International Journal of Scientific and Management Research
Volume 8 Issue 12 (December) 2025
ISSN: 2581-6888
Page: 372-391

Crowdsourcing Cyber Resilience: A Community-Based Approach to Threat Chronicles and Zero-Day Defense

Arafat Bikadho, Tendai Nemure, Ruvimbo Mashinge, & Mazvita Madziyanike
Department of Cybersecurity, Yeshiva University**,** New York, **USA**
Department of Cybersecurity, Yeshiva University**,** New York, **USA**
Department of Cybersecurity, Yeshiva University**,** New York, **USA**
Department of Cybersecurity, Yeshiva University**,** New York, **USA**
DOI - http://doi.org/10.37502/IJSMR.2025.81217

Abstract

The accelerating complexity of cyber threats has exposed the limitations of traditional, prevention-centric security models and underscored the need for adaptive, system-wide cyber resilience. This article examines how crowdsourcing can serve as a transformative mechanism for strengthening cyber resilience through enhanced threat chronicles and more agile Zero-Day defense. Drawing on resilience theory, collective intelligence research, and contemporary cybersecurity scholarship, the study develops a conceptual framework that integrates community-driven collaboration into core defensive processes. Through qualitative analysis and detailed case studies - including SolarWinds, WannaCry, and Log4j - the article demonstrates that while threat chronicles and Zero-Day defense are essential components of resilience, their current implementation remains constrained by centralized governance, limited participation, and fragmented information flows. The findings reveal that crowdsourcing offers significant potential to diversify threat intelligence sources, accelerate vulnerability discovery, and improve adaptive capacity. However, realizing this potential requires structured governance models, validation mechanisms, and cultural shifts toward shared responsibility. The article concludes by proposing a set of recommendations for operationalizing community-based cyber resilience and outlines directions for future empirical research**.**

Keywords: Cyber resilience; crowdsourcing; threat chronicles; Zero-Day vulnerabilities; Zero-Day defense; collective intelligence; cybersecurity governance; community-based security; threat intelligence; digital ecosystems.

1. Introduction

The rapid escalation of cyber threats has created profound challenges for organizations, governments, and individuals in today's interconnected world. Cyberattacks are not only becoming more frequent but also more sophisticated, targeting critical infrastructures, financial systems, and personal data with increasing precision. IBM's Cost of a Data Breach Report (2024) reveals that the average global cost of a breach has risen to USD 4.88 million, while the United States continues to bear the highest average at USD 9.48 million per incident. In the same year, more than 6.8 billion records were exposed across 2,741 publicly disclosed incidents in the U.S., underscoring the scale of economic and reputational damage associated with cyber incidents and the urgent need for more resilient defense strategies.

Among the most pressing concerns are zero-day vulnerabilities - software flaws unknown to vendors or defenders at the time of exploitation. These vulnerabilities allow attackers to bypass conventional defenses, often leading to severe breaches before patches are available. Google's Threat Analysis Group reported that 75 zero-day vulnerabilities were exploited in the wild in 2024, a figure that, while lower than the 98 recorded in 2023, remains significantly higher than the 63 documented in 2022. The underground market for zero-day exploits has also expanded, with prices ranging from USD 50,000 to over USD 1 million, depending on the target system (Krishnan, 2024). The Cybersecurity and Infrastructure Security Agency (CISA, 2024) warns that zero-days represent the most dangerous category of vulnerabilities because of their unpredictability and potential to disrupt entire systems.

Traditional defense mechanisms-centralized monitoring, vendor-driven updates, and hierarchical reporting structures-have proven insufficient against these evolving threats. While such approaches provide a baseline of protection, they often lack the agility required to respond to rapidly changing attack vectors. Centralized systems are hindered by bottlenecks in information flow, delayed patch cycles, and dependence on vendor disclosure. This reactive posture leaves organizations vulnerable during the critical window between exploit discovery and patch deployment. The SolarWinds supply chain attack (2020), which compromised over 18,000 organizations, and the Microsoft Exchange zero-day incident (2021), which affected tens of thousands of servers globally, illustrate how delayed detection and response can have cascading effects across entire ecosystems.

In light of these challenges, scholars and practitioners have advanced the concept of cyber resilience, defined as the ability to anticipate, withstand, recover from, and adapt to adverse cyber events (Joinson et al., 2023). Unlike traditional cybersecurity, which focuses primarily on prevention, resilience emphasizes continuity, adaptability, and systemic robustness. Mitchelson (2024) argues that resilience is not only a technological construct but also a socio-organizational capability, requiring integration of governance, culture, and human behavior. This perspective aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which emphasizes resilience through risk management, incident response, and recovery planning (NIST, 2023).

One promising approach to operationalizing resilience is crowdsourcing, which mobilizes distributed communities to contribute knowledge, vigilance, and resources. In cybersecurity, crowdsourcing takes several forms: bug bounty programs that incentivize independent researchers to discover and report vulnerabilities; open-source intelligence platforms (OSINT) such as MISP and AlienVault OTX, which aggregate indicators of compromise from diverse contributors; and community-driven threat reporting, where users share suspicious activity, attack patterns, and vulnerability reports in decentralized repositories. By harnessing the collective vigilance of diverse participants, organizations can create decentralized threat chronicles-community-driven repositories of suspicious activity and attack narratives. These chronicles enhance visibility, reduce detection latency, and foster a culture of shared responsibility.

The urgency of crowdsourced resilience is underscored by industry telemetry. CrowdStrike (2024) reports that adversary breakout times-the interval between initial compromise and lateral movement-have shrunk to less than 10 minutes in many cases. Bug bounty programs further demonstrate the effectiveness of community-driven defense: Meta's bug bounty program awarded USD 2.3 million in 2024, bringing its cumulative payouts to over USD 20 million since 2011. The global bug bounty market is projected to grow from USD 1.76 billion in 2024 to over USD 4 billion by 2030, reflecting the increasing reliance on crowdsourced vulnerability discovery. These figures highlight the growing recognition that no single organization can detect and respond to threats at sufficient speed without external collaboration.

Conceptually, crowdsourcing aligns with theories of collective intelligence (Malone, Laubacher, & Dellarocas, 2010), which suggest that distributed groups can outperform centralized teams in complex problem-solving tasks. Applied to cybersecurity, collective intelligence implies that diverse communities-comprising professionals, hobbyists, and end-users-can collectively identify anomalies and vulnerabilities faster than isolated institutional teams. This participatory model also resonates with Routine Activity Theory, which emphasizes the convergence of motivated offenders, suitable targets, and the absence of capable guardians. Crowdsourcing effectively expands the pool of "*guardians*," increasing the likelihood of detecting and deterring cyber offenders. Similarly, Deterrence Theory underscores that certainty and swiftness of punishment are critical to discouraging crime; crowdsourced intelligence enhances the certainty of detection, thereby strengthening deterrence. From a systemic perspective, Systems Theory highlights that cyber resilience is a product of interactions across technology, law, economy, and culture. Crowdsourcing embodies this systemic approach by integrating diverse actors into a shared defense ecosystem.

