American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Capability Maturity in Community-Based Nonprofits

Dr. Sophia R. Bennett

Associate Professor, York University, Canada

Abstract

Community-based nonprofit organizations increasingly depend on digital technologies for donor administration, volunteer coordination, grant management, beneficiary communication, fundraising, financial transactions, case management, cloud collaboration, and delivery of community services. Their digital dependence is not always accompanied by comparable cybersecurity capability. Small nonprofits may operate with limited information-technology staffing, volunteer-managed systems, constrained budgets, donated or legacy technology, numerous cloud services, and inconsistent formal security governance. The problem is sufficiently recognized in current public guidance that the National Institute of Standards and Technology's Cybersecurity Framework 2.0 Small Business Quick-Start Guide explicitly states that its recommendations can assist relatively small organizations including nonprofits, while CISA has issued separate guidance for civil-society organizations facing significant threats with limited defensive resources.

This study develops a cybersecurity capability-maturity framework specifically for community-based nonprofits. The proposed model evaluates governance, asset knowledge, identity and access security, data protection, technology maintenance, third-party management, detection, incident response, recovery, and workforce awareness. Small nonprofits can advance substantially through governance clarity, multifactor authentication, secure backups, prompt account removal, basic asset inventories, prioritized patching, staff and volunteer awareness, supplier oversight, incident-response planning, and use of shared or no-cost cybersecurity resources. Current NIST and CISA guidance supports this prioritized approach for smaller and less-resourced organizations.

The paper concludes that mature nonprofit cybersecurity should be interpreted as an organizational capacity to understand risk, protect mission-critical services, detect abnormal activity, respond proportionately, restore trusted operations, and learn continuously. A community-supported maturity model is particularly suitable for smaller organizations because cybersecurity clinics, sector partnerships, shared expertise, external service providers, grant networks, and public cybersecurity resources can amplify limited internal capacity without transferring responsibility for governance.

Keywords: nonprofit cybersecurity, cybersecurity capability maturity, community-based organizations, cyber resilience, NIST Cybersecurity Framework, cybersecurity governance, civil society cybersecurity, cyber hygiene, incident readiness, nonprofit digital resilience

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Community-based nonprofits occupy an increasingly digital operating environment. Organizations involved in social assistance, youth development, education, cultural activities, community health, humanitarian support, advocacy, environmental programs, local development, and other mission-oriented activities commonly use email, cloud storage, digital payment platforms, donor databases, constituent-management systems, videoconferencing, web portals, mobile applications, and third-party software. Their technology environments can therefore hold financial information, employee and volunteer records, donor details, beneficiary information, confidential communications, credentials, and operational records. For many organizations, digital interruption can impair not merely administration but delivery of community services.

The cybersecurity challenge is intensified by organizational scale. A community nonprofit may not employ a chief information security officer, dedicated security operations team, network engineer, privacy specialist, or incident-response professional. Technology administration may be distributed among a small number of employees, part-time contractors, volunteers, managed service providers, and cloud vendors. NIST specifically designed its CSF 2.0 Small Business Quick-Start Guide for organizations with modest or nonexistent cybersecurity plans and states that the guidance is also applicable to relatively small nonprofit organizations, schools, and government agencies. CISA's guidance for civil-society organizations similarly recognizes that some mission-based organizations operate in a high-threat environment while having limited defensive capacity.

Limited resources do not imply that cybersecurity must remain informal. The NIST Cybersecurity Framework 2.0 organizes cybersecurity risk management around six interconnected Functions: Govern, Identify, Protect, Detect, Respond, and Recover. NIST presents these functions as a comprehensive view of cybersecurity risk management rather than a technology checklist. This structure is useful for nonprofits because it reveals that cybersecurity capability includes leadership decisions, asset knowledge, staff practices, incident preparation, supplier oversight, and recovery planning in addition to technical safeguards. A small nonprofit may therefore strengthen maturity substantially before investing in sophisticated security technology.

