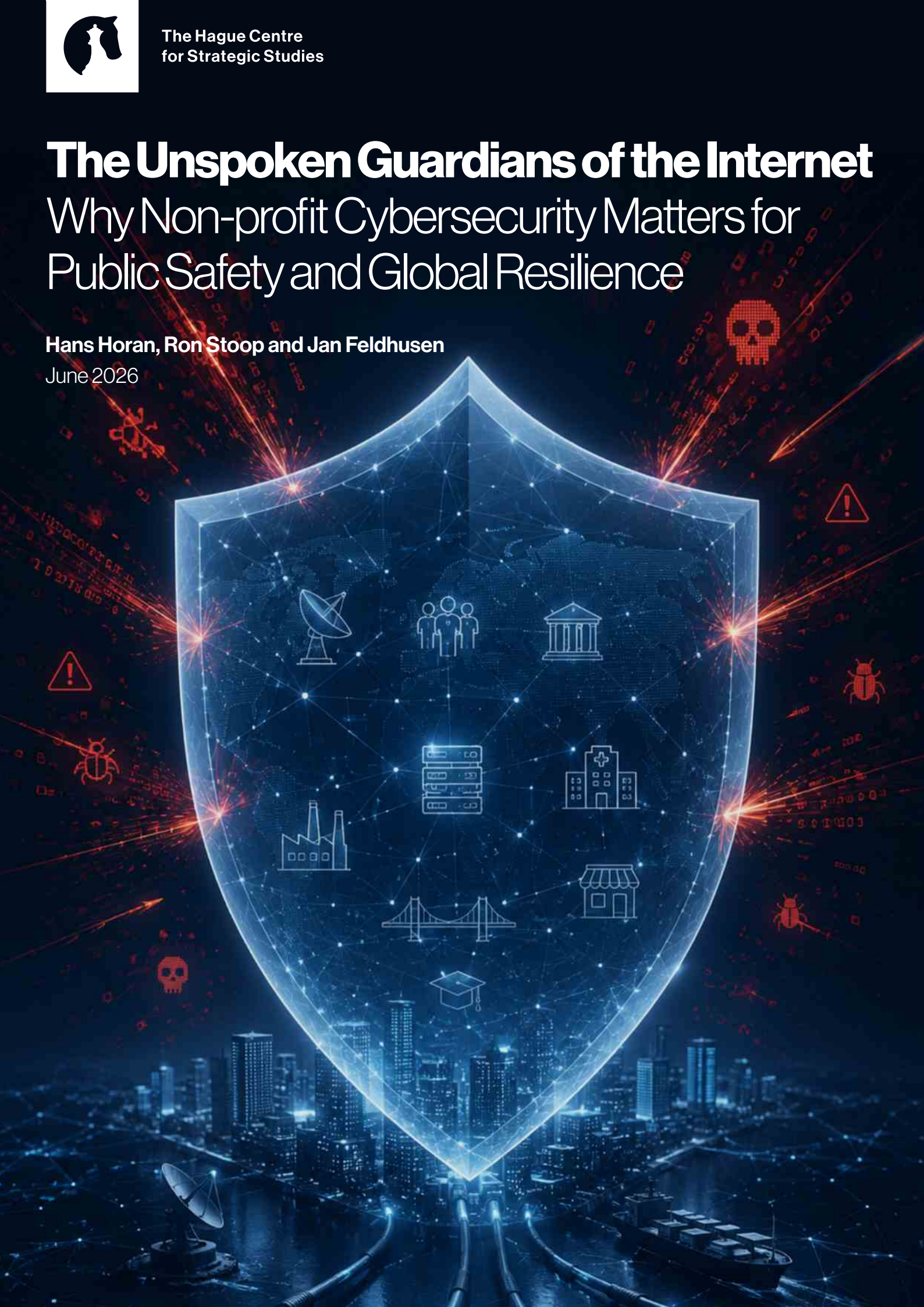
The Hague Centre
for Strategic Studies

The Unspoken Guardians of the Internet

Why Non-profit Cybersecurity Matters for Public Safety and Global Resilience

Hans Horan, Ron Stoop and Jan Feldhusen

June 2026



The Hague Centre
for Strategic Studies

The Unspoken Guardians of the Internet

Why Non-profit Cybersecurity Matters for Public Safety and Global Resilience

Authors:
Hans Horan, Ron Stoop and Jan Feldhusen

Quality Assurance:
Paul Sinning

The cover image was AI-generated
with OpenAI's ChatGPT.

June 2026

The research was commissioned by the Common Good Cyber and executed by The Hague Centre for Strategic Studies (HCSS). Responsibility for the contents and for the opinions expressed, rests solely with the authors.

Table of Contents

Executive Summary

As societies, economies, and public institutions become ever more dependent on digital systems, cybersecurity has become a core condition of public safety, economic continuity, and social resilience. Yet the rapid expansion of the cyber threat landscape has exposed a structural gap in the global cybersecurity ecosystem. Commercial providers remain essential, but market incentives, high costs, and a persistent talent shortage constrain them. Governments, meanwhile, are limited by jurisdiction, mandate, and political priorities. It is within this gap that non-profit cybersecurity organisations have emerged as critical actors, providing services that protect vulnerable communities, strengthen institutional resilience, and sustain critical parts of the digital environment that neither for-profit organisations nor the state can adequately secure on their own.

In this context, this study examines the value provided by non-profit cybersecurity organisations as being both substantial and systematically under-recognised. Its central finding is that these organisations do useful work and perform functions on which the wider cyber ecosystem depends. Their contribution lies not only in direct service provision but also in reducing harm, raising baseline resilience, supporting collective cyber hygiene, and maintaining shared infrastructure and standards.

The report first sets out the methodological framework used. Because the effects of cybersecurity interventions are preventive, distributed, and often not directly observable, the report adopts a three-pronged analytical framework: a threat-landscape-grounded assessment, an inventorisation/categorisation of the non-profit cybersecurity ecosystem, and a counterfactual assessment of the economic and social value generated by these organisations. This approach combines desk research, interviews, stakeholder consultations, and case-based inference to capture forms of value that conventional quantitative methods would otherwise overlook.

This is followed by setting the foundation of the methodology by examining the global cyber threat landscape against which non-profit organisations operate. It shows that cyber threats are unevenly distributed across regions and sectors, and that resilience varies not only by geography but also by levels of digitalisation, economic capacity, and organisational size. The report notes that highly digitalised and economically significant regions tend to face greater exposure to cyber threats. The chapter also highlights a widening resilience gap between large organisations and Small- and medium-sized enterprises (SMEs). While larger organisations have generally strengthened their cyber posture, smaller organisations remain structurally disadvantaged by limited budgets and insufficient staffing. This trend highlights that such SMEs require more structural help to maintain high cyber resiliency levels, but lack the financial capacity to do so; a gap that non-profits are able to fill.

The aforementioned foundation is built upon by mapping the non-profit cybersecurity ecosystem and demonstrating that it is a layered, interdependent architecture rather than a loose collection of isolated initiatives. Five main service pillars are identified: 1) threat intelligence collection and sharing; 2) incident response coordination; 3) standards, benchmarking, accreditation, and protocols; organisations with broader mandates; 4) and 5) digital security support for at-risk communities and civil society. It also identifies organisations that provide capacity-building and technical assistance, and a foundational support layer underpinning

the wider ecosystem. Another finding is that the sector's value lies in the way its different functions reinforce one another.

With this as a given, a counterfactual assessment of the economic and social value generated by non-profit cybersecurity organisations is provided. It does so through three categories: 1) market-equivalent value, 2) cost-avoided value, and 3) supported-underlying value. The findings are deliberately conservative and based on a limited sample of organisations, but they, nevertheless, point to very large orders of magnitude. The analyses show that:

- replacing non-profit services with market alternatives could cost hundreds of millions of dollars;
- that the harms they help prevent amount to billions in avoided losses; and
- that the infrastructure, standards, and coordination mechanisms they sustain underpin economic activity worth hundreds of billions of dollars.

As Table 1 illustrates, single organisations such as ShadowServer and CIS account for market-equivalent values of USD 830M–980M and USD 354M, respectively. Meanwhile, foundational support organisations like NLnet Labs and GCA underpin facilitated economic value estimated at USD 150–800 billion.

Finally, the main conclusion is that non-profit cybersecurity organisations are foundational to the resilience, safety, and continuity of the global cyber ecosystem, not merely supplementary to state or commercial provision. Their value becomes fully visible only when viewed holistically, in terms of the harms they reduce, the resilience they strengthen, and the collective cyber hygiene they sustain. Without them, cyber service gaps would widen, resilience would weaken, and governments, businesses, and civil society would face a more dangerous and less governable threat landscape.

Given the aforementioned context, it is recommended that governments establish dedicated multi-year funding streams, formally integrate non-profit actors into national cybersecurity strategies, and create rapid-response financing mechanisms for crises. Meanwhile, industry players should adopt a standing norm of financial support for the sector, and non-profits themselves should take greater ownership of articulating the value they provide. The report's final implication is clear: the relevant policy question is no longer whether non-profit cybersecurity organisations matter, but whether a robust and equitable cybersecurity system remains possible without them.

