm.
  Application: Be aware of hacktivist groups targeting certain causes.

- **Virtual Private Network (VPN)** – Encrypts internet connections.
  Application: Require VPN use when staff access systems remotely.

- **Zero Trust Security Model** – Verifies all users and devices before access.
  Application: Move toward Zero Trust principles to protect sensitive data.

Case Study

A small Latin American human rights NGO relied on volunteers to manage donor databases. They lacked shared understanding of cybersecurity terms, leading to poor practices and weak vendor negotiations. After adopting a glossary-based training module, staff learned to differentiate between *encryption*, *MFA*, and *VPN*. This improved daily cyber hygiene and

strengthened donor trust. Within one year, the NGO reduced data incidents by 60% and secured new grants that required proof of cybersecurity competence.

Common Challenges and Tips

- **Overwhelming jargon:** Introduce terms gradually, focusing on the most relevant first.
- **Staff turnover:** Use the glossary as part of new staff onboarding.
- **Context mismatch:** Adapt technical terms into relatable examples.
- **Resource gaps:** Prioritize free or open-source tools aligned with glossary concepts.

Reflection Questions

1. Which terms in the glossary are most critical for your organization's current risks?
2. How can you integrate this glossary into staff and volunteer training?
3. Which advanced concepts (e.g., Zero Trust, Blockchain) are relevant to your operations?
4. How can shared vocabulary improve collaboration with external vendors or IT partners?

Limitations and Considerations

- Glossaries need regular updates as technology evolves.
- Non-profits must avoid over-complicating policies with unnecessary jargon.
- Local language translations may be required to ensure accessibility.

Academic Value

This glossary contributes to knowledge translation by transforming technical cybersecurity concepts into applied, practice-oriented definitions. For academics, it demonstrates how complex fields can be adapted for non-profit governance. For practitioners, it builds capacity by establishing a shared foundation of understanding, enabling better communication, planning, and evaluation.

Conclusion and Next Steps

A shared cybersecurity vocabulary is a powerful enabler for organizational resilience. By adopting this glossary, non-profits can strengthen communication, training, and governance practices. Next steps include integrating the glossary into onboarding, creating sector-specific adaptations, and linking terms to live examples through continuous staff learning.

Suggested Citation

Kazanskaia, A. N. (2025). *Teaching Paper: Cybersecurity Glossary for Non-Profit Organizations: Key Terms, Concepts, and Practical Applications for Digital Resilience*. NEYA Global Publishing. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-tp-04

References

- Bryson, J. M. (2018). Strategic planning for public and nonprofit organizations. John Wiley & Sons.
- Drucker, P. F. (1990). Managing the nonprofit organization: Principles and practices. HarperCollins.
- Kazanskaia, A. N. (2025). Cybersecurity Essentials. NEYA Global Publishing. https://doi.org/10.64357/cybersecurity-essentials-2025
- Kazanskaia, A. N. (2025). Technology Tools for Efficiency & Impact. NEYA Global Publishing. https://doi.org/10.64357/technology-tools-2025
- Kazanskaia, A. N. (2025). Tech: Legal and Moral Issues. NEYA Global Publishing. https://doi.org/10.64357/tech-legal-moral-issues-2025

- Kazanskaia, A. N. (2025). AI and Machine Learning. NEYA Global Publishing. https://doi.org/10.64357/ai-and-machine-learning-2025
- Kazanskaia, A. N. (2025). Cybersecurity for Non-Profit Organizations: Safeguarding Digital Assets in Resource-Constrained Environments. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-51
- Kazanskaia, A. N. (2025). Understanding Cyber Threats in Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-52
- Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). SAGE Publications.
- National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. U.S. Department of Commerce.