Prioritization is essential because resource-constrained organizations cannot implement every possible control simultaneously. CISA's Cybersecurity Performance Goals are designed as a prioritized baseline of cybersecurity practices and include measures such as stronger authentication, vulnerability management, logging, incident planning, and other foundational protections. The Center for Internet Security uses a similar prioritization concept through Implementation Group 1, which it describes as essential cyber hygiene and an entry point to the CIS Critical Security Controls for organizations building foundational defensive capability. For nonprofits, the strategic implication is that maturity should advance from the most consequential and feasible safeguards rather than through indiscriminate technology procurement.

The present paper therefore develops a Community Nonprofit Cybersecurity Capability Maturity Model (CN-CMM). The model recognizes that community nonprofits differ in mission, size, funding, sensitivity of information, public profile, technology architecture, and threat exposure. It does not assume that every organization requires enterprise-scale security infrastructure. Instead, maturity is defined as the increasing institutional ability to govern cybersecurity risk, maintain basic cyber hygiene,

coordinate external support, respond to disruption, protect vulnerable stakeholders, and improve security over time. Because no nonprofit survey or operational dataset was supplied, the analysis uses explicitly simulated maturity distributions. No simulated value is presented as an observed characteristic of the nonprofit sector.

2. Objectives of the Study

2.1 To Define Cybersecurity Capability Maturity for Community Nonprofits

The first objective is to establish a maturity concept that reflects the operational realities of smaller mission-based organizations. Cybersecurity capability is treated as an integrated combination of governance, people, processes, technology, external partnerships, and recovery capacity.

The model distinguishes between possessing individual controls and maintaining a dependable organizational security capability. A nonprofit may, for example, enable antivirus software while lacking account-removal procedures, tested backups, clear incident ownership, or supplier-risk awareness. Such an organization has individual technical safeguards but remains institutionally immature.

2.2 To Identify Affordable High-Impact Capability Improvements

The second objective is to identify security practices capable of generating significant risk reduction without requiring enterprise-level expenditure.NIST's guidance for smaller organizations emphasizes practical cybersecurity risk management, while CISA's Performance Goals and no-cost resource collections provide prioritized and externally supported paths for organizations that cannot maintain extensive internal security teams.

The study therefore considers identity protection, backups, asset awareness, access control, software maintenance, staff and volunteer awareness, third-party oversight, incident planning, and external support as maturity-building priorities.

2.3 To Develop a Community-Supported Maturity Pathway

The third objective is to determine how shared capability can compensate for limited in-house specialization.

A small nonprofit may reasonably obtain vulnerability assessment, security training, incident assistance, managed security, cyber clinics, legal guidance, and specialized technical support externally while retaining responsibility for risk decisions. CISA maintains cybersecurity resources and services intended to improve access to assistance for smaller and high-risk organizations.

The resulting maturity model therefore includes community-supported capability as a distinct developmental stage rather than assuming that security maturity requires complete technical self-sufficiency.

3. Review of Literature

3.1 Cybersecurity Maturity as Progressive Organizational Capability

Cybersecurity maturity models provide organizations with a structured means of evaluating their current security state and identifying a more capable future state. Recent maturity research increasingly emphasizes progression, risk sensitivity, continuous improvement, and organizational scalability rather

than a fixed checklist. Papachristofis and colleagues' Cyber-Resistivity Maturity and Scoring Framework, for example, was developed to help organizations of different sizes evaluate cybersecurity and resilience through progressive assessment, weighting, criticality, complexity, and benchmarking. The framework explicitly emphasizes quick wins and prioritized improvements where high value can be achieved with comparatively low implementation complexity.

This approach is particularly relevant to nonprofits because capability improvement rarely occurs through one major transformation. A small organization may first establish clear responsibility for cybersecurity, then identify important data and accounts, strengthen authentication, improve backups, formalize onboarding and offboarding, add vulnerability management, and later introduce more mature monitoring and incident-response capabilities. The progression is cumulative.