Table 1: Overview of Value Estimates of Case Studies by Value Category

	Value Estimation Method		
Cybersecurity Domain	**Market Equivalent Value**	**Cost Avoided Value**	**Facilitated/Supported Value**
Foundational Support	USD 10–13M (NLnet Labs)	USD 1–10B (NLnet Labs, GCA)	USD 150–800B (NLnet Labs, GCA)
Threat Intelligence	USD 830M–980M (ShadowServer)		USD 14.6B (CTA)
Incident Response		USD 800M–1.2B (CTA)	
Capacity Building	USD 17.5M (CRI)		FIRST (see breakdown on page 37)
Digital Security Support	USD 15M (Access Now), USD 1.9M–6.4M (CPI)	USD 1.23B (Access Now)	
Broader Mandate		USD 2.3M (IST)	
Standards, Benchmarks and Accreditation	USD 354M (CIS) USD 78M (CREST)		

Chapter 1: **Introduction**

Society has become increasingly digitalised in recent years, with the onset of the COVID-19 pandemic in 2020 and the subsequent emergence of new technologies aimed at improving working-from-home arrangements and easing businesses' financial burdens only hastening this trend.[1] Indeed, the rapid adoption of remote work technologies, such as cloud services and Remote Desktop Protocol (RDP), and emerging technologies, such as Artificial Intelligence (AI), has not only enabled businesses to operate more efficiently but also created new economic opportunities for everyday citizens.

However, the growing utilisation of these new technologies has also increased the threat posed by malicious actors via cyberspace. This trend is accelerated by growing geopolitical fragmentation, widening technological divides, and governance frameworks that cannot keep pace with the rapid technological development shaping the cyber threat landscape. As a result, demand for largely for-profit cybersecurity services has increased substantially in recent years, with the cybersecurity market projected to reach USD 1 trillion by 2031.[2] Nevertheless, the for-profit sector seems unable to fulfil growing cybersecurity needs due to a funding and talent gap, on both the supplier and client side, with the market estimated to be short at least 4.76 million qualified employees.[3]

This aforementioned trend has accelerated the pace of change in the current cyber threat landscape and forced organisations to rethink their traditional cyber defences. Moreover, cyber actors' geopolitical and geo-economic objectives have also further driven the adoption of emerging technologies to penetrate systems, creating new challenges for organisations' security hygiene. This adoption can be seen across the cyber actor spectrum, from cyber-criminal groups extorting companies for financial gain through AI-enabled campaigns to state-sponsored actors conducting cyber espionage via software supply chain attacks.[4]

The rapid development of this threat has made it difficult for for-profit cybersecurity firms to keep pace vis-à-vis developing adequate defensive measures. It is within this gap that entities such as non-profit cybersecurity organisations play a vital role in strengthening the global cybersecurity ecosystem. Indeed, non-profit cybersecurity organisations have proven themselves as an "indispensable actor in the global cybersecurity ecosystem", with 49% of the total security solutions analysed by Common Good Cyber maintained by non-profit

1 Florence Jaumotte et al., 'How Pandemic Accelerated Digital Transformation in Advanced Economies', International Monetary Fund, 21 March 2023, https://www.imf.org/en/blogs/articles/2023/03/21/how-pandemic-accelerated-digital-transformation-in-advanced-economies.

2 Calif Sausalito, 'GLOBAL CYBERSECURITY MARKET TO REACH $1 TRILLION ANNUALLY BY 2031', Cybercrime Magazine, 14 November 2025, https://cybersecurityventures.com/wp-content/uploads/2023/11/Cybersecurity-Market-Report-2026.pdf.

3 Khalil Mohammed, 'Cybersecurity Skills Gap Statistics: What the Numbers Reveal', DeepStrike, 8 August 2025, https://deepstrike.io/blog/cybersecurity-skills-gap.

4 Microsoft, *Microsoft Digital Defence Report 2025* (2025), 85, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

organisations.[5] These non-profit entities have filled in the gap left by for-profit organisations to "protect vulnerable communities, secure digital infrastructure, and enhance cyber resilience across sectors and regions".[6]

However, the security provisions of these non-profit organisations, despite their importance, are underappreciated relative to those of their for-profit counterparts and receive inadequate funding as a result.[7] These factors create operational instability and pose a risk of long-term security vulnerabilities if their services were to decline or disappear.

Given the disparity between escalating cyber threats and the underfunding of widely relied-upon non-profit cybersecurity services, The Hague Centre for Strategic Studies (HCSS) analysed in this paper the economic and social value generated by non-profit cybersecurity services. More specifically, the central question at the heart of this study will be what systemic costs and risks would arise should these non-profit cybersecurity services fail or scale back. In the same vein, this paper will propose policy recommendations to help sustain these services and the integral functions they play in global public safety and cyber resilience.

To address this, the report adopts an evidence-based approach to assessing the economic and social value generated by non-profit cybersecurity services. Chapter 2 outlines the methodological framework underpinning this analysis, which employs heuristics, counterfactuals, and scenarios to demonstrate the economic and social damage that non-profit cybersecurity actors help prevent. This would include assessing the contribution of non-profits to general cybersecurity.

After this methodological framework is defined, Chapter 3 sketches the global cyber threat landscape and the threats that non-profit cybersecurity organisations defend against. This analysis draws on open-source intelligence (OSINT), including industry reports, threat actor profiles, and attack-surface management reports, as well as human intelligence (HUMINT), e.g., interviews with non-profit cybersecurity organisations, to map these threats. This chapter then examines how these threats manifest across regions worldwide (i.e., the Americas, Europe, Sub-Saharan Africa, the Middle East & North Africa, and the Asia-Pacific) and how these pressures are felt differently not only across regions but also an organisation's economic standing (e.g., small and medium-sized enterprises vs Fortune 500) as well.

Chapter 4 further refines the focus by providing a taxonomy of non-profits that provide cybersecurity services and by examining how they deter or mitigate the threats categorised in the cyber threat landscape section. Non-profits provide a wide range of services, including those with direct economic impacts that are harder to quantify, such as advocacy for minorities to address the growing workforce and skill gap within cybersecurity. However, to ensure a consistent scope, this report will focus specifically on organisations that provide services that directly enhance a company's cybersecurity, such as cyber intelligence, cybersecurity training and workforce development, cybersecurity metrics, and cybersecurity testing, or support these services.

---

5 Kayle Giroud and Rayna Stamboliyska, *Nonprofit Contributions to Cybersecurity: Stories, Gaps, and Opportunities for Policy and Collaboration* (Common Good Cyber, 2025), 49, https://commongoodcyber.org/wp-content/uploads/2025/07/EUISS-Common-Good-Cyber-PAPER_Soft-Launch-1-1.pdf.

6 Giroud and Stamboliyska.

7 Giroud and Stamboliyska, *Nonprofit Contributions to Cybersecurity: Stories, Gaps, and Opportunities for Policy and Collaboration*, 30.

Chapter 5 builds on the findings of the previous two chapters by estimating the economic value of non-profit cybersecurity services by combining basic economic indicators with disruption multipliers derived from past incidents. These multipliers provide ballpark estimates of potential losses without implying precision. This is based mostly on case studies of major cyber disruptions or system failures and their estimated losses. These provide concrete reference points that demonstrate the importance of non-profit cybersecurity organisations, rather than attempting to quantify the exact monetary value of the savings from their cybersecurity services. The analysis in this chapter will inform the conclusions and recommendations at the end of this report.

Chapter 2: **Methodology**

Defining Non-Profit Cybersecurity Organisations

In addition to defining our methodological framework, it is important to clarify what this paper means by non-profit cybersecurity organisations. Non-profit cybersecurity organisations (NPOs) exist to serve collective interests rather than generate financial returns. They take different legal forms depending on jurisdictions, foundations, associations, public benefit corporations, and internationally registered bodies. Moreover, their governance typically includes technical experts, civil society advocates, government liaisons, and private-sector participants.

Non-profit cybersecurity organisations (NPOs) exist to serve collective interests rather than generate financial returns.

What unites the sector is a commitment to a mission that exists prior to, and independently of, the financial or political pressures that shape commercial firms and government agencies. In practical terms, that mission is making the digital environment safer for everyone, including those who cannot secure it themselves, by treating cybersecurity as a public good rather than a market commodity. The concept of the cyber poverty line, coined by researcher Wendy Nather in 2013, describes organisations that lack the resources, expertise, or institutional capacity to attain a basic level of cyber protection.[8] Below this line typically sit small and medium-sized enterprises, municipal governments, hospitals, schools, humanitarian organisations, and civil society groups, or entities routinely called "target-rich, resource-poor".[9] Serving this population is, at least partially, what the non-profit cybersecurity sector is for.

Commercial firms cannot do this work at scale, at least not sustainably. They answer to revenue targets and investor returns; services are designed and priced for paying clients. For example, threat intelligence may be kept proprietary precisely because its scarcity is what makes it valuable. Vulnerability knowledge may be handled in ways that privilege client relationships over public disclosure. In contrast, non-profits can more freely distribute services such as threat intelligence, release defensive tools without licensing costs, and offer training and capacity-building programmes to organisations that could never afford commercial alternatives.

Government cybersecurity agencies face a different set of limits. Their mandates are defined by legislation or executive direction; their jurisdiction is national; and their operations tend to serve national interests rather than the global collective benefit. This limits both who they can help and how openly they can act. Non-profit organisations work across borders, serve communities regardless of nationality, and are not bound by the political calculations that determine what a government agency can publicly say or do.

8 Tenchi Security, 'The "security Poverty Line" and Its Impact on Third-Party Cyber Risk', 14 April 2025, https://tenchisecurity.com/en/insights-news/the-security-poverty-line-and-its-impact-on-third-party-cyber-risk.

9 Center for Long-Term Cybersecurity, 'Call for Papers: Public Interest Cybersecurity Research', 13 December 2023, https://cltc.berkeley.edu/2023/12/13/call-for-papers-public-interest-cybersecurity/.

That independence comes at a cost. Non-profit cybersecurity organisations generate no commercial revenue. They depend on membership fees, philanthropic foundations, government grants, corporate sponsorship, and donations, a funding mix that raises real questions about both long-term sustainability and the practical limits of their independence.