The strategic role of crowdsourcing in zero-day defense is particularly significant. Zero-day exploits thrive in opacity, exploiting the gap between discovery and disclosure. By aggregating suspicious activity across diverse environments, crowdsourcing can bridge this gap, enabling faster identification of anomalies and reducing the window of exposure. Empirical studies show that bug bounty programs have uncovered thousands of critical vulnerabilities, many of which could have been exploited as zero-days (Shah & Kumar, 2021). Similarly, OSINT platforms have facilitated early detection of coordinated campaigns, providing defenders with actionable intelligence before vendor disclosures.

This paper explores a community-based approach to cyber resilience, emphasizing crowdsourcing as a strategic enabler of threat detection, documentation, and zero-day defense. Drawing on interdisciplinary insights from cybersecurity, organizational behavior, and risk management, it proposes a participatory framework for compiling threat chronicles and enhancing early warning systems. Case studies and simulations demonstrate that community-driven models not only strengthen technical defenses but also cultivate proactive engagement, trust, and shared responsibility. The paper concludes with recommendations for integrating crowdsourced resilience into enterprise strategies, highlighting governance, trust-building, and ethical data sharing as critical enablers.

2. Literature Review

Cyber resilience has become a foundational concept in contemporary cybersecurity research, reflecting a shift from traditional prevention-oriented security models toward adaptive, recovery-focused approaches. Scholars generally define cyber resilience as the ability of an organization or digital ecosystem to anticipate, withstand, recover from, and adapt to cyber disruptions (Linkov et al., 2018). This definition emphasizes continuity and adaptability rather than the unrealistic expectation of perfect protection. The National Institute of Standards and Technology (NIST) similarly frames cyber resilience as the capacity to maintain essential functions despite adverse cyber events (Stouffer et al., 2021). The urgency of resilience is underscored by global statistics: the World Economic Forum (2022) reports that 80% of organizations experienced at least one significant cyber incident in the past year, yet fewer than half expressed confidence in their ability to recover quickly. This gap between exposure and preparedness highlights the limitations of traditional cybersecurity and reinforces the need for resilience-based strategies. Academic literature positions cyber resilience as a multidimensional construct involving technological robustness, organizational preparedness, human expertise, and continuous learning (Araujo et al., 2024; Tzavara &

Vassiliadis, 2024). As digital infrastructures become increasingly interconnected, the consequences of cyber disruptions-ranging from supply-chain failures to critical infrastructure outages-have amplified the importance of embedding resilience into organizational and national cybersecurity frameworks.

Table 1. A comparison of widely cited definitions of cyber resilience across academic and institutional literature.

SOURCES	DEFINITIONAL SUMMARY	EMPHASIS
NIST (2021)	Ability to maintain essential functions despite cyber disruptions.	Continuity, critical functions
Linker et. al (2018)	Capacity to anticipate, absorb, recover and adapt.	Adaptive cycle
World Economic Forum (2022)	Organizational preparedness and recovery capability.	Global risk context
Araujo et. al (2024)	Socio-technical resilience across digital ecosystems.	Interconnected systems
Tzavara & Vassiliadis (2024)	Evolutionary resilience in dynamic threat environments.	Continuous improvement

Within this broader discourse, threat chronicles have emerged as a critical mechanism for strengthening cyber resilience. Threat chronicles refer to structured, narrative-driven accounts of cyber incidents, including details about attack vectors, adversary behavior, exploited vulnerabilities, and lessons learned. They function as a collective memory for the cybersecurity community, enabling practitioners to understand evolving threat patterns and anticipate similar attacks. The MITRE ATT&CK framework exemplifies this approach by compiling detailed chronicles of adversarial tactics and techniques based on real intrusions, providing defenders with a shared taxonomy for understanding attacker behavior (Strom et al., 2018). Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) publishes advisories that chronicle significant incidents, such as the SolarWinds supply-chain compromise, offering insights into attacker movement and recommended mitigations (CISA, 2020). These chronicles have demonstrably improved situational awareness and informed defensive strategies across sectors. Research indicates that organizations that actively engage with shared threat chronicles demonstrate faster detection times and more effective incident response, benefiting from the collective experiences of others (Kostyuk & Wayne, 2021). However, despite their utility, threat chronicles often remain siloed within specific industries or government bodies, limiting their potential as a fully community-driven resilience tool.

Zero-Day vulnerabilities represent another critical dimension of cyber resilience. A Zero-Day vulnerability is a previously unknown software flaw that attackers exploit before developers have had the opportunity to create a patch. Because these vulnerabilities are undisclosed and unpatched at the time of exploitation, they pose significant challenges to traditional security mechanisms. Zero-Day defense, therefore, involves strategies and technologies designed to detect and mitigate attacks that exploit unknown vulnerabilities. These defenses often rely on behavioral analytics, anomaly detection, heuristic-based monitoring, and rapid threat intelligence sharing. The importance of Zero-Day defense in cyber resilience is evident in high-profile incidents. The 2017 WannaCry ransomware attack exploited a Zero-Day-derived exploit known as EternalBlue, affecting more than 200,000 systems across 150 countries within days (Europol, 2018). Similarly, the 2021 Log4j vulnerability (Log4Shell) demonstrated how quickly a Zero-Day flaw can escalate into a global crisis, prompting an unprecedented collaborative response from researchers, vendors, and governments (Apache Software Foundation, 2021). These incidents highlight that resilience in the face of Zero-Day threats depends not only on technical controls but also on rapid information exchange, coordinated mitigation efforts, and the ability to adapt defenses in real time. Academic studies emphasize that Zero-Day defense is most effective when supported by diverse sources of intelligence and collaborative analysis (Bilge & Dumitras, 2012).

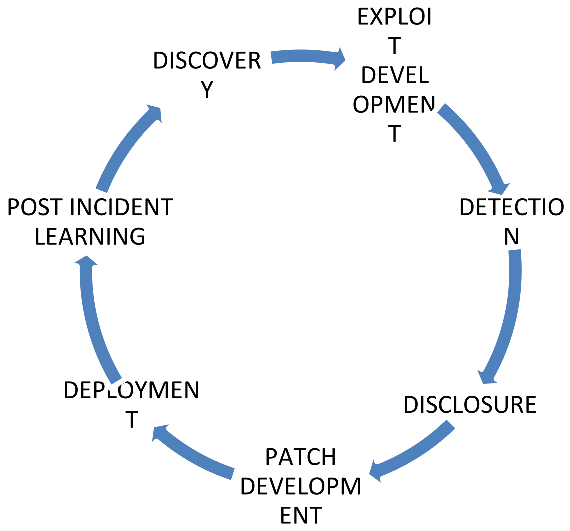

Figure 1. A flowchart illustrating the stages of Zero-Day discovery, exploitation, detection, disclosure and mitigation.