The distinction between cybersecurity and cyber resilience is also important. Preventive capability concerns reducing the likelihood and impact of compromise, whereas resilience additionally concerns the organization's ability to continue, restore, and adapt after adverse cyber events. Recent maturity research treats resilience and security as related but distinct dimensions of organizational preparedness.

NIST's June 2020 Ransomware Risk Management Community Profile reinforces this lifecycle perspective and explicitly states that it is intended for organizations including nonprofits regardless of size. NIST notes that the profile may be particularly valuable to smaller and less-resourced organizations because it helps prioritize efforts across governance, identification, protection, detection, response, and recovery. Although ransomware is only one threat category, the profile demonstrates how maturity can be structured around mission continuity rather than prevention alone.

3.2 Limited Resources, Human Factors, and Implementation Gaps

Cybersecurity maturity is frequently limited not by lack of awareness but by difficulties converting awareness into routine organizational practice. Luor and Wang's 2026 exploratory cross-sector study found a persistent gap between perceived importance and actual implementation across cybersecurity measures, highlighting the broader governance problem of translating security awareness into organizational behavior. Although their study was not nonprofit-specific and used a limited sample, its implementation-gap finding is highly relevant to small organizations where staffing, funding, and role ambiguity can prevent recognized risks from becoming sustained controls.

Nonprofits face additional workforce characteristics that make the human dimension especially significant. Employees may perform multiple roles, volunteers may receive temporary access, leadership turnover can alter security priorities, and technology administration may be delegated informally. These characteristics increase the value of simple and repeatable practices: documented account ownership, rapid offboarding, minimum-access principles, secure password management, multifactor authentication, role-specific awareness, and clear escalation channels.

Recent work specifically addressing NGO cybersecurity awareness also reflects the importance of accessible training formats. Borissova, Dimitrova, and Angelov's 2026 work on micro-learning for NGO cybersecurity awareness demonstrates continuing research interest in developing training models suited to nonprofit and nongovernmental organizational settings. Training alone cannot create maturity, but it can support maturity when connected to enforceable processes and technical safeguards.

CISA's civil-society guidance provides a practical complement to this research by focusing on organizations facing meaningful threats with constrained defense resources. This reinforces the need for maturity models that prioritize a limited number of actions with broad protective value rather than assume that every nonprofit can sustain enterprise cybersecurity programs.

3.3 Foundational Controls, External Services, and Adaptive Resilience

NIST, CISA, and CIS all support the principle that smaller organizations can begin with foundational practices and expand progressively. NIST SP 1300 is explicitly oriented toward modest cybersecurity programs. CISA's Cross-Sector Cybersecurity Performance Goals identify prioritized baseline security measures for organizations of varying sizes. CIS Implementation Group 1 describes a foundational set of safeguards intended as essential cyber hygiene.

These frameworks converge around several underlying ideas. Organizations should know which assets and accounts matter, reduce unnecessary privileges, maintain systems, strengthen authentication, prepare to restore important information, develop incident-response capability, and establish governance capable of sustaining these practices.

The June 2020 NIST ransomware profile places particular emphasis on governance integration, user education, supplier participation in response and recovery, identity management, awareness and training, availability of audit records, incident mitigation, and tested response planning. This combination is highly applicable to nonprofits because third-party suppliers often provide email, cloud storage, payment processing, donor management, website hosting, and other critical services.

External capability can also increase maturity. CISA maintains no-cost cybersecurity services and tools intended to help organizations reduce exposure, while its high-risk-community resources provide additional support pathways for organizations with limited internal defenses. A nonprofit can therefore develop mature governance even when some technical functions are obtained through external partners. The critical requirement is that responsibilities, escalation arrangements, data access, service expectations, and recovery roles remain understood.

4. Research Methodology

4.1 Research Design

The study adopts a conceptual-methodological research design supported by simulation-based maturity analysis.

No nonprofit organization was audited, no employee or volunteer survey was conducted, and no confidential cybersecurity incident dataset was used. The quantitative component is therefore not an empirical estimate of nonprofit-sector cybersecurity.