Assessing Non-profit Cybersecurity Organisations' Economic and Social Value

With the previous context in mind and the complexity of assessing the economic and social value of non-profit cybersecurity organisations, this paper applies a three-pronged framework to capture both the economic and societal dimensions of their contributions. Instead of treating value solely in financial terms, the approach situates non-profit activity within the broader cyber-risk environment and examines how such organisations reduce harm, strengthen resilience, and support collective cyber-hygiene standards. To achieve this, this framework combines 1) a threat-landscape-grounded assessment; 2) an inventorisation and categorisation of the non-profit cybersecurity ecosystem; and 3) a counterfactual assessment of the economic and social value generated by these non-profits.

This design seeks to address the challenge of evaluating a phenomenon in which the effects of cybersecurity intervention are not only preventive, systemic, and distributed across multiple actors but also not directly observable. Indeed, the value of non-profit cybersecurity organisations is in somewhat intangible factors such as how they proactively reduce risks, manage incidents, and strengthen capacities. Therefore, a methodology that is limited to conventional impact metrics would understate or overlook certain aspects of their contributions.

This paper's methodology seeks to address those limitations by combining a qualitative and heuristic analytical approach grounded in open-source data/desk research, expert interviews, stakeholder consultations, and case-based inferences. This three-pronged framework is broken down as follows:

A Threat Landscape Grounded Assessment

This first component establishes the threat environment in which non-profit cybersecurity organisations operate. Indeed, Chapter 3 provides the analytical foundation for understanding what these organisations help their beneficiaries prevent, mitigate, or recover from.

The cyber threat landscape is based on multiple forms of open-source information, academic literature, policy reports, industry reporting, incident databases, and expert interviews. It should be noted that this landscape is not meant to be an exhaustive catalogue of all cyber risks, but rather a means of identifying the most consequential global cyber threats affecting businesses and critical digital infrastructure.

This chapter's analysis is grounded in three questions: 1) Which threat categories present the greatest economic and social disruptions for the NPOs' beneficiaries?; 2) How are these threats changing in terms of scale, sophistication, and diffusion?; and 3) Which aspects of these threats change depending on the size of the beneficiaries? In this vein, this chapter serves as background information and a basis for linking the organisational activities presented in Chapter 4 to the forms of economic and social value generated in Chapter 5.

Inventorisation of Non-profit Cybersecurity Ecosystem

The second prong of this framework builds upon the threat landscape by mapping and categorising the non-profit cybersecurity ecosystem. This prong identifies the different types of activities that non-profits engage in. This inventorisation is not meant to simply provide a reference list of all non-profit cybersecurity organisations. Instead, its purpose is to identify the types of organisations that exist, provide examples of these organisations, the functions they perform, where they operate in the cyber ecosystem, and how their activities relate to improving global cyber resilience standards. This was done through a combination of desk research and insights drawn from the interviews conducted for this study. The resulting categorisation is broken up into several pillars identified during the research process:

- **Threat intelligence collection and sharing**: including the gathering, analysis, and dissemination of threat data that supports earlier detection, improved situational awareness, and faster defensive action across organisations and jurisdictions;
- **Incident response coordination**: including the facilitation of trusted cross-border and cross-sector collaboration, common response protocols, and collective mechanisms for managing large-scale incidents;
- **Standards, benchmarking, accreditation, and protocols:** including the development and maintenance of technical standards and protocols, consensus-based security configuration guidance, and professional accreditation frameworks that set quality expectations for both the tools organisations deploy and the providers they hire;
- **Capacity building and technical assistance:** including training, tool development, operational support, and the provision of free or low-cost resources to organisations with limited cybersecurity capability;
- **Digital security support for at-risk communities and civil society**: including direct assistance to journalists, human rights defenders, non-governmental organisations, and other groups exposed to targeted surveillance, repression, or cyberattack and underserved by both the market and the state;
- **Organisations with broader mandates**: whose contribution lies not in one specialised service but in convening, coordinating, and enabling activity across multiple cybersecurity functions, often spanning policy, operational support, ecosystem-building, and public-interest advocacy.
- **Foundational Support**: Organisations that do not provide traditional cybersecurity services, but instead whose services underpin and support the infrastructure and services provided by other non-profit organisations.

Methodologically, this categorisation translates a diverse and uneven thematic field into a comparable analytical structure. Secondly, it clarifies the means through which non-profit organisations generate economic and social value, which is essential for the later assessment. Lastly, it will also aid the later assessment in distinguishing between direct operational services and ecosystem-enabling functions, allowing the paper to capture forms of value that are often overlooked when impact is assessed solely in terms of immediate outputs.

Counterfactual Assessment: The Economic and Social Value Generated by Non-profits

The analysis of economic value estimation is based on a mixed-method approach, combining qualitative interviews with quantitative value estimations derived from these interviews and publicly available data. Interviewees were selected, ensuring broad coverage of the non-profit cybersecurity domain. In total, 11 companies were interviewed for this research and selected to provide an equal distribution across the seven aforementioned pillars, as far as possible.

The interviews were conducted in a semi-structured format. First, a set of general questions was asked about the organisation's operations. This was followed by more specific questions focused on economic value generation. In many cases, these questions did not yield direct quantitative data. Instead, they explored operational effects of interventions, which were then translated into economic estimates using a heuristic approach. For example, if a certain cybersecurity training would result in a 30% reduction in the trainees across the board clicking on phishing links, this would generate an economic value of a 30% reduction in successful cyberattacks, based on the average cost of successful cyberattacks and the average impact this had on organisations of varying sizes (e.g., SMEs vs large corporations).

This method allows flexibility, combining structured data with estimates based on interviewees' qualitative assessments. In general, purely quantitative data were prioritised. Where this was unavailable, illustrative or anecdotal examples from specific use cases were subsequently converted into data points. All estimates are conservative. Actual values are likely higher, as certain economic benefits that were difficult to quantify have been excluded.

Throughout the interviews and accompanying desk research, it became clear that value can be expressed in several distinct ways, such as:

Market Equivalent Value: This refers to benchmarking non-profit services against what for-profit organisations would charge for similar services. In this way, the services can be understood as delivering a comparable level of economic value under normal market conditions.

Cost Avoided Value: This primarily reflects the security benefits generated for beneficiaries. These benefits may arise from faster threat intelligence sharing, improved protection following participation in programmes or services, or quicker resolution and prevention of cybersecurity incidents, along with their associated economic impacts.

Supported Underlying Value. This approach captures the economic activity enabled or supported by organisations acting as facilitators or market enablers. For example, some organisations provide free services that underpin significant parts of the internet infrastructure. A case in point is the Domain Name System (DNS) resolver developed by NLnet Labs, which functions as an industry standard and enables substantial economic activity. Facilitated values are typically higher in magnitude, as they relate to broader segments of the digital economy. However, they should not be treated as directly equivalent to other forms of economic benefit estimation. Rather, they provide a more comprehensive perspective on the direct and indirect value generated by non-profit cybersecurity organisations.

Together, these three categories provide an overview of the directly measurable economic value generated by non-profit cybersecurity organisations. This framework helps to contextualise these benefits in relation to the operational costs required to sustain such organisations.

Chapter 3: **Global Cyber Threat Landscape**

Before an assessment of the non-profit cybersecurity sector's economic and social value can be conducted, it is essential to contextualise the cyber threat landscape against which the organisations they protect are threatened. Similar to its kinetic counterparts, the cyber threat landscape comprises a variety of attack types, vectors, and actors, all of which pose unique societal and business risks.

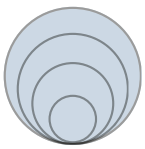
To provide a solid foundation for assessing the potential economic and social value of non-profit cybersecurity organisations, this chapter will present a spectrum of general cyber trends in the current landscape. This chapter should be viewed as providing illustrative examples of the breadth of threats and trends faced by global organisations and which sectors and organisational sizes are at the highest risk, rather than a comprehensive list of all cyber-related threats. By exploring these variations, the chapter sets the stage for a more detailed discussion of how non-profit organisations provide resilience to their beneficiaries and the general public, and of the potential consequences of their disappearance.

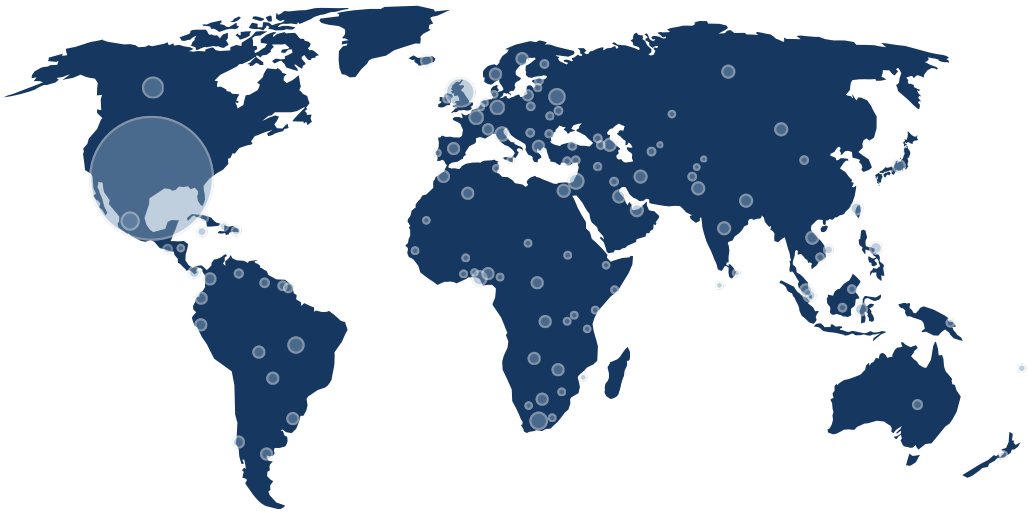
Figure 1: Countries Where Microsoft Customers were Most Frequently Impacted by Cyber Threats (January-June 2025)[10]