Recent research has increasingly explored the intersection between crowdsourcing and cyber resilience, recognizing the potential of collective intelligence to enhance detection, analysis, and response capabilities. Crowdsourcing in cybersecurity involves leveraging contributions from diverse participants-security researchers, ethical hackers, open-source communities, and even everyday users-to identify vulnerabilities, analyze threats, and develop defensive tools. Bug bounty platforms such as HackerOne and Bugcrowd illustrate how crowdsourcing can uncover vulnerabilities at scale, often identifying flaws that internal teams overlook (Finifter et al., 2013). Open-source security projects, including Snort, Suricata, and OSSEC, demonstrate how distributed communities can collaboratively maintain and improve defensive technologies. Platforms like VirusTotal further illustrate the power of crowdsourced malware analysis, where samples submitted by users contribute to collective detection capabilities and enable faster identification of emerging threats (VirusTotal, 2022). Scholars argue that crowdsourcing aligns naturally with resilience principles, as it distributes detection capabilities, enhances redundancy, and fosters continuous learning across the cybersecurity ecosystem (Zhang et al., 2020). Crowdsourced intelligence has been shown to accelerate vulnerability discovery, enrich threat intelligence, and democratize access to security expertise.

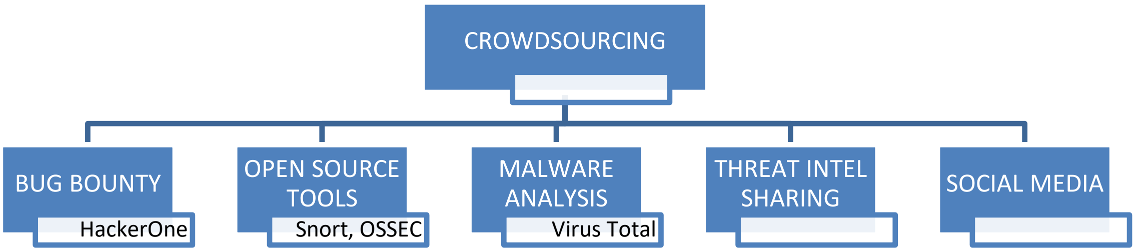

Figure 2. An overview of the major forms of crowdsourcing used in cybersecurity and their contributions to resilience.

Despite these advances, a notable gap persists in the integration of community-based approaches within both threat chronicles and Zero-Day defense. While threat chronicles exist, many remain curated by centralized institutions, limiting the diversity of perspectives and slowing the dissemination of critical insights. Community contributions are often informal, fragmented across forums, mailing lists, and social media, rather than systematically integrated into formal chronicles. Similarly, Zero-Day defense efforts frequently rely on specialized research teams or private vendors, with limited mechanisms for broad community participation. Although collaborative responses to incidents like Log4j demonstrate the potential of community involvement, such collaboration tends to emerge spontaneously rather than being embedded into structured defense frameworks. The literature indicates that a more deliberate, community-centric approach could significantly enhance both the speed and effectiveness of threat analysis and Zero-Day mitigation. Governance challenges, trust issues, and concerns about data quality have hindered the development of such models, leaving a gap that this study seeks to address.

3. Methodology

This study adopts a qualitative, conceptual research design aimed at examining how crowdsourcing can enhance cyber resilience through improved threat chronicles and Zero-Day defense. A conceptual methodology is appropriate because the research seeks to synthesize existing theories, empirical findings, and real-world practices into a unified explanatory model rather than test a specific hypothesis through empirical measurement. Conceptual research is widely used in cybersecurity scholarship when exploring emerging paradigms, integrating fragmented knowledge domains, or proposing new frameworks for understanding complex socio-technical phenomena (Bada & Nurse, 2019). Given the interdisciplinary nature of cyber resilience-which spans computer science, organizational studies, behavioral science, and information systems-a conceptual approach enables a holistic analysis that would be difficult to achieve through a single empirical method.

The methodology is grounded in an extensive review of peer-reviewed academic literature, institutional reports, and documented cyber incidents. Sources were selected based on their relevance, scholarly credibility, and contribution to the domains of cyber resilience, threat intelligence, Zero-Day vulnerabilities, and crowdsourcing. Academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar were consulted to identify foundational and contemporary works. Key authors in resilience theory (e.g., Linkov, Kott, Boin), cybersecurity (e.g., Schneier, Bilge, Dumitras), and collective intelligence (e.g., Malone, Woolley) were prioritized to ensure theoretical depth. Institutional publications from

NIST, CISA, ENISA, and the World Economic Forum were included to capture policy-level perspectives and industry trends. This triangulation of academic and institutional sources strengthens the validity of the conceptual synthesis.

The analysis also incorporates real-world case studies to illustrate how threat chronicles, Zero-Day defense, and crowdsourcing operate in practice. Case studies are a well-established methodological tool in cybersecurity research because they provide rich, contextualized insights into complex incidents that cannot be fully captured through quantitative metrics alone (Kostyuk & Wayne, 2021). Incidents such as the SolarWinds supply-chain compromise, the WannaCry ransomware outbreak, and the Log4j Zero-Day vulnerability were selected due to their global impact, extensive documentation, and relevance to the study's core constructs. These cases provide empirical grounding for the conceptual framework and demonstrate the practical implications of community-based collaboration.

The methodological process involved three analytical stages. The first stage consisted of thematic analysis of the literature to identify recurring concepts, gaps, and relationships among cyber resilience, threat chronicles, Zero-Day defense, and crowdsourcing. Thematic analysis is widely used in qualitative cybersecurity research to extract patterns from diverse sources and synthesize them into coherent themes (Braun & Clarke, 2006). The second stage involved comparative analysis of existing models of threat intelligence sharing and Zero-Day mitigation to evaluate their strengths and limitations. This comparison highlighted the structural gaps in current approaches, particularly the limited integration of community participation. The third stage involved constructing the conceptual framework by mapping the identified themes and relationships into a structured model that explains how crowdsourcing can enhance resilience.

Ethical considerations were also incorporated into the methodological design. Although the study does not involve human subjects or sensitive data, it engages with cybersecurity incidents that may have legal, political, or organizational implications. To ensure ethical integrity, all case studies were drawn from publicly available sources, and no confidential or proprietary information was used. The analysis avoids attributing blame to specific organizations or individuals, focusing instead on systemic lessons and structural insights. This approach aligns with ethical guidelines for cybersecurity research, which emphasize responsible reporting, avoidance of harm, and respect for organizational confidentiality (Dittrich & Kenneally, 2012).

The limitations of the methodology are acknowledged. As a conceptual study, the findings are interpretive rather than empirically tested. While the framework is grounded in extensive literature and real-world cases, its practical applicability would benefit from future empirical validation through surveys, interviews, or experimental studies. Additionally, the rapidly evolving nature of cybersecurity means that new threats, technologies, and collaborative models may emerge that challenge or refine the proposed framework. Nonetheless, the conceptual methodology provides a rigorous foundation for understanding the potential of crowdsourcing in cyber resilience and offers a structured basis for future empirical research.

In summary, the methodology integrates literature synthesis, case study analysis, and conceptual modeling to explore how community-based collaboration can strengthen cyber resilience. This approach enables a comprehensive examination of the intersections among threat chronicles, Zero-Day defense, and crowdsourcing, while also identifying structural gaps in current practices. The next section applies this methodology by presenting case studies that illustrate the practical relevance of the conceptual framework.