The conceptual model was derived from NIST CSF 2.0, NIST SP 1300 for smaller organizations, NIST's 2020 ransomware Community Profile, CISA Cybersecurity Performance Goals, CISA civil-society guidance, CIS Controls Implementation Group 1, and recent maturity and implementation-gap research.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

4.2 Community Nonprofit Cybersecurity Capability Framework

Ten capability domains are included because cybersecurity maturity in nonprofit organizations cannot be represented adequately through technical controls alone.

Table 1: Community Nonprofit Cybersecurity Capability Maturity Framework

Capability Domain	Foundational Requirement	Mature Practice	Resource-Sensitive Implementation
Governance and Leadership	Named responsibility for cybersecurity	Cyber risk integrated into leadership and board oversight	Assign one accountable owner even where security is not a full-time role
Asset and Data Awareness	Know critical accounts, devices, systems and information	Maintained inventories and criticality classification	Prioritize mission-critical assets before pursuing exhaustive inventories
Identity and Access	Unique accounts and stronger authentication	MFA, least privilege, lifecycle management and privileged-access controls	Begin with administrators, finance, email and donor systems
Data Protection	Backups and controlled access to sensitive information	Tested recovery, encryption where appropriate and retention governance	Protect highest-impact data first
Technology Maintenance	Basic updates and supported software	Risk-based vulnerability and configuration management	Prioritize internet-facing and critical systems
Workforce Security	Basic awareness for staff and volunteers	Role-sensitive, recurring security learning with phishing and incident reporting	Use short practical training and onboarding checklists
Third-Party Risk	Know critical suppliers	Security expectations, access review and incident responsibilities incorporated into supplier management	Focus initially on cloud, payment, donor and managed-IT vendors
Detection and Visibility	Basic security alerts	Centralized monitoring and review of significant events	Use provider alerts and managed services where internal monitoring is unrealistic

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Source: Author-developed framework synthesized from NIST CSF 2.0 guidance for smaller organizations, the 2020 NIST Ransomware Community Profile, CISA CPGs, CISA limited-resource civil-society guidance, and CIS foundational controls.

4.3 Maturity Levels and Simulation Procedure

Five maturity states were developed.

- Reactive maturity represents an organization in which cybersecurity is primarily addressed after problems occur and responsibility remains informal.
- Baseline maturity represents an organization that has introduced basic security hygiene, account controls, backups, awareness, and some asset knowledge.
- Managed maturity represents repeatable cybersecurity processes, defined ownership, stronger access control, vulnerability management, incident preparation, supplier awareness, and routine review.
- Community-Supported maturity represents an organization that combines mature internal governance with trusted external capability such as managed security, nonprofit cyber-support networks, cybersecurity clinics, sector partners, or public services.
- Adaptive maturity represents an organization that continuously reviews risk, validates controls, exercises response and recovery, monitors important systems, and updates security practices as technology, mission priorities, and threats change.

A conceptual Community Nonprofit Cybersecurity Maturity Index (CNCMI) is proposed:

$$CNCMI=0.15G+0.10A+0.15I+0.10D+0.10T+0.10W+0.08S+0.07V+0.08R+0.07C$$

where:

G = governance A = asset awareness I = identity and access security D = data protection T = technology maintenance W = workforce capability S = supplier governance V = visibility and detection R = response readiness C = continuity and recovery

The weights are an author-developed simulation instrument and are not official NIST, CISA, or CIS weights.

5. Analysis

5.1 Simulated Capability Maturity Progression

Fifty simulated nonprofit workflows were distributed across the five maturity conditions to illustrate how capability scores might shift as governance and operational discipline become more mature.