Scale of impact

Most impacted

Least impacted





	% of total
1. United States	24.8%
2. United Kingdom	5.6%
3. Israel	3.5%
4. Germany	3.3%
5. Ukraine	2.8%
6. Canada	2.6%
7. Japan	2.6%
8. India	2.3%
9. United Arab Emirates	2.0%
10. Australia / Taiwan	1.8%

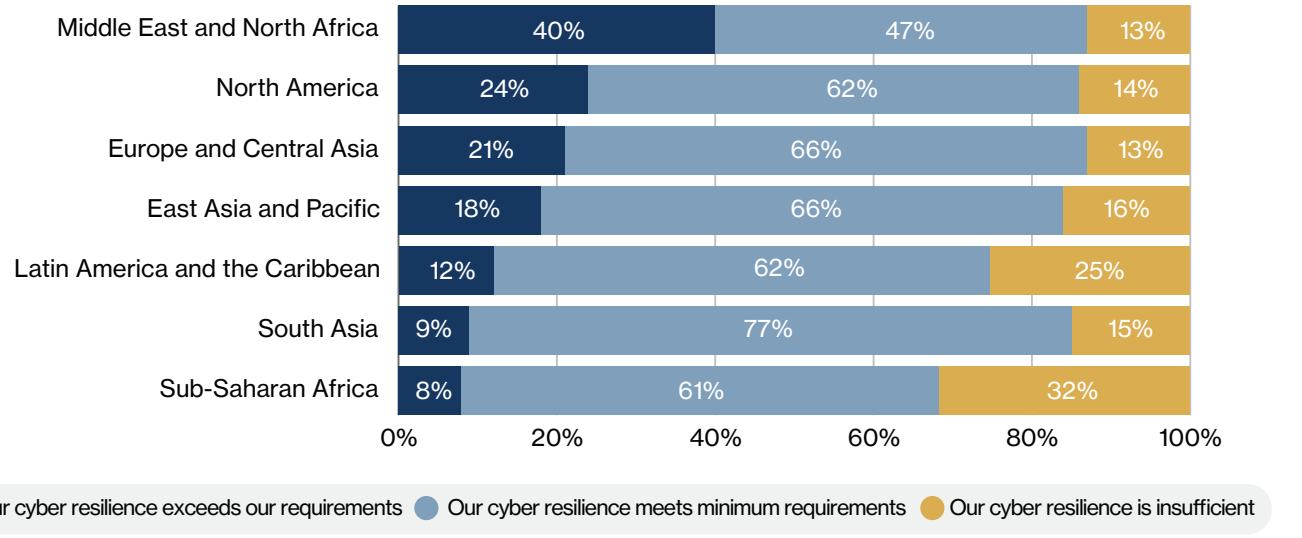
[10] The lower data presence in China stems from geopolitical considerations, with China's strict data sovereignty laws and US-China tension-related security concerns leading the company to slowly shift services out of the country. Similar considerations exist for Russia due to the Ukraine conflict. As for India, it is a growing market for Microsoft, and they are acquiring more data on a regular basis.

The Global Differentiation in Cyber Threats & Resilience

While cybersecurity is increasingly becoming a global concern, certain regions are impacted by threats emanating from cyberspace to varying degrees and intensities. According to Microsoft's 2025 Digital Defence report, the US was the country most frequently impacted by cyber threats, accounting for 24.8% of the attacks detected by the firm that year. Other countries in the top 10 include countries in Europe, North America, the Middle East, and the Asia-Pacific (please see the footnote below Figure 1 for further clarification on how geopolitics impacts the graph's findings).[11]

Indeed, regions with higher levels of digitalisation, internet connectivity, and economic importance are more often targeted by cyber threat actors. For example, while Europe (94.2%) has higher internet penetration than North America (93.3%), the US's status as the world's largest economy and home to many Fortune 500 companies makes it a slightly more attractive target for cybercriminals than Europe-based organisations.[12]

Figure 2: How did Organisations per Region Rate their Cyber Resilience?[13]



These different threat exposure rates have led regions with higher exposure to be better prepared to tackle the growing threat posed by cyberspace. For example, a survey conducted by the World Economic Forum (WEF) in 2026 amongst global Chief Information Security Officers (CISOs) found that organisations in countries with a longer history of digitalisation and higher levels of economic activity were more likely to believe their organisation's cyber resilience exceeded requirements (see Figure 2). However, the majority of organisations across all regions did believe they met at least the minimum requirements for cyber resilience.[14]

11 Microsoft, *Microsoft Digital Defence Report 2025*, 10.

12 Christy Tila, 'Global Internet Penetration Rate as of October 2025, by Region', Statista, 19 November 2025, https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/?srsltid=AfmBOoqHEPKm-kxUH2KBiOTexuj3cso52FpjgeO1d10WsP8zbvmUKuNf.

13 World Economic Forum, *Global Cybersecurity Outlook 2026* (World Economic Forum, 2026), 49.

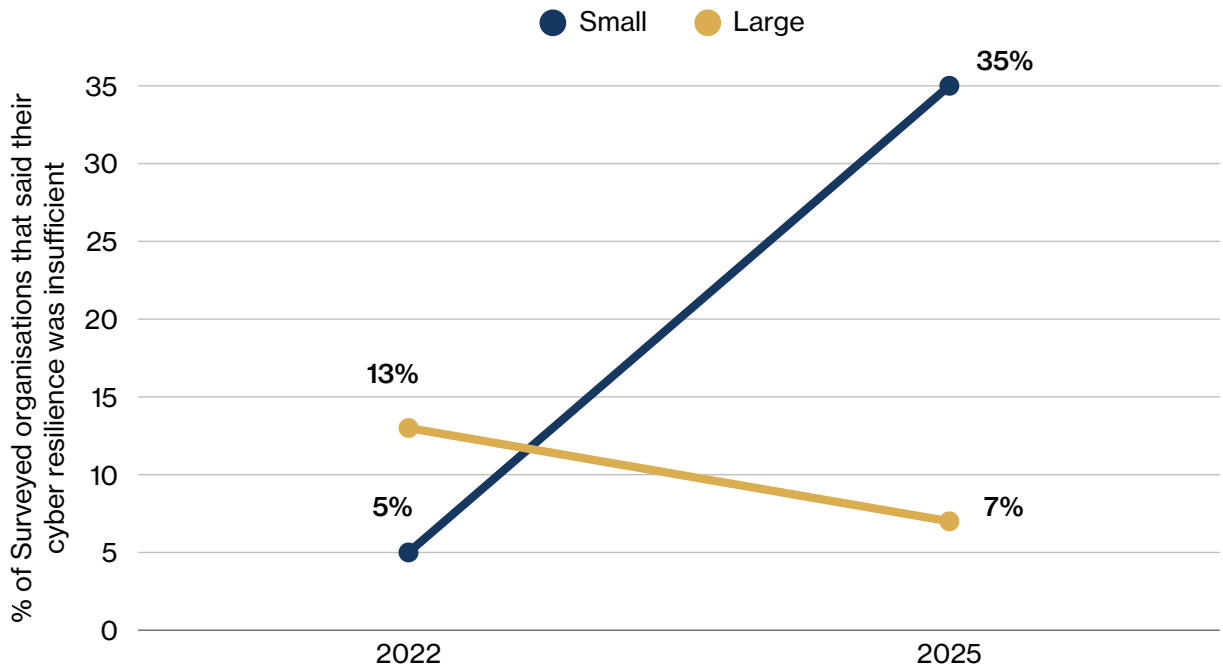
14 World Economic Forum, 49.

The only exception to this trend is the Middle East and North Africa (MENA) region. However, this exception can be partially explained by the MENA region's unique geopolitical situation. For example, the ongoing tit-for-tat cyber conflict between Israel and Iran creates an environment in which regional organisations must rapidly increase their cyber resilience to maintain regular business operations.[15]

Difference in Cyber Resilience between Large and Small- and Medium-sized Enterprises (SMEs)

Geographical location, socio-economic health, education, and digitalisation rates are key determinants of whether a region and its organisations are resilient to the cyber threats they face. However, there remains a disparity among organisations of differing economic size as well. Indeed, according to a 2025 WEF survey, smaller organisations "are struggling to ensure cyber resilience, while larger organisations show steady progress". This survey found that 35% of security personnel interviewed believed their cyber resilience was insufficient to address the threats they faced, up from 5% in 2022. Meanwhile, larger organisations have shown the inverse trajectory, with the amount decreasing from 13% to 7% over the same period (see Figure 3).[16]

Figure 3: The Disparity between Smaller and Larger Organisations vis-à-vis Cyber Resilience



[15] Jack Alexander, 'How "Big 4" Nations' Cyber Capabilities Threaten the West', Dark Reading, 9 February 2024, https://www.darkreading.com/vulnerabilities-threats/how-big-4-nations-cyber-capabilities-threaten-the-west.

[16] World Economic Forum, 'Global Cybersecurity Outlook 2025: Insight Report', World Economic Forum, 13 January 2025, 5, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

This disparity in resiliency levels can largely be explained by budget constraints. According to the 2025 IANS Research and Artico Search Security Budget Benchmark Report, companies spend on average "0.69% of revenue on cybersecurity in 2024 and 2025". However, this spending reflects averages across organisations of all sizes. As such, a business generating "5 million in annual revenue" translates to an estimated USD 34,000 yearly cybersecurity budget. As such, SMEs are inherently at a disadvantage vis-à-vis larger organisations in terms of securing the funds needed to support their IT infrastructure.[17]

Therefore, when examining the upcoming threat landscape and the economic and social value that non-profit cybersecurity services provide in the upcoming chapters, it is important to note that this value varies significantly by organisational size. Moreover, this underscores the essential need for non-profit cybersecurity organisations that provide services for either free or at a severe discount, as they help less economically well-off organisations maintain robust cybersecurity standards.