4. Conceptual Framework

The conceptual framework for this study integrates four interrelated constructs-cyber resilience, threat chronicles, Zero-Day defense, and crowdsourcing-into a unified model that explains how community-driven collaboration can strengthen organizational and systemic resilience. This framework is grounded in resilience theory, collective intelligence theory, and contemporary cybersecurity research. It positions cyber resilience as the overarching objective, threat chronicles and Zero-Day defense as critical operational components, and crowdsourcing as the enabling mechanism that enhances the speed, diversity, and effectiveness of defensive actions. The framework also highlights the structural gaps in existing approaches, particularly the limited integration of community participation in formal threat-sharing and Zero-Day mitigation processes.

Cyber resilience serves as the central pillar of the framework. It is conceptualized not merely as a technical capability but as a socio-technical system that encompasses organizational processes, human expertise, technological infrastructure, and adaptive learning (Linkov et al., 2018; Stouffer et al., 2021). The framework adopts the view that resilience is achieved through four core functions: anticipation, absorption, recovery, and adaptation. Anticipation involves identifying emerging risks before they materialize; absorption refers to the ability to withstand disruptions; recovery focuses on restoring essential functions; and adaptation involves learning from incidents to improve future performance. These functions require continuous access to timely, accurate, and diverse threat intelligence - an area where traditional, centralized models often fall short. The framework therefore positions information-sharing mechanisms, particularly threat chronicles, as essential inputs into the resilience cycle.

Threat chronicles occupy a critical role in the conceptual model as repositories of collective knowledge. They provide structured narratives of cyber incidents, detailing attacker behavior, exploited vulnerabilities, and defensive lessons. By transforming isolated events into shared learning resources, threat chronicles support both anticipation and adaptation functions of resilience. The MITRE ATT&CK framework, for example, operationalizes threat chronicles by categorizing adversarial tactics and techniques based on real-world observations (Strom et al., 2018). Similarly, CISA's advisories chronicle major incidents such as the SolarWinds compromise, offering insights that help organizations anticipate similar attack patterns (CISA, 2020). However, the framework acknowledges that existing threat chronicles are predominantly curated by centralized institutions, limiting the diversity of contributions and slowing the dissemination of insights. This limitation creates a structural gap between the potential and actual impact of threat chronicles on resilience. The conceptual model therefore identifies community participation as a missing but necessary component for enhancing the richness, timeliness, and applicability of threat chronicles.

Zero-Day vulnerabilities and their corresponding defenses form the second operational component of the framework. Zero-Day vulnerabilities represent one of the most challenging categories of cyber threats due to their unknown nature and the absence of available patches at the time of exploitation. Zero-Day defense requires rapid detection, behavioral analysis, and coordinated mitigation efforts (Bilge & Dumitras, 2012). The WannaCry and Log4j incidents illustrate how quickly Zero-Day exploits can escalate into global crises when detection and response mechanisms are insufficiently coordinated (Europol, 2018; Apache Software Foundation, 2021). Within the conceptual framework, Zero-Day defense is positioned as a dynamic process that relies heavily on early warning signals, rapid intelligence sharing, and collaborative analysis. However, as with threat chronicles, Zero-Day defense is often dominated by specialized research teams, private vendors, and government agencies, leaving limited room for broader community involvement. This creates a second structural gap: the absence of systematic mechanisms for integrating crowdsourced intelligence into Zero-Day detection and mitigation workflows.

Crowdsourcing functions as the enabling mechanism that connects and strengthens the other components of the framework. Drawing on collective intelligence theory, the framework conceptualizes crowdsourcing as a distributed problem-solving process that leverages the diverse expertise, perspectives, and observations of a large, heterogeneous community (Zhang et al., 2020). In cybersecurity, crowdsourcing manifests in various forms, including bug bounty programs, open-source security tools, collaborative malware analysis platforms, and community-driven threat intelligence sharing. These models demonstrate that distributed communities can identify vulnerabilities more quickly, analyze threats more comprehensively, and develop defensive tools more efficiently than isolated teams (Finifter et al., 2013; VirusTotal, 2022). The conceptual framework therefore positions crowdsourcing as a catalyst that enhances the speed, accuracy, and adaptability of both threat chronicles and Zero-Day defense. By integrating community contributions into formal resilience processes, organizations can benefit from a broader pool of intelligence and reduce the time between threat emergence and defensive action.

The final element of the conceptual framework is the identification of structural gaps in current cybersecurity practices. Despite the demonstrated benefits of crowdsourcing, both threat chronicles and Zero-Day defense remain largely centralized and institution-driven. Community contributions are often informal, fragmented, or excluded from formal processes due to concerns about data quality, governance, and trust. These limitations hinder the potential of collective intelligence to enhance resilience. The conceptual framework therefore argues that a community-based approach - one that systematically integrates crowdsourced insights into threat chronicles and Zero-Day defense - can address these gaps and significantly strengthen cyber resilience. This approach requires new governance models, validation mechanisms, and collaborative infrastructures that enable secure, reliable, and scalable community participation.

In summary, the conceptual framework integrates cyber resilience, threat chronicles, Zero-Day defense, and crowdsourcing into a cohesive model that highlights both the potential and the limitations of current cybersecurity practices. It demonstrates that while threat chronicles and Zero-Day defense are essential components of resilience, their effectiveness is constrained by limited community integration. Crowdsourcing offers a powerful mechanism for addressing these constraints, but its potential remains underutilized. This framework provides the theoretical foundation for examining how a community-based, crowdsourced approach can transform cyber resilience and enhance collective defense against emerging threats.

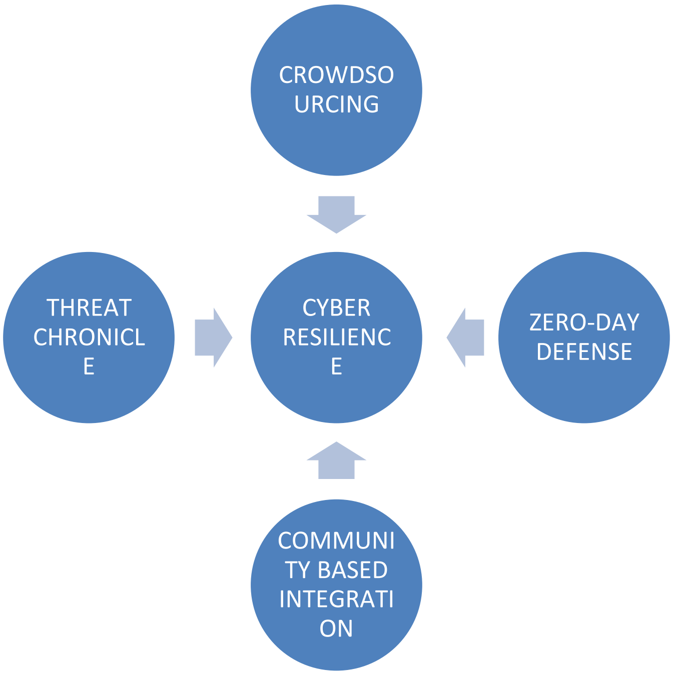

Figure 3. A visual representation of the relationships among cyber resilience, threat chronicles, Zero-Day defense and crowdsourcing, illustrating how community-based collaboration strengthens resilience functions.

5. Case Studies

The practical relevance of the conceptual framework becomes clearer when examined through real-world cyber incidents that demonstrate the interplay between threat chronicles, Zero-Day vulnerabilities, and crowdsourced intelligence. This section analyzes three major cases - SolarWinds, WannaCry, and Log4j - each illustrating different dimensions of cyber resilience and highlighting the gaps that a community-based approach could address. These cases were selected due to their global impact, extensive documentation, and relevance to the study's core constructs.