Table 2: Simulated Cybersecurity Capability by Nonprofit Maturity Model

Maturity Model	Simulated Mean	Median	Minimum	Maximum	Dominant Capability Characteristic
Reactive	35.7	36.0	24	46	Security depends primarily on individual initiative and post-incident action
Baseline	52.3	53.0	42	61	Essential cyber hygiene and

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Maturity Model	Simulated Mean	Median	Minimum	Maximum	Dominant Capability Characteristic
					minimum governance have been established
Managed	68.7	69.0	58	78	Repeatable processes, risk ownership and incident preparation are present
Community-Supported	80.6	81.0	70	90	Internal governance is amplified by shared or externally supplied specialist capability
Adaptive	90.0	90.5	81	97	Continuous monitoring, exercising, learning and risk-sensitive adjustment are institutionalized

Note: All values are synthetic analytical data and do not represent actual nonprofit organizations.

The progression shows that substantial improvement can occur between the Reactive and Baseline conditions without assuming advanced technology. The simulated increase reflects elementary but consequential improvements: named accountability, MFA for important accounts, tested backups, access removal for departing personnel, awareness training, software updates, critical-system inventories, and an incident contact process.

Moving from Baseline to Managed maturity requires greater repeatability. Security becomes less dependent on an individual technically capable employee and more dependent on institutional processes that survive staff turnover.

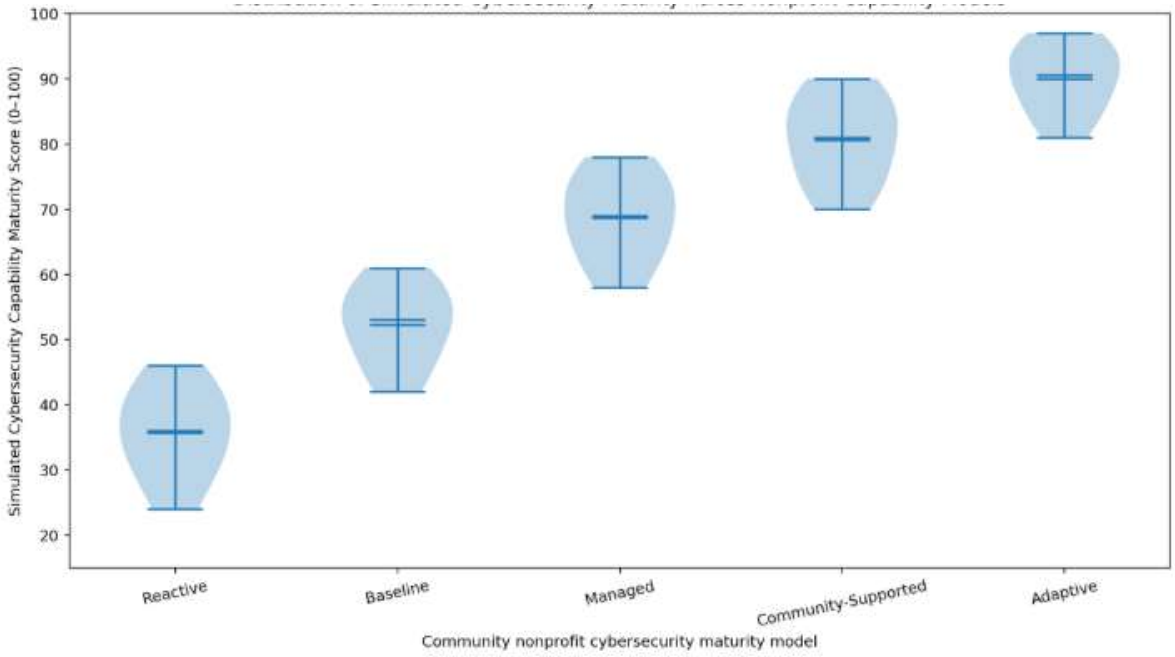
The Community-Supported condition produces another significant increase because small nonprofits may acquire expertise that would be economically inefficient to reproduce internally. This maturity state is consistent with the availability of external and no-cost cybersecurity resources for smaller and high-risk organizations.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.2 Violin-Plot Analysis of Maturity Distributions

Graph 1: Distribution of Simulated Cybersecurity Capability Maturity Across Community Nonprofit Models



Source: Author-generated simulation.