General Cyber Trends

Emerging Technologies: A Double-Edge Blade in an Increasingly Cloud-based Environment

In tandem with global organisations' digitalisation, there has been a shift towards the adoption of emerging technologies, enabling greater scalability and hopes of increased output. However, alongside this, the adoption of technologies such as cloud and Artificial Intelligence (AI) has also introduced complex security challenges by providing threat actors with more tools at their disposal and an increased surface area to operate across.

The adoption of technologies such as cloud and Artificial Intelligence (AI) has also introduced complex security challenges by providing threat actors with more tools at their disposal and an increased surface area to operate across.

Cloud Solution Adoption

The key benefit for organisations in adopting the cloud has been the offloading of certain cybersecurity responsibilities to cloud service providers (CSPs). This "shared responsibility model" is particularly attractive to SMEs with limited resources and/or digital expertise.[18] However, cyber threat actors are increasingly targeting organisations' cloud environments to "compromise assets, disrupt operations, and exfiltrate sensitive data". Indeed, Microsoft's 2025 Digital Defence Report found that the "number of observed incidents against Azure-based environments" increased by 26% during the second half of its reporting period. Similarly, Microsoft recorded an "87% increase in campaigns aimed at disrupting customer environments through ransomware, mass deletion, or other destructive actions". This trend underscores the accelerating impact of emerging technologies not just on businesses but also on cyber actors' capabilities.[19]

---

17 IANS, 'Cybersecurity Budgeting for Small Businesses: What to Expect in 2026', Cyber Unit, 8 February 2026, https://cyberunit.com/insights/cybersecurity-budgeting-small-business-2026/.

18 Christine Zhenwei Qiang and Ghislain de Salins, 'Cloud Adoption: A Catalyst for Cyber Resilience in Developing Countries', World Bank Blogs, 27 February 2025, https://blogs.worldbank.org/en/digital-development/cloud-adoption--a-catalyst-for-cyber-resilience-in-developing-co.

19 Microsoft, *Microsoft Digital Defence Report 2025*, 41.

AI Integration and Leveraging

Similar to Cloud Solutions, AI has acted as a force multiplier for cyber actors' malicious operations. Most notably, these actors have leveraged AI to improve the quality of their phishing, impersonation, extortion, and evasion tactics. According to cybersecurity firm Fortinet's 2025 Global Threat Landscape Report, AI is "lowering the barrier to entry for aspiring cybercriminals, increasing access to tactics and intelligence needed to execute attacks regardless of an adversary's technical knowledge".[20]

For example, the European Union Agency for Cybersecurity (ENISA) disclosed in its 2025 Threat Landscape Report that AI-supported phishing campaigns "reportedly represented more than 80% of observed social engineering activity worldwide, with adversaries leveraging jailbroken models, synthetic media, and model poisoning techniques to enhance their operational effectiveness".[21] Microsoft underscored the financial impact that these AI-enhanced operations had in 2025, noting that "the value of fraud schemes (many AI-enabled) blocked by Microsoft in one year" was USD 4 billion.[22]

Social Engineering: Humans Remain a Key Weakness for Cyber Resilience

Social engineering is a term that refers to a wide range of attacks that "leverage human interaction and emotions to manipulate the target [...] During the attack, the victim is fooled into giving away sensitive information or compromising security". As a part of this, cyber actors prey on certain human behaviours to increase the success rate of their cyberattacks, these include:[23]

Figure 4: Types of Human Behaviour Exploited by Cyber Criminals

Liking	People tend to lend greater credibility to those they like. To exploit this, a social engineering attacker may try to appear trustworthy, attractive, or like someone who shares similar interests.
Reciprocity	Social engineering attackers exploit people's tendency to trust those who give them things by offering advice, exclusive access, or personalising their approach to make the target feel obliged to reciprocate.
Commitment	An attacker using social engineering techniques can exploit this by first making small requests before making a larger request. They may also have them agree to an action before its risks are obvious.
Social Proof	Attackers may use social networking to exploit the social proof concept by claiming that the victim's online friends have already endorsed an action, product, or service.
Authority	People naturally tend to trust authorities more than those with less experience or expertise. Hence, an attacker may use phrases such as "according to experts" or "science proves" to persuade a target to agree.

[20] Fortinet, *2025 Fortinet Global Threat Landscape Report* (2025), 13, https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf.

[21] *ENISA Threat Landscape 2025* (European Union Agency for Cybersecurity, 2025), 6, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

[22] Microsoft, *Microsoft Digital Defence Report 2025*, 33.

[23] Fortinet, 'What Is Social Engineering In Cybersecurity?', Fortinet, accessed 18 February 2026, https://www.fortinet.com/resources/cyberglossary/social-engineering.

While phishing is the most common form of social engineering, Business Email Compromise (BEC) scams pose a greater risk to businesses. BEC is a more targeted, well-planned version of phishing, in which "cybercriminals impersonate trusted leaders [or client] to trick employees into sending money or data".[24] Oftentimes, this is done by either spoofing email addresses or utilising a compromised email account. In some cases, BEC actors target companies with numerous financial transactions, hoping that their requests to transfer funds or data to an actor-controlled bank account or data storage platform will not be subject to rigorous scrutiny.

BEC scams account for only an estimated 2% of total threats observed in 2025. Nevertheless, their impact was disproportionately high, with BEC being registered as "a more frequent outcome in attacks (21%) than ransomware (16%)".

According to Microsoft's 2025 Digital Defence Report, BEC scams account for only an estimated 2% of total threats observed in 2025. Nevertheless, their impact was disproportionately high, with BEC being registered as "a more frequent outcome in attacks (21%) than ransomware (16%).[25]

The industries most affected by BEC scams are those that regularly send and receive documents, such as financial statements. This includes research and academic institutions, telecommunication firms, financial service organisations, and logistics companies. This specific targeting stems from the very nature of BEC scams. These actors' focus on this weak link has resulted in over USD 55 billion in losses for companies over the last decade, despite only around 305,000 incidents being recorded during this timeframe.[26] Research conducted by IBM further underscores the financial cost of such scams to businesses, with BEC scams ranking second-most expensive, at an average of USD 4.89 million per incident.[27]

Ransomware: Remains a Primary Concern and Threat for Businesses

More disruptive and destructive threats, such as ransomware, also remain a persistent concern for businesses across all sectors. According to the World Economic Forum's Global Cyber Outlook 2026 report, ransomware constituted the top concern for CISOs in both 2025 and 2026.[28]

Indeed, despite dating back to the 1980s, ransomware attacks remain the third most common cyberattack method today and account for over 10% of all data breaches globally.[29]

24 'What Is Business Email Compromise (BEC)?', Microsoft, accessed 18 February 2026, https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec.

25 Microsoft, *Microsoft Digital Defence Report 2025*.

26 Ben Kapon, 'Combating Business Email Compromise (BEC): The Costliest Phishing Tactic', KELA, 24 April 2025, https://www.kelacyber.com/blog/combating-business-email-compromise/.

27 'What Is Business Email Compromise (BEC)?', IBM, accessed 18 February 2026, https://www.ibm.com/think/topics/business-email-compromise.

28 World Economic Forum, *Global Cybersecurity Outlook 2026*, 11.

29 Fortinet, 'Ransomware: Types, Examples & Removal Tactics', Fortinet, accessed 17 February 2026, https://www.fortinet.com/resources/cyberglossary/ransomware.

Figure 5: Which Cyber Risks Concern You Most for Your Organisation?

Source: World Economic Forum

Rank	2025	2026
1	Ransomware Attack	Ransomware Attack
2	Supply Chain Disruption	Supply Chain Disruption
3	Cyber-enabled Fraud & Phishing (Social Engineering)	Exploitation of Software Vulnerabilities

Ransomware can largely be categorised into four different categories:[30]

Figure 6: Different Types of Ransomware

Scareware	A type of malware that utilises social engineering tactics to "scare, shock, or cause a victim anxiety" as to convince them that their computer has been encrypted with ransomware and either pay to have it decrypted or buy software to address the non-existent malware.
Screen Locking	This type of ransomware attack makes it appear as if your computer is locked and inaccessible. For example, it could claim that it was encrypted by a "law enforcement agency" and ask for an online payment.
Encrypting (crypto) ransomware	This type of ransomware utilises advanced encryption algorithms to actually encrypt a victim's device(s). This type of attack also comes with a "ransom" note that typically explains how and where you can pay to have your device(s) unencrypted.
Ransomware-as-a-service (RaaS)[31]	RaaS is a business model whereby operators of a particular ransomware strain rent out their strain (much like a cloud platform) to affiliates. These affiliates then launch ransomware attacks in the name of the operators and split the profits.

Given ransomware actors' financial motivations, they typically target organisations across a wide range of industries. However, these cybercriminals are also known to target "low-hanging fruit" or organisations that do not possess strong security, such as SMEs that lack the necessary funds to employ an IT professional who fully understands the entire ransomware lifecycle. According to Microsoft's 2025 Digital Defence report, approximately 48% of ransomed organisations in 2025 had annual revenue of USD 50 million or less. Of these organisations, the top three targets were 1) industrial projects and services, 2) engineering and construction, and 3) retail, wholesale, and distribution.[32] What these three industries have in common is that they either pose a high amount of highly sensitive data that can be encrypted (e.g., engineering work), they provide a time-sensitive service (e.g., industrial production of raw materials such as steel or aluminium that require a high-level of precision) or provide a critical service that cannot be offline for a long period of time (e.g., food and groceries supply chains that would negatively impact citizens if taken offline). Targeting these specific types of organisations increases the likelihood that they will pay the cyber actor's ransom demand to quickly restore their systems, as prolonged offline periods (i.e., several weeks or months) would have significant reputational and financial implications.