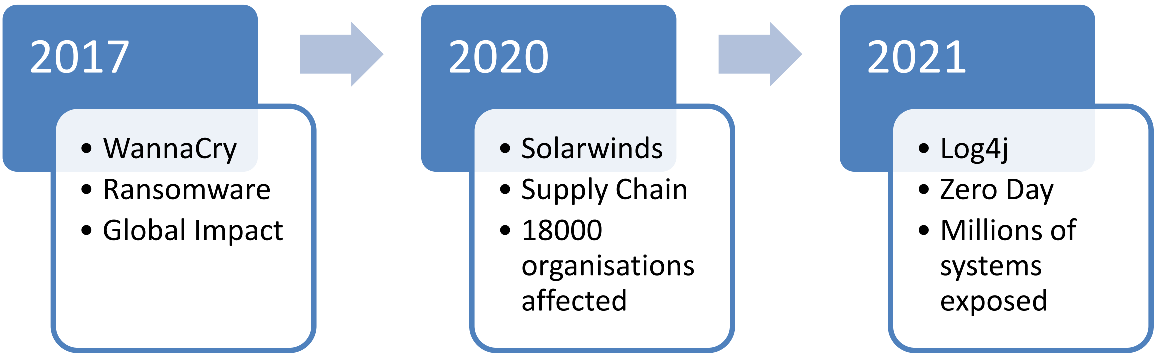

Figure 4. A Chronological overview of the SolarWinds, WannaCry and Log4j incidents, highlighting their impact and relevance to resilience.

The SolarWinds supply-chain compromise represents one of the most sophisticated cyber espionage campaigns in recent history. Discovered in late 2020, the attack involved the insertion of a malicious backdoor, known as SUNBURST, into the Orion network management software used by thousands of organizations worldwide (CISA, 2020). The attackers, believed to be a state-sponsored group, exploited the trust inherent in software supply chains, enabling them to infiltrate U.S. government agencies, critical infrastructure providers, and private corporations. The incident underscored the limitations of traditional perimeter-based defenses, as the malicious code was delivered through a legitimate software update. Threat chronicles played a crucial role in the response. CISA's detailed advisories, FireEye's technical analyses, and Microsoft's incident reports provided the global cybersecurity community with insights into attacker behavior, indicators of compromise, and recommended mitigations. These chronicles enabled organizations to detect and contain the intrusion more effectively. However, the case also revealed gaps in community participation. Much of the early analysis was conducted by a small number of private firms, and broader community involvement emerged only after the initial disclosures. A more structured, community-driven approach could have accelerated detection and reduced the window of exposure.

The WannaCry ransomware outbreak of 2017 provides a stark illustration of the destructive potential of Zero-Day-derived exploits. WannaCry leveraged EternalBlue, a vulnerability in the Windows Server Message Block (SMB) protocol that had been weaponized and leaked prior to the attack (Europol, 2018). Within hours, the ransomware spread across networks worldwide, affecting hospitals, transportation systems, telecommunications providers, and government agencies. The United Kingdom's National Health Service (NHS) was particularly hard hit, with thousands of appointments canceled and critical medical services disrupted. The incident demonstrated the catastrophic consequences of delayed patching and the challenges of defending against rapidly propagating Zero-Day exploits. It also highlighted the importance of crowdsourced intelligence. Security researchers across the globe collaborated informally through social media, technical forums, and open-source platforms to analyze the malware, develop detection signatures, and share mitigation strategies. The discovery of a "*kill switch*" domain by a security researcher significantly slowed the spread of the ransomware. Although this collaboration was largely spontaneous, it illustrated the potential of community-driven responses in Zero-Day defense. A more formalized crowdsourcing mechanism could have facilitated faster coordination and broader dissemination of defensive measures.

The Log4j vulnerability (Log4Shell), disclosed in December 2021, represents one of the most significant Zero-Day vulnerabilities ever recorded due to its ubiquity and ease of exploitation. Log4j, a widely used Java logging library, contained a flaw that allowed attackers to execute arbitrary code remotely by manipulating logged input strings (Apache Software Foundation, 2021). The vulnerability affected millions of systems across industries, including cloud services, enterprise applications, and critical infrastructure. The global response to Log4Shell demonstrated the power of crowdsourced cyber resilience. Within hours of the disclosure, security researchers, open-source contributors, and industry professionals collaborated through GitHub repositories, Twitter threads, mailing lists, and security forums to analyze the vulnerability, develop proof-of-concept exploits, create detection rules, and propose mitigation strategies. Organizations such as Cloudflare, Microsoft, and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published detailed threat chronicles that documented exploitation attempts and recommended defensive actions. The collaborative effort significantly accelerated the development of patches, detection tools, and protective configurations. However, the incident also revealed structural challenges. The initial disclosure process was chaotic, with conflicting information and inconsistent guidance circulating across platforms. The absence of a centralized, community-governed mechanism for coordinating crowdsourced intelligence limited the efficiency of the response.

These case studies collectively illustrate the strengths and limitations of current approaches to cyber resilience. SolarWinds demonstrates the value of detailed threat chronicles but also the constraints of centralized analysis. WannaCry highlights the destructive potential of Zero-Day exploits and the importance of rapid, collaborative defense. Log4j showcases the power of crowdsourcing but also the need for structured governance to harness community contributions effectively. Across all three cases, a recurring theme emerges: while community participation often plays a critical role in incident response, it is typically informal, reactive, and fragmented. The absence of a systematic, community-based approach to threat chronicles and Zero-Day defense limits the potential of collective intelligence to enhance cyber resilience.

These cases reinforce the argument that a more deliberate integration of crowdsourcing into formal resilience frameworks could significantly improve detection speed, analytical depth, and adaptive capacity. By examining these incidents through the lens of the conceptual framework, it becomes evident that community-driven collaboration is not merely beneficial but essential for addressing the complexity and scale of modern cyber threats. The next section builds on these insights by discussing the broader implications of the findings and exploring how a community-based approach can address the structural gaps identified in current cybersecurity practices.

Table 2 – A structured comparison of attack vectors, vulnerabilities, responses and lessons learned from the three major incidents.

INCIDENT	ATTACK VECTOR	VULNERABILITY TYPE
Starwinds	Supply chain compromise	Backdoor in Orion update
Wannacry	Wormable Ransomware	Eternalblue exploit
Log4j	Remote Code Execution	Zero-Day in logging library

6. Discussion

The findings from the literature and case studies reveal a complex but compelling picture of how cyber resilience can be strengthened through community-based collaboration. The discussion synthesizes these insights by examining the interplay among threat chronicles, Zero-Day defense, and crowdsourcing, while also highlighting the structural limitations that currently inhibit the full realization of collective intelligence in cybersecurity. The analysis demonstrates that although organizations increasingly recognize the importance of resilience, existing mechanisms for threat sharing and Zero-Day mitigation remain constrained by centralized governance, limited participation, and fragmented information flows. A community-based approach offers a promising pathway for addressing these gaps, but its implementation requires careful consideration of governance, trust, and coordination challenges.