The violin plot demonstrates both increasing central maturity and changing performance distribution. Reactive organizations cluster within comparatively low capability ranges and display substantial vulnerability to gaps in governance, recovery, monitoring, or access management.

The Baseline distribution shifts upward but still contains material variation. This reflects the conceptual possibility that organizations may implement some controls strongly while leaving other areas informal.

Managed organizations occupy a stronger range because security practices become repeatable rather than episodic. Community-Supported organizations move higher because external capability helps address areas—such as specialized monitoring, incident response, vulnerability assessment, or policy advice—that may otherwise remain inaccessible.

The Adaptive model has the highest simulated distribution because cybersecurity becomes a continuous management process rather than a set of completed projects.

5.3 Priority Pathway for Resource-Constrained Nonprofits

The analysis suggests that the first maturity objective should be mission preservation rather than technical completeness. A nonprofit should identify which accounts, datasets, applications, and digital services would most seriously affect beneficiaries, staff, finances, legal obligations, or service delivery if compromised.

The next priority should be protection against common and high-impact failure pathways. CISA's prioritized Performance Goals emphasize foundational measures, while NIST's current ransomware guidance highlights identity management, workforce education, supplier coordination, monitoring, tested response planning, and recovery.

Nonprofits should therefore treat MFA, backups, access control, supported and patched technology, strong account administration, basic logging, and incident escalation as organizational capabilities rather than isolated IT settings.

Maturity should then extend to third-party dependency management. Many nonprofits rely extensively on external platforms precisely because cloud and managed services reduce internal infrastructure requirements. This creates efficiency but also makes supplier access, data handling, authentication, incident notification, and recovery dependencies part of the nonprofit's own cybersecurity posture. NIST's ransomware Community Profile specifically includes suppliers and third parties within incident planning, response, and recovery considerations.

6. Discussion

6.1 Cybersecurity Maturity Should Be Measured by Dependability, Not Technology Spending

The findings indicate that cybersecurity maturity in community nonprofits should not be inferred from security budgets, staff size, or the number of products installed. A nonprofit can purchase several security tools while remaining immature if nobody reviews alerts, privileged accounts are unmanaged, backups are untested, volunteers retain access after leaving, or incident responsibility is unclear. Conversely, a small nonprofit can establish meaningful maturity through a comparatively modest set of carefully governed controls. NIST's small-organization guidance supports this logic by providing an accessible pathway for organizations with modest cybersecurity programs, while CIS Implementation Group 1 explicitly frames foundational controls as essential cyber hygiene rather than as an enterprise-only security program.

Dependability is a stronger maturity concept because it asks whether security processes function consistently when personnel change, systems fail, or an incident occurs. An organization is more mature when account removal happens reliably every time a staff member or volunteer departs, not merely when someone remembers to do it. It is more mature when restoration from backup has been tested rather than when a backup product reports that files were copied successfully. It is more mature when leadership understands which digital services are mission-critical and knows who can authorize emergency decisions than when cybersecurity remains solely an informal responsibility of a technically knowledgeable employee.

This understanding also makes maturity measurable. Nonprofits can examine evidence such as percentage of critical accounts protected with MFA, age of unresolved critical patches, backup restoration success, time required to remove departed-user access, staff completion of practical security learning, availability of incident contacts, or number of important suppliers with defined breach-notification responsibilities. These indicators do not require sophisticated security operations, but they create evidence that security controls are functioning.

6.2 Community-Supported Cybersecurity Can Convert Resource Scarcity into Shared Capability

The simulated advantage of the Community-Supported maturity condition reflects an important organizational principle: cybersecurity maturity does not require every capability to be owned internally. Community-based nonprofits routinely collaborate in fundraising, service delivery, legal support, training, public policy, and program networks. Cybersecurity can use the same cooperative logic. CISA currently provides cybersecurity resources for high-risk communities and maintains collections of no-cost tools and services, while NIST's smaller-organization resources are specifically designed to make cybersecurity risk management more accessible to organizations with limited capability.