Indeed, ransomware attacks are among the most expensive cybersecurity incidents, with IBM's 2025 Cost of a Data Breach Report finding that, on average, victims paid USD 5.08 million in ransom that year.[33]

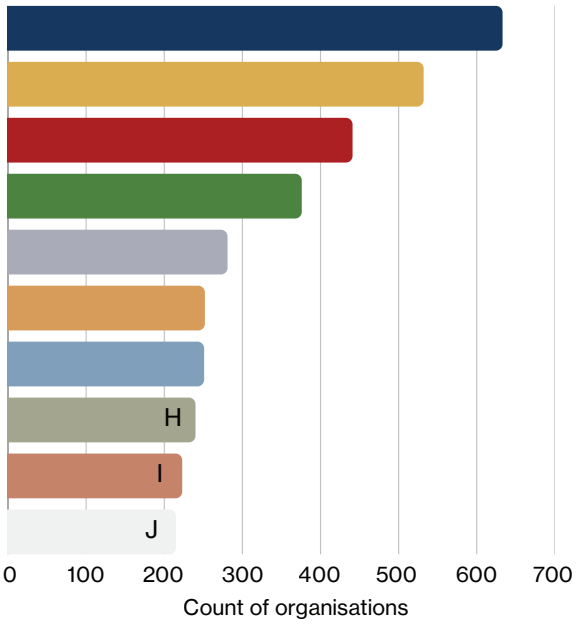
30 Fortinet.

31 Kurt Baker, 'Ransomware as a Service (RaaS) Explained How It Works & Examples', Crowdstrike, 30 January 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

32 Microsoft, *Microsoft Digital Defence Report 2025*, 28.

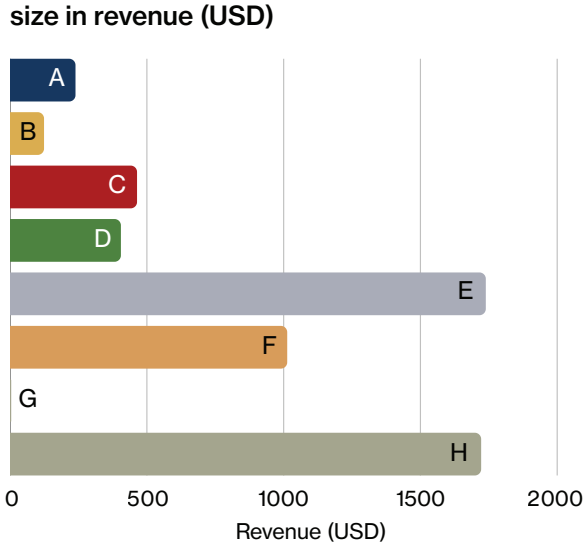
33 IBM, *Cost of a Data Breach Report 2025* (IBM, 2025), https://www.ibm.com/reports/data-breach.

Figure 7: Ransomed Organisations by Organisation Size in Revenue (USD) – Microsoft Digital Defence Report 2025



A. Industrial products and services	633
B. Engineering and construction	532
C. Retail, wholesale, and distribution	441
D. Health care providers and services	376
E. Technology	281
F. IT or technology consulting	252
G. Education	251
H. Law services and consulting	240
I. Transportation	223
J. Financial and investment consulting	215

Figure 8: Top Ten Industries Impacted by Ransomware – Microsoft Digital Defence Report 2025



A. Over 1 billion	239
B. 500 million – 1 billion	124
C. 100–500 million	464
D. 50–100 million	405
E. 10–50 million	1,739
F. 5–10 million	1,013
G. 1–5 million	4
H. Revenue not available	1,722

Software Supply Chain Attacks

The aforementioned social engineering and ransomware represent examples of more rudimentary and intermediate-level cyberattacks, respectively. In contrast, a software supply chain attack is an example of a more sophisticated, resource- and time-intensive cyberattack. During this cyberattack, hackers "target third-party suppliers, vendors, partners, or software dependencies to compromise downstream organisations". These types of attacks can be further separated into two types:[34]

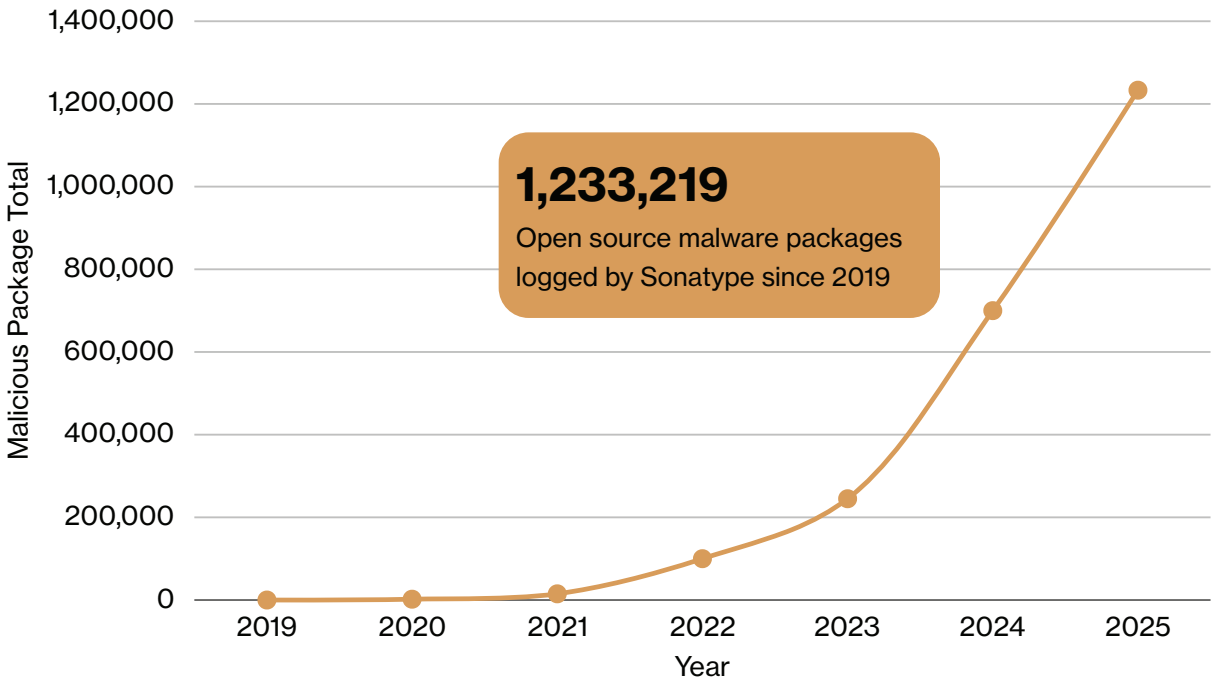
1. **Attacks on the software supply chain**: these target code repositories, open-source libraries, software update pipelines, and development tools to add harmful code to real applications
2. **Attacks on the operational supply chain**: these take advantage of third-party service providers, such as managed security providers (MSPs), cloud vendors, or business partners who have special access to the network they seek to target.

[34] Proofpoint, 'What Is a Supply Chain Attack?', Proofpoint, accessed 3 March 2026, https://www.proofpoint.com/us/threat-reference/supply-chain-attack#:~:text=A%20supply%20chain%20attack%20is,networks%20they%20seek%20to%20target.

A salient example of a software supply chain attack and its implications is the 2020 SolarWinds incident. In March 2020, it was discovered that alleged Russian Foreign Intelligence Service (FIS) hackers gained access to SolarWinds' Orion system and inserted malicious code into a system update.[35] Subsequently, the Orion system pushed the malicious update to more than 30,000 public- and private-sector clients worldwide, including the US Department of Homeland Security, Cisco, and Nvidia.[36]

The widespread growth, success, and impact of software supply chain attacks stem from the growing importance of open-source code for society's deepening digitalisation (see Figure 9). Open source has run on a simple premise, providing shared building blocks to make all digital processes faster. However, the community-based trust model that open-source code sharing uses is increasingly being abused because developers "sit closest to credentials, tokens, and build systems", which hackers can exploit for their individual motives, be that geopolitical or financial.

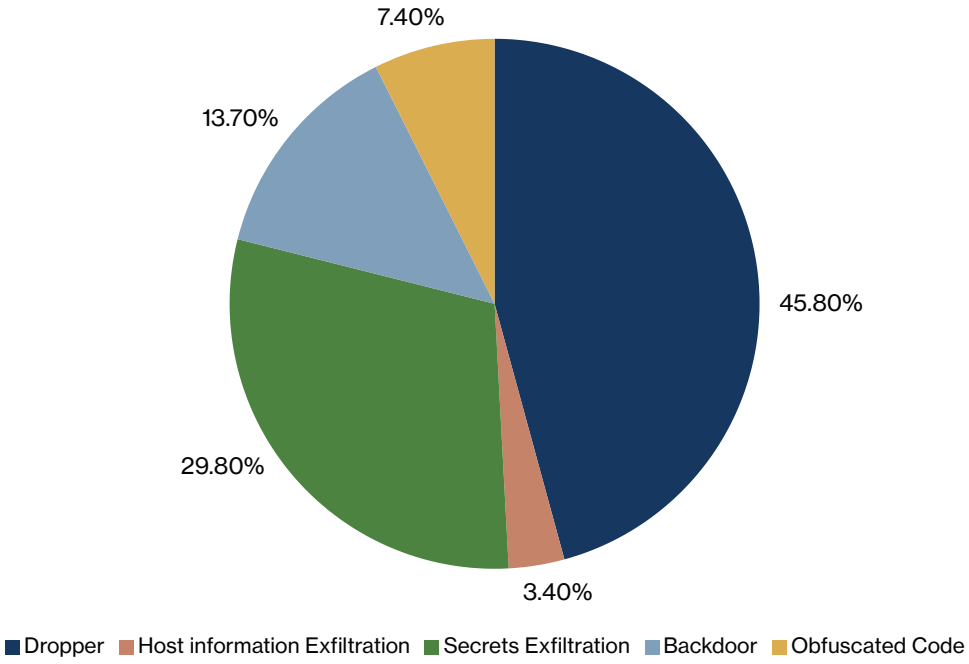
Figure 9: Annual Open-Source Malware Growth. Source: Sonatype



35 Saheed Oladimeji and Sean Michael Kerner, 'SolarWinds Hack Explained: Everything You Need to Know', Tech Target, 3 November 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

36 Maria Korolov, 'The List of Known SolarWinds Breach Victims Grows, as Do Attack Vectors', Data Center Knowledge, 23 December 2020, https://www.datacenterknowledge.com/data-breaches/the-list-of-known-solarwinds-breach-victims-grows-as-do-attack-vectors.