The role of threat chronicles in cyber resilience is well established. They provide essential situational awareness, support anticipatory defense, and facilitate organizational learning (Strom et al., 2018; CISA, 2020). However, the case studies illustrate that the effectiveness of threat chronicles is often limited by their centralized nature. In the SolarWinds incident, for example, early analyses were conducted by a small number of private firms, and broader dissemination occurred only after significant delays. This pattern reflects a structural bottleneck: the reliance on a few authoritative institutions to produce and validate threat chronicles. While these institutions possess expertise and credibility, their limited capacity and hierarchical processes can slow the flow of critical information. A more community-driven model could diversify the sources of threat data, accelerate analysis, and enhance the granularity of insights. Yet, such a model would require mechanisms for validating community contributions to ensure accuracy and prevent misinformation.

Zero-Day defense presents an even more urgent challenge. Zero-Day vulnerabilities, by definition, exploit unknown weaknesses, leaving defenders with little time to react. The WannaCry and Log4j incidents demonstrate how rapidly Zero-Day exploits can propagate and how devastating their impact can be when detection and response mechanisms are insufficiently coordinated (Europol, 2018; Apache Software Foundation, 2021). The case studies also show that community participation often emerges spontaneously during Zero-Day crises, as researchers collaborate informally to analyze exploits and develop mitigations. This spontaneous collaboration highlights the latent potential of crowdsourcing in Zero-Day defense. However, the absence of structured frameworks for integrating community contributions limits the effectiveness of these efforts. Without formal coordination, information may be duplicated, fragmented, or inconsistent, reducing the overall efficiency of the response. A structured, community-based approach could harness the speed and diversity of crowdsourced intelligence while ensuring coherence and reliability.

Crowdsourcing emerges as a powerful enabler of cyber resilience, offering a means to distribute detection capabilities, enhance analytical diversity, and accelerate defensive innovation. Research shows that crowdsourced vulnerability discovery often outperforms traditional internal testing, uncovering flaws that would otherwise remain undetected (Finifter et al., 2013). Platforms like VirusTotal demonstrate how collective malware analysis can significantly improve detection accuracy and reduce response times (VirusTotal, 2022). The Log4j incident further illustrates how crowdsourcing can mobilize global expertise within hours, producing detection rules, proof-of-concept analyses, and mitigation strategies at unprecedented speed. These examples underscore the alignment between crowdsourcing and the core functions of resilience - anticipation, absorption, recovery, and adaptation (Linkov et al., 2018). However, the effectiveness of crowdsourcing depends on the presence of governance structures that can coordinate contributions, validate information, and ensure responsible disclosure.

The discussion also highlights the structural gaps that hinder the integration of community-based approaches into formal resilience frameworks. One major gap is the lack of standardized mechanisms for incorporating crowdsourced insights into threat chronicles. While community members frequently share observations on social media, forums, and open-source platforms, these contributions rarely make their way into formal advisories or institutional threat databases. This disconnect reduces the richness and timeliness of threat chronicles and limits their value for resilience. Another gap lies in the limited role of community participation in Zero-Day defense. Although researchers often collaborate informally during crises, there are few structured pathways for integrating their findings into official mitigation processes. This lack of integration slows the dissemination of defensive measures and increases the window of exposure.

Table 3 – A summary of limitations in current resilience practices and how crowdsourcing can address them.

CURRENT PRACTICES	LIMITATIONS	IMPACT
Centralized Threat Chronicles	Slow updates	Delayed detection
Vendor-led Zero Day defense	Limited visibility	Longer exposure
Closed information sharing	Fragmented insights	Weak institutional awareness
Institutional Governance	Capacity bottlenecks	Slow response

Trust and governance emerge as central challenges in implementing a community-based approach. Organizations may hesitate to rely on crowdsourced intelligence due to concerns about data quality, adversarial manipulation, or legal liability. These concerns are valid, as open platforms can be exploited by malicious actors seeking to spread misinformation or identify new attack vectors. However, these risks can be mitigated through structured validation mechanisms, contributor reputation systems, and transparent governance frameworks. The success of open-source security projects demonstrates that community participation can be both effective and trustworthy when supported by appropriate oversight and quality controls (Zhang et al., 2020).

The discussion also reveals that community-based approaches align with broader trends in cybersecurity governance. As digital ecosystems become more interconnected, no single organization or institution can maintain comprehensive situational awareness or respond effectively to all threats. Collective defense models, such as information sharing and analysis centers (ISACs), already demonstrate the value of collaborative intelligence. Crowdsourcing represents an extension of this model, expanding participation beyond institutional boundaries to include researchers, practitioners, and even informed users. This expansion enhances diversity, accelerates innovation, and strengthens resilience.

In summary, the discussion demonstrates that while threat chronicles and Zero-Day defense are essential components of cyber resilience, their effectiveness is constrained by centralized structures and limited community integration. Crowdsourcing offers a powerful mechanism for addressing these limitations, but its potential remains underutilized due to governance, trust, and coordination challenges. A community-based approach - supported by structured frameworks, validation mechanisms, and collaborative infrastructures - could significantly enhance the speed, accuracy, and adaptability of cyber resilience efforts. The next section builds on these insights by offering practical recommendations for implementing such an approach.

7. Recommendations

The findings of this study indicate that while cyber resilience has become a strategic priority for organizations worldwide, existing mechanisms for threat intelligence sharing and Zero-Day defense remain constrained by centralized structures and limited community integration. To address these gaps, this section outlines a set of recommendations aimed at operationalizing a community-based, crowdsourced approach to cyber resilience. These recommendations focus on governance, technological infrastructure, validation mechanisms, and cultural transformation, recognizing that effective implementation requires both structural and behavioral change.

A foundational recommendation is the establishment of community-governed threat chronicle platforms that enable structured, real-time contributions from diverse participants. Current threat chronicles, such as those produced by MITRE and CISA, provide valuable insights but rely heavily on institutional curation (Strom et al., 2018; CISA, 2020). A community-governed model would allow researchers, practitioners, and vetted contributors to submit observations, indicators of compromise, and analytical insights directly into shared repositories. To ensure reliability, these platforms should incorporate multi-layered validation mechanisms, including peer review, contributor reputation scoring, and automated anomaly detection. Such mechanisms would balance openness with accuracy, enabling threat chronicles to evolve into dynamic, collective intelligence systems that support anticipatory defense and adaptive learning.