A mature nonprofit should therefore know when external capability is preferable to weak internal imitation. Continuous security monitoring may be more realistic through a managed provider. Vulnerability assessment may be obtained periodically from a cybersecurity clinic or specialized partner. Legal interpretation after a data breach may require external counsel. Highly technical incident investigation may require an external response firm. Such dependence is not itself immaturity. Immaturity occurs when the organization does not know who the provider is, what the provider can access, how an emergency is escalated, whether backups are included, or what will happen when the provider is unavailable.

Community-supported maturity thus requires governed interdependence. External expertise should amplify local capability without obscuring accountability. The nonprofit's leadership remains responsible for defining which services are critical, which risks are acceptable, which information requires protection, and how the organization's mission should continue during disruption. This combination of internal governance and external specialization is likely to be more sustainable for small nonprofits than attempting to reproduce the security structure of large corporations.

6.3 Adaptive Maturity Requires Continuous Learning and Recovery Readiness

The final maturity stage is defined less by technology than by organizational learning. Cybersecurity practices become obsolete when software changes, employees leave, new cloud systems are introduced, suppliers change, fundraising platforms are replaced, or attackers adopt new methods. The 2026 NIST ransomware profile emphasizes preparation, tested plans, role clarity, supplier involvement, awareness, monitoring, incident mitigation, and recovery as ongoing risk-management activities rather than one-time actions. Recent maturity research similarly conceptualizes cybersecurity improvement as a continuous journey in which organizations assess present and target states and identify prioritized improvements.

For nonprofits, adaptive maturity should remain proportionate. Continuous improvement does not necessarily require a sophisticated security operations center. It can mean reviewing cybersecurity after major technology changes, testing recovery annually or after significant system migration, examining incidents and near misses, updating account inventories, confirming emergency contacts, reviewing supplier access, and reassessing which data are genuinely necessary to retain. These practices make cybersecurity responsive to the organization's evolving mission.

The strongest maturity model therefore treats cyber incidents as organizational learning opportunities. A phishing incident should prompt analysis of authentication, awareness, reporting, and email protections rather than simply blame the employee who clicked. A failed backup restoration

should lead to revised recovery testing rather than installation of another product without understanding the failure. A supplier incident should trigger review of third-party governance and contingency arrangements. This learning orientation is what transforms cybersecurity from reactive defense into institutional resilience.

7. Conclusion

Community-based nonprofit organizations depend increasingly on digital infrastructure to sustain their missions, yet many cannot support the personnel, budgets, or specialized cybersecurity functions associated with large enterprises. This disparity makes conventional maturity models difficult to apply without adaptation. The present study responds by framing maturity around dependable organizational capabilities rather than technology accumulation. Governance, identity security, data protection, technology maintenance, workforce behavior, third-party management, detection, response, and recovery collectively determine whether a nonprofit can manage cyber risk without undermining its mission.

The proposed Community Nonprofit Cybersecurity Capability Maturity Model organizes improvement across Reactive, Baseline, Managed, Community-Supported, and Adaptive states. The simulated analysis shows an illustrative increase in mean maturity from 35.7 in the Reactive condition to 90.0 in the Adaptive condition. These values are not empirical observations, but the progression demonstrates a practical principle: substantial maturity can be achieved incrementally. A nonprofit does not need to become technologically sophisticated before it can become more secure. Clear accountability, MFA, reliable backups, appropriate access removal, basic asset awareness, supported software, workforce education, incident contacts, and recovery planning can create meaningful early gains.

The Community-Supported stage is particularly important because it recognizes that organizational maturity and organizational self-sufficiency are different concepts. Small nonprofits can combine internal governance with managed providers, cybersecurity clinics, public resources, sector networks, and specialized technical partners. Current NIST guidance explicitly extends small-organization cybersecurity resources to nonprofits, while CISA provides resources for organizations operating with limited defenses and maintains no-cost cybersecurity resource collections. The challenge is therefore not to eliminate dependency but to govern it transparently.