Figure 10: Typical Software Supply Chain Tactics used by Lazarus Group to Compromise Targets



For example, the North Korean Advanced Persistent Threat (APT) group Lazarus (which is a moniker used to refer to several North Korean hacking groups) exploits coders/developers' lax security practices to slip malicious code by audits through masquerading their code "packages" under "familiar names, ecosystems, add-ons, or configurations" to increase the likelihood that their malware will be downloaded and added to organisations' digital supply chain. Once downloaded, such code is used to carry out acts such as backdoor installations and data exfiltration, which are leveraged to advance Pyongyang's geopolitical ambitions.

Cyber-Physical Nexus: Cyberspace is Increasingly Being Used in Geopolitical Conflicts

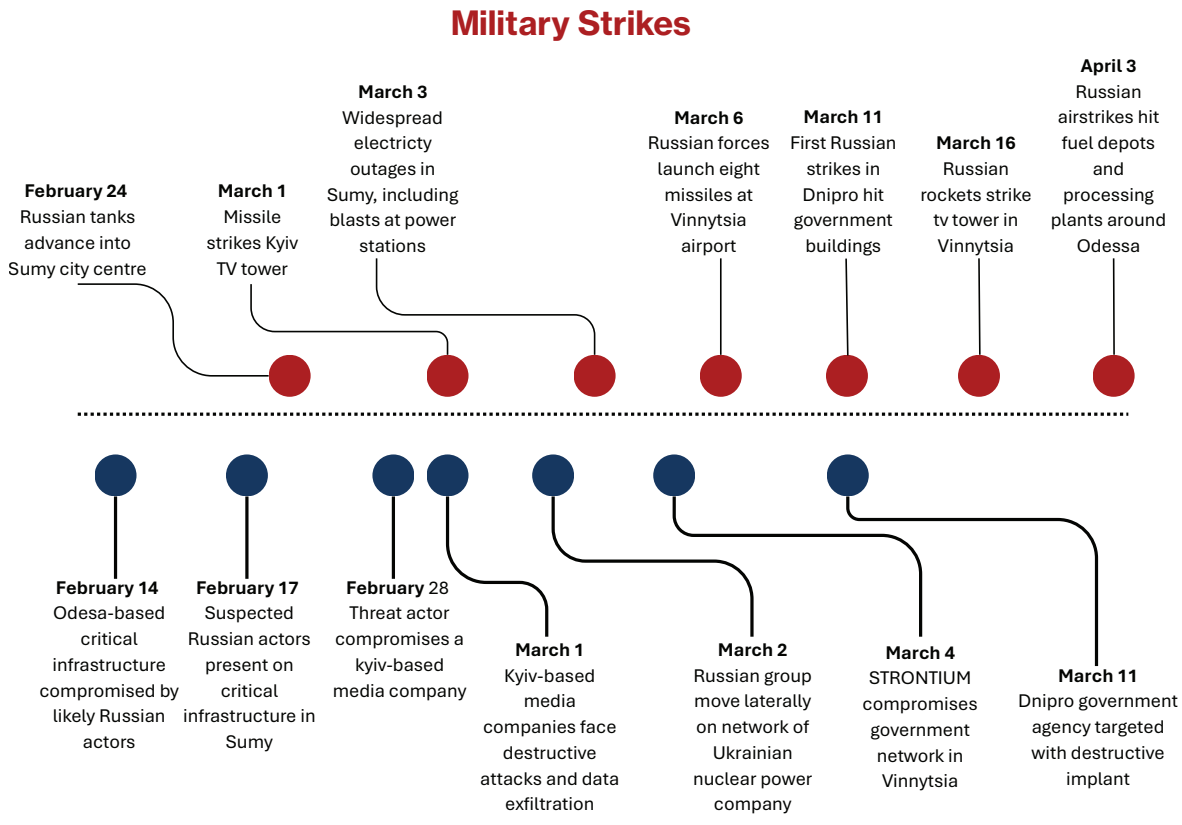
The aforementioned digitalisation trend and the growing use of IT services to maintain critical infrastructure have led malicious hackers to make little distinction between military and civilian targets, especially during geopolitical conflicts. This means that public or private industry organisations, particularly critical infrastructure operators, are at risk of being targeted via cyber means with kinetic impacts, e.g., aiding kinetic military operations, as part of pre-existing geopolitical conflicts. However, the intent of these cyber-physical operations serves three unique purposes: 1) ensuring that a "cold" conflict does not rise to the level of full-scale kinetic warfare, 2) acting as an enabler to increase the success rate of kinetic military operations, and 3) creating chaos and undermining trust between society, government, and the private sector.

With regard to the first category, the salient example can be seen in the long-standing and ongoing tit-for-tat cyber conflict (or shadow conflict) between Iran and Israel. Israel and Iran's state-directed and backed hackers regularly target their counterparts' critical infrastructure and military systems to cause disruptions or destruction without triggering a full-scale kinetic war. This tit-for-tat logic often intensifies a cycle of retaliation. For example, Iranian state-directed hackers reportedly targeted an Israeli water system in 2020, with the intent to cause

physical harm to the local population. This campaign attempted to "increase chlorine levels in the water flowing to residential areas", which could have led to hundreds of people getting sick and/or dying.[37] In response, Israeli hackers reportedly launched a cyberattack against Iran's Shahid Rajaee port in May 2020, resulting in significant economic damage by creating "massive backups on waterways and roads leading to the facility".[38]

In contrast, the secondary rationale of cyberattacks is best highlighted by the Russian operations against Ukraine during Moscow's 2022 invasion. According to Microsoft, which is directly involved in defending Ukraine's critical infrastructure against Russian cyberattacks, "Russia's use of cyberattacks appears to be strongly correlated and sometimes directly timed with its kinetic military operations targeting services and institutions crucial for civilians".[39] As shown in the timeline above, Russian hacking groups launched several cyberattacks against Ukraine's critical infrastructure operators just before a physical strike against key Ukrainian targets, with the aim of improving the physical operation's success rate.

Figure 11: Timeline of Russian Cyber-Military Strikes against Ukrainian Targets in 2022



37 TOI Staff, 'Iran Cyberattack on Israel's Water Supply Could Have Sickened Hundreds – Report', The Times of Israel, 1 June 2020, https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/.

38 Joby Warrick and Ellen Nakashima, 'Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility', The Washington Post, 18 May 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

39 Tom Burt, 'The Hybrid War in Ukraine', Microsoft, 27 April 2022, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.

Conclusion

The cyber threat landscape is highly diverse, but its impacts are uneven. Exposure is typically higher in more digitally advanced and wealthier regions, yet greater exposure does not necessarily imply stronger resilience. Financial capacity plays a key role: larger organisations can generally absorb cybersecurity costs, whereas SMEs face structural disadvantages and often cannot access adequate protection through commercial services alone.

These disparities, geographic exposure, economic vulnerability, increasing threat sophistication, and the growing link between cyber and geopolitics, form the basis of this report's analysis. Cyber threats must now be understood not only in technical terms, but also in broader societal and physical contexts. As both large enterprises and SMEs are pushed to strengthen resilience, often beyond their means, a structural gap emerges. This creates a critical role for non-profit organisations in helping to bridge cybersecurity capacity gaps where they are most needed.

The cyber threat landscape is highly diverse, but its impacts are uneven. Exposure is typically higher in more digitally advanced and wealthier regions, yet greater exposure does not necessarily imply stronger resilience.

Chapter 4: Inventorisation and Assessment of Non-Profit Cybersecurity Services

Services Provided by Non-Profit Cybersecurity Organisations

Cybersecurity is commonly understood through two institutional lenses: the private firms that design, sell, and operate protective technologies and services, and the government bodies that regulate, coordinate, and defend national digital infrastructure. But between and around these two sectors sits a large and often underappreciated non-profit sector doing work that neither commercial nor state actors are well-positioned to do. Any serious effort to determine the value of cybersecurity non-profits requires, first, a clear picture of who these organisations are and what services they provide.

The services provided by the organisation we interviewed group into five broad categories: 1) the collection and distribution of threat intelligence; 2) the coordination of incident response; 3) the development of standards, benchmarks, and accreditation frameworks; 4) capacity building and technical assistance for organisations below the cyber poverty line; and 5) digital security support for at-risk communities and civil society. Further categories capture organisations whose mandates cut across several of these at once. These categories are analytical, not watertight: several of the organisations below operate in more than one category, and the line between, for example, capacity building and the dissemination of standards, proves to be blurry in practice.