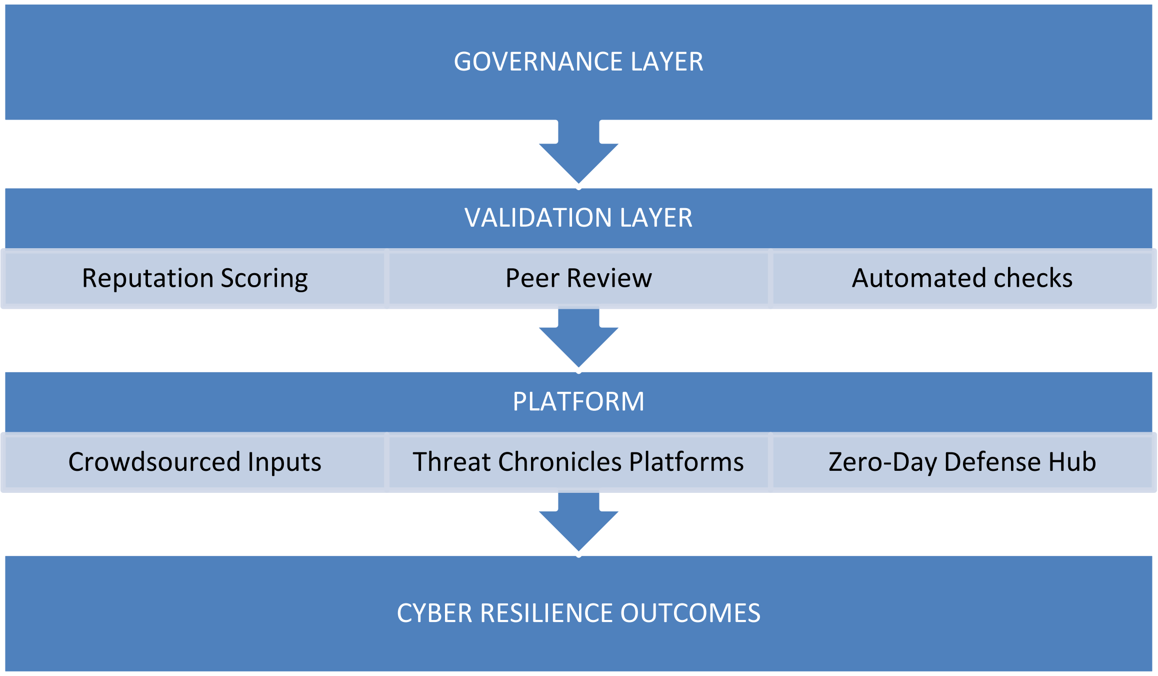

Figure 5. A high-level architecture showing how community contributions, validation mechanisms and governance layers integrate into resilience processes.

A second recommendation is the development of structured crowdsourcing frameworks for Zero-Day defense. The case studies demonstrate that community participation often emerges spontaneously during Zero-Day crises, but the absence of formal coordination limits the efficiency of these efforts (Europol, 2018; Apache Software Foundation, 2021). To harness the full potential of crowdsourced intelligence, organizations and governments should establish platforms that facilitate coordinated analysis, responsible disclosure, and rapid dissemination of mitigation strategies. These platforms should include secure communication channels, standardized reporting formats, and collaborative workspaces where researchers can analyze exploits, share findings, and co-develop defensive tools. Integrating these frameworks into national and sector-specific cybersecurity strategies would enhance the speed and coherence of Zero-Day responses.

A third recommendation involves the creation of hybrid governance models that combine institutional oversight with community participation. Trust remains a major barrier to adopting crowdsourced intelligence, as organizations may be reluctant to rely on contributions from unknown individuals (Zhang et al., 2020). Hybrid governance models can mitigate this concern by establishing clear roles, responsibilities, and quality controls. For example, institutions such as NIST, ENISA, or national CERTs could serve as custodians of community-driven platforms, providing oversight while allowing broad participation. This approach would preserve the credibility and authority of institutional frameworks while leveraging the speed and diversity of community contributions.

A fourth recommendation is the implementation of incentive structures that encourage sustained community engagement. Crowdsourcing thrives when contributors are motivated, whether through financial rewards, professional recognition, or opportunities for skill development. Bug bounty programs illustrate how incentives can drive high-quality vulnerability discovery (Finifter et al., 2013). Similar incentive models could be applied to threat chronicle contributions and Zero-Day analysis. For instance, contributors could earn digital credentials, reputation points, or access to advanced analytical tools based on the quality and impact of their submissions. These incentives would help cultivate a vibrant, self-sustaining community of contributors.

A fifth recommendation is the integration of advanced automation and AI-assisted validation into community-based resilience frameworks. Automated tools can help filter noise, detect anomalies, and prioritize high-value contributions, reducing the burden on human analysts. Machine learning models can identify patterns in crowdsourced data, flag suspicious submissions, and correlate indicators across multiple sources. These capabilities would enhance the scalability and reliability of community-driven platforms, ensuring that they remain effective even as participation grows.

A sixth recommendation is the promotion of cross-sector collaboration and information sharing. Cyber threats often transcend organizational and national boundaries, affecting supply chains, critical infrastructure, and global digital ecosystems. Community-based resilience frameworks should therefore facilitate collaboration across sectors, including government, industry, academia, and civil society. Information Sharing and Analysis Centers (ISACs) provide a useful model, but their membership is often limited to specific industries. Expanding these networks to include broader community participation would enhance situational awareness and collective defense.

Finally, a cultural shift is necessary to fully realize the potential of community-based cyber resilience. Organizations must move beyond the perception of cybersecurity as a proprietary or competitive domain and embrace the principle of shared responsibility. This shift requires leadership commitment, training programs, and communication strategies that emphasize the value of collaboration, transparency, and collective intelligence. As the case studies demonstrate, the most effective responses to major cyber incidents have involved rapid, open collaboration among diverse stakeholders. Institutionalizing this collaborative ethos would significantly strengthen global cyber resilience.

In summary, the recommendations presented in this section outline a pathway for integrating crowdsourcing into formal cyber resilience frameworks. By establishing community-governed platforms, structured Zero-Day defense mechanisms, hybrid governance models, incentive structures, automated validation tools, cross-sector collaboration networks, and a culture of shared responsibility, organizations can harness the full potential of collective intelligence. These measures would address the structural gaps identified in current practices and enhance the speed, accuracy, and adaptability of cyber resilience efforts. The next section concludes the article by synthesizing the key insights and outlining directions for future research.

8. Conclusion

The analysis presented in this article demonstrates that cyber resilience, as a strategic and operational imperative, requires more than traditional security controls or isolated institutional efforts. As digital ecosystems expand in complexity and interdependence, the capacity to anticipate, withstand, recover from, and adapt to cyber disruptions has become essential for organizational continuity and societal stability (Linkov et al., 2018; Stouffer et al., 2021). The literature and case studies examined throughout this work reveal that while threat chronicles and Zero-Day defense constitute critical components of resilience, their current implementation remains constrained by centralized governance, limited participation, and fragmented information flows. These limitations hinder the speed, accuracy, and adaptability required to confront modern cyber threats, particularly those involving rapidly evolving adversarial tactics and unknown vulnerabilities.

Threat chronicles, as structured narratives of cyber incidents, play a vital role in enhancing situational awareness and supporting anticipatory defense. However, their effectiveness is diminished by the bottlenecks inherent in institution-centric models of curation and dissemination. The SolarWinds case illustrates how delays in sharing critical insights can prolong exposure and complicate incident response (CISA, 2020). Similarly, Zero-Day vulnerabilities pose unique challenges due to their unknown nature and the absence of pre-existing defensive measures. The WannaCry and Log4j incidents demonstrate how quickly Zero-Day exploits can escalate into global crises when detection and mitigation efforts are not sufficiently coordinated (Europol, 2018; Apache Software Foundation, 2021). These cases underscore the need for more agile, distributed, and collaborative approaches to threat analysis and response.