The central conclusion is that cybersecurity capability maturity in community-based nonprofits should be judged by whether the organization can protect its mission, recognize significant risk, respond when preventive controls fail, restore trusted operations, and improve from experience. Future empirical research should validate the proposed framework using nonprofit-sector surveys, maturity assessments, incident histories, board and executive interviews, and longitudinal evaluations of capability improvement. Particular attention should be given to small organizations serving vulnerable communities, because cybersecurity failure in such settings can affect people who depend on nonprofit services and may have limited alternatives. A mature nonprofit cybersecurity program should ultimately protect not only information systems but the continuity, dignity, and trust embedded in the organization's community mission.

References

1. Ozkan, B. Y., van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) model. *Journal of Cybersecurity and Privacy, 1*(1), 119–139. https://doi.org/10.3390/jcp1010007
2. Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal, 22*(2), 201–215. https://doi.org/10.1016/j.eij.2020.08.001
3. Garba, A. A., Siraj, M. M., & Othman, S. H. (2020). An explanatory review on cybersecurity capability maturity models. *Advances in Science, Technology and Engineering Systems Journal, 5*(4), 762–769.
4. Garba, A. A., Bade, A. M., Yahuza, M., & Nuhu, Y. (2020). Cybersecurity capability maturity models review and application domain. *International Journal of Engineering & Technology, 9*(3), 779–784. https://doi.org/10.14419/ijet.v9i3.30719
5. Mohammed, I., & Bade, A. M. (2019). Cybersecurity capability maturity model for network system. *International Journal of Development Research, 9*, 28858–28862.
6. Brown, R. D. (2019). Towards a Qatar Cybersecurity Capability Maturity Model with a legislative framework. *International Review of Law, 2018*(3), 1–19. https://doi.org/10.29117/irl.2018.0036
7. NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018
8. National Institute of Standards and Technology. (2018). *Cybersecurity Framework: Small Business Resources*. U.S. Department of Commerce. The NIST framework was explicitly designed to be adaptable to smaller organizations with limited IT resources.
9. National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5)*. U.S. Department of Commerce.
10. National Institute of Standards and Technology. (2020). *Developing Cybersecurity and Privacy Learning Programs (NIST SP 800-50)*. U.S. Department of Commerce.
11. Center for Internet Security. (2021). *CIS Controls Version 8*. Center for Internet Security.
12. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Technology—Security Techniques—Information Security Management Systems—Requirements*. ISO.
13. ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. ISACA.
14. U.S. Department of Energy. (2014). *Cybersecurity Capability Maturity Model (C2M2), Version 1.1*. U.S. Department of Energy.
15. Carnegie Mellon University Software Engineering Institute. (2016). *Cyber Resilience Review (CRR): Self-Assessment Package*. Software Engineering Institute.
16. National Cyber Security Centre. (2020). *Small Charities Guide to Cyber Security*. UK National Cyber Security Centre.
17. NTEN. (2018). *2018 State of Nonprofit Cybersecurity Report*. Nonprofit Technology Enterprise Network. The report examined nonprofit security practices, policies, staff training, technology protection, and operational vulnerabilities.

18. Community IT Innovators. (2020). *2020 Nonprofit Cybersecurity Incident Report*. Community IT Innovators. The report highlights nonprofit-specific issues including security-awareness training, business-email compromise, MFA adoption, and resource constraints.
19. Tech Impact. (2021). *Practical Security: What Nonprofits Need to Know*. Tech Impact. The guidance emphasizes organizational security awareness and the importance of building cybersecurity practices among nonprofit personnel.
20. Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM): 2021 Edition*. University of Oxford. The 2021 model includes civil-society cybersecurity awareness, coordination, information sharing, and capacity-building dimensions relevant to community-based organizations.