The 11 organisations discussed in the sections that follow were selected because we were able to interview them, and they are not meant to represent the sector as a whole. They skew toward those with established track records, public profiles, and the capacity to engage with an external research project; smaller, newer, and regionally focused organisations are underrepresented. The list should therefore be read as illustrative rather than exhaustive. In the same vein, there is significant diversity in the type of models and services provided by these organisations, even within the same categories. This diversity is also highlighted by the organisations selected.

Threat Intelligence Collection and Sharing

Threat intelligence, the collection, processing, and analysis of data to understand a threat actor's motives, targets, and attack methods, is key to effective cyber defence.[40] As outlined in Chapter 3, the disparity in cyber resilience between larger organisations and SMEs is largely driven by budget constraints, leaving smaller entities ill-equipped to anticipate sophisticated threats such as ransomware or software supply chain attacks. Yet in commercial and governmental contexts, threat intelligence is frequently treated as a proprietary or classified asset. Commercial threat intelligence products can cost upwards of tens of thousands of dollars annually,[41] placing them far beyond the reach of smaller organisations, national Computer Emergency Response Teams (CERTs) in developing economies, or public sector bodies with constrained budgets. Therefore, some non-profit organisations collect intelligence at scale and distribute it freely.

The ***Shadowserver Foundation***, founded in 2004 in California by a group of security professionals operating initially as volunteers, is one of the largest organisations working in this space. Registered as a public benefit non-profit in both the United States (as a 501(c)(3)) and the Netherlands,[42] Shadowserver runs one of the world's most extensive internet monitoring infrastructures, scanning every publicly reachable address on the internet 148 times per day.[43] Across 90 countries, it also operates honeypots (decoy systems designed to attract and observe attackers) and sinkholes (servers that intercept traffic destined for malicious infrastructure).[44] Each day, this infrastructure ingests and analyses over 1.1 million malware samples.[45]

In an interview, Shadowserver stressed that its intelligence is operationally specific by design: rather than profiling threat actors or producing strategic assessments, it tells subscribers what is happening on their own networks (e.g. compromises, vulnerabilities, malware infections, and infrastructure abuse visible from the outside) and sends close to one billion such events every day.[46] The Foundation also quickly tracks newly exploited vulnerabilities. In some cases, data on affected devices reaches subscribers globally within 24 hours of a vulnerability being published.[47]

Shadowserver distributes up to 76 different report types daily to over 10,000 subscribing organisations, including 201 national CERTs, entirely free of charge.[48] In an interview, Shadowserver noted that recipients include CISA in the United States, the NCSC in the United Kingdom, the BSI in Germany, ANSSI in France, and the CCB in Belgium, as well as telecoms, hospitals, universities, and critical infrastructure operators.[49] Several governments, including the UK and Germany, use Shadowserver data to run their own domestic early

40 Kurt Baker, 'Cyber Threat Intelligence Explained', CrowdStrike, 4 March 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/.

41 Zvelo, 'In-House Cyber Threat Intelligence Begs a Multi-Million Dollar Question', 12 July 2022, https://zvelo.com/in-house-cyber-threat-intelligence-begs-a-multi-million-dollar-question/.

42 This is a US-based non-profit entity exempt from federal income tax under section 501(c)(3) of the Internal Revenue Code.

43 Shadowserver Foundation, 'What We Do', 2026, https://www.shadowserver.org/what-we-do/.

44 Shadowserver Foundation, 'Data Collection', 2026, https://www.shadowserver.org/what-we-do/data-collection/.

45 Shadowserver Foundation, 'What We Do'.

46 Shadowserver Foundation, 'Interview between Shadowserver Foundation and HCSS', 5 March 2026.

47 Shadowserver Foundation.

48 Shadowserver Foundation.

49 Shadowserver Foundation.

warning systems, through which they push intelligence to subscribing organisations locally.[50] The Foundation also partners with law enforcement agencies and has supported major operations, including the disruption of the Qakbot and GRU-controlled Moobot botnets.[51]

Meanwhile, the ***Cyber Threat Alliance*** (CTA) runs a different model. Founded in 2014 by Fortinet, McAfee, Palo Alto Networks, and Symantec, the Alliance's non-profit structure is the neutral ground that allows 38 private-sector members, who are otherwise commercial competitors, to share threat data with one another.[52] Members contribute between 500,000 and 600,000 data points per day: digital fingerprints of malicious files, suspicious network traffic patterns, infected machine characteristics, and email markers, each stamped with when it was seen, how it fits into an attack, and how widespread it appears to be. Such information is collated and distributed in various ways, including through the MITRE ATT&CK framework.[53]

In an interview, CTA was direct about who this intelligence is for: it stays within the membership, and access to the shared pool is a primary reason to join.[54] Moreover, by not commercialising this deep reservoir of intelligence, CTA is able to maintain its neutral party status and provide a platform for major for-profit organisations to better protect their clientele, which includes major and minor organisations, across the globe.

Building the legal and governance structure to make competitors share sensitive data was, in the words of CTA in an interview, considerably harder than building the technology: roughly two years and two million dollars, against two to three months and a quarter of a million for the platform itself.[55] The model runs on strict neutrality: anything about the bad actors is fair game; pricing, product plans, and the like are off limits, as is membership for anyone on a major sanctions list, including organisations in countries such as Russia.

Incident Response Coordination

When significant cyber incidents occur, whether ransomware campaigns against critical infrastructure, large-scale data breaches, or coordinated attacks spanning multiple sectors and jurisdictions, effective response requires coordination across organisational and national boundaries. As Chapter 3 illustrated through the SolarWinds incident, a single software supply chain compromise can cascade to more than 30,000 public- and private-sector clients worldwide, spanning government agencies and major corporations across jurisdictions. Non-profit organisations are particularly well positioned to provide incident response coordination, given their ability to operate across sectors and jurisdictions without the competitive constraints that affect commercial actors or the sovereign limitations that apply to government agencies. A list of non-profits that conduct such services includes:

FIRST, or the Forum of Incident Response and Security Teams, was founded in 1990 in the immediate aftermath of the Morris Worm of November 1988, which affected major portions

50 Shadowserver Foundation.

51 Shadowserver Foundation, 'Qakbot Botnet Disruption', 29 August 2023, https://www.shadowserver.org/news/qakbot-botnet-disruption/; Shadowserver Foundation, 'Shadowserver 2024: Highlights of the Year in Review', https://www.shadowserver.org/news/shadowserver-2024-highlights-of-the-year-in-review/.

52 Cyber Threat Alliance, 'Our Sharing Model', https://www.cyberthreatalliance.org/about/our-sharing-model/; Cyber Threat Alliance, 'Membership', 2026, https://www.cyberthreatalliance.org/membership/.

53 Cyber Threat Alliance, 'Interview between Cyber Threat Alliance and HCSS', 5 March 2026.

54 Cyber Threat Alliance.

55 Cyber Threat Alliance.

of the early internet and revealed that incident response was "isolated and uncoordinated, resulting in much duplicated effort, and in conflicting solutions."[56] FIRST was established to provide the trusted relationships, shared protocols and language, and communication channels that cross-border incident response requires. Today, FIRST brings together over 820 member teams across more than 110 countries from government, private sector, and academic institutions.[57]

FIRST's contributions extend well beyond bringing together incident response and security teams. It has developed and maintains some of the most widely adopted technical standards in the incident response field, including the Common Vulnerability Scoring System (CVSS) for vulnerability severity ratings;[58] the Traffic Light Protocol (TLP), a standard for classifying sensitive information for sharing;[59] and the Exploit Prediction Scoring System (EPSS).[60] Meanwhile, its Computer Security Incident Response Team and Product Security Incident Response Team Services Frameworks define how incident response teams may be organised and operate.[61] FIRST also provides training with the goal of supporting new and current CSIRTs and raising awareness and understanding of incident response.[62]

Non-profit organisations working in this space produce the reference materials, quality assurance mechanisms, and foundational code that shape how cybersecurity is practised across the ecosystem.

Standards, Benchmarking, Accreditation, and Protocols

A third domain of non-profit activity involves the development, maintenance, and dissemination of technical standards, security configuration benchmarks, professional accreditation frameworks; and the open-source software that implements the protocols the internet runs on. Chapter 3 showed that cloud and AI adoption have widened the attack surface available to threat actors. Consistent baseline configurations and shared technical reference points are therefore prerequisites, not optional layers. Non-profit organisations working in this space produce the reference materials, quality assurance mechanisms, and foundational code that shape how cybersecurity is practised across the ecosystem. In addition to the aforementioned **FIRST**, this category includes:

The ***Center for Internet Security*** (CIS), founded in October 2000 in New York, sits in this space. CIS produces two widely adopted free security references: the *CIS Controls*, a prescriptive, prioritised set of 18 cybersecurity best practices designed to mitigate the most common cyber threats.[63] Meanwhile, *CIS Benchmark* entails consensus-based configuration recommendations for securing specific IT systems.[64] In an interview, CIS was direct about where it fits in the standards landscape. Exhaustive catalogues such as ISO 27001 or NIST 853 list every control an organisation could consider, leaving enterprises to choose based on

56 Forum of Incident Response and Security Teams, 'FIRST History', 2026, https://www.first.org/about/history.

57 Forum of Incident Response and Security Teams, 'FIRST Reports Record Growth and Expanding Global Impact', 2026, https://www.first.org/newsroom/releases/20251210.

58 Forum of Incident Response and Security Teams, 'Common Vulnerability Scoring System SIG', 2026, https://www.first.org/cvss/.

59 Forum of Incident Response and Security Teams, 'Traffic Light Protocol (TLP)', 2026, https://www.first.org/tlp/.

60 Forum of Incident Response and Security Teams, 'Exploit Prediction Scoring System', 2026, https://www.first.org/epss/.

61 Forum of Incident Response and Security Teams, 'FIRST Services Framework', 2026, https://www.first.org/standards/frameworks/.

62 Forum of Incident Response and