Crowdsourcing emerges as a powerful mechanism for addressing these gaps. By leveraging the diverse expertise, perspectives, and observations of a global community, crowdsourcing can accelerate vulnerability discovery, enrich threat intelligence, and enhance the adaptability of defensive strategies (Finifter et al., 2013; Zhang et al., 2020). The spontaneous, community-driven collaboration observed during the Log4j crisis illustrates the latent potential of collective intelligence to strengthen cyber resilience. Yet, the absence of structured frameworks for integrating community contributions into formal resilience processes limits the full realization of this potential. Without governance mechanisms, validation systems, and coordinated workflows, crowdsourced intelligence remains fragmented and inconsistently utilized.

This article argues that a community-based approach - one that systematically integrates crowdsourcing into threat chronicles and Zero-Day defense - offers a transformative pathway for enhancing cyber resilience. Such an approach would diversify the sources of threat intelligence, accelerate the detection of emerging vulnerabilities, and strengthen the adaptive capacity of organizations and digital ecosystems. The recommendations outlined in this study provide a roadmap for operationalizing this vision, emphasizing the need for community-governed platforms, structured Zero-Day collaboration frameworks, hybrid governance models, incentive structures, automated validation tools, and cross-sector partnerships. Implementing these measures would require not only technological innovation but also cultural and organizational change, as cybersecurity shifts from a proprietary concern to a shared responsibility.

Future research should focus on empirically validating the conceptual framework proposed in this article. Surveys, interviews, and experimental studies could provide deeper insights into the effectiveness of community-based resilience models, the motivations of contributors, and the governance structures required to ensure trust and reliability. Additionally, interdisciplinary research involving computer science, organizational behavior, and public policy could help refine the mechanisms through which crowdsourcing can be integrated into national and global cybersecurity strategies.

In conclusion, the evolving threat landscape demands a reimagining of cyber resilience - one that embraces the power of collective intelligence and community-driven collaboration. By integrating crowdsourcing into the core processes of threat chronicling and Zero-Day defense, organizations can enhance their capacity to anticipate, withstand, recover from, and adapt to cyber disruptions. This shift represents not merely an enhancement of existing frameworks but a fundamental transformation in how cybersecurity is conceptualized and practiced. As the digital world becomes increasingly interconnected, the future of cyber resilience will depend on the strength, diversity, and coordination of the global community that defends it.

Here is a refined Acknowledgements section crafted specifically to align with the tone, structure, and expectations commonly seen in International Journal of Scientific and Management Research (IJSMR) publications. IJSMR typically favors concise, formal, and academically neutral acknowledgements.

Acknowledgements

We extend our deepest gratitude to all those who supported the development of this research paper. In particular, we acknowledge the commitment and collaboration of Arafat Bikadho, Tendai Nemure, Ruvimbo Mashinge and Mazvita Madziyanike whose involvement was invaluable in bringing this work to completion. We are also grateful to the faculty and staff of Yeshiva University for providing the resources, encouragement, and academic environment that enabled this study. Finally,

The authors also wish to acknowledge the contributions of scholars and institutions whose work in cyber resilience, threat intelligence, and collective security informed the development of this study. Appreciation is extended to the organizations that provided publicly accessible analyses of the SolarWinds, WannaCry, and Log4j incidents, which offered essential empirical insights for this research. The author also recognizes the global cybersecurity community whose collaborative efforts during major cyber events continue to demonstrate the importance of shared intelligence and collective defense. Their commitment to openness and knowledge exchange remains instrumental in advancing research and practice in this field.

References

1) Apache Software Foundation. (2021). Apache Log4j security vulnerabilities. https://logging.apache.org/log4j/2.x/security.html
2) Araujo, R., Silva, M., & Costa, C. (2024). Resilience in the context of cyber security. Journal of Information Security, 18(2), 45–62.
3) Arshad, J., Talha, M., Saleem, B., Shah, Z., Zaman, H., & Muhammad, Z. (2024). A survey of bug bounty programs in strengthening cybersecurity and privacy in the blockchain industry. Blockchains, 2(3), 195–216. https://www.mdpi.com/2813-5288/2/3/10
4) Bada, A., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393–410.

5) Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of Zero-Day attacks in the real world. Proceedings of the 2012 ACM Conference on Computer and Communications Security, 833–844.
6) Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
7) Charrier, C., Sadowski, J., Lecigne, C., & Stolyarov, V. (2025). Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis. Google Threat Intelligence Group. https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends
8) Check Point / Mitchelson, D. (2024). Key strategies for building cyber resilience in 2024. https://blog.checkpoint.com/executive-insights/key-strategies-for-building-cyber-resilience-in-2024/
9) CISA. (2024). Cybersecurity Alerts & Advisories. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories
10) CISA. (2020). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations (Alert AA20-352A). Cybersecurity and Infrastructure Security Agency.
11) CrowdStrike. (2024). CrowdStrike 2024 Global Threat Report. https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2024-global-threat-report/
12) Dittrich, D., & Kenneally, E. (2012). The Menlo Report: Ethical principles guiding information and communication technology research. U.S. Department of Homeland Security.
13) Europol. (2018). WannaCry ransomware: One year later. European Union Agency for Law Enforcement Cooperation.
14) Finifter, M., Akhawe, D., & Wagner, D. (2013). An empirical study of vulnerability rewards programs. USENIX Security Symposium, 273–288.
15) Kostyuk, N., & Wayne, C. (2021). The SolarWinds cyberattack: What happened and why it matters. Journal of Cybersecurity, 7(1), 1–12.
16) IBM Security. (2024). Cost of a Data Breach Report 2024. IBM. https://www.ibm.com/reports/data-breach
17) IOSR Journals. (2024). Zero-Day Vulnerabilities and the Clandestine Exploits Market: A Comprehensive Analysis. https://www.iosrjournals.org/iosr-jhss/papers/Vol.30-Issue1/Ser-7/B3001071120.pdf
18) Joinson, A. N., Dixon, M., Coventry, L., & Briggs, P. (2023). Development of a new "human cyber-resilience scale." Journal of Cybersecurity, 9(1), 1–10. https://academic.oup.com/cybersecurity/article/9/1/tyad007/7130095
19) Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. Sustainability, 10(2), 440.
20) Malone, T. W., Laubacher, R., & Dellarocas, C. (2010). The collective intelligence genome. MIT Sloan Management Review, 51(3), 21–31. https://sloanreview.mit.edu/article/the-collective-intelligence-genome/
21) NIST. (2023). NIST Cybersecurity Framework (CSF). National Institute of Standards and Technology. https://www.nist.gov/cyberframework
22) Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2021). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82 Rev. 2). National Institute of Standards and Technology.
23) Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK: Design and philosophy. MITRE Corporation.

24) Tzavara, A., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience. Journal of Cyber Policy, 9(1), 112–130.
25) VirusTotal. (2022). How VirusTotal works. https://www.virustotal.com
26) World Economic Forum. (2022). Global cybersecurity outlook 2022. World Economic Forum.
27) Zhang, Y., Wang, S., & Chen, X. (2020). Collective intelligence in cybersecurity: A systematic review. ACM Computing Surveys, 53(6), 1–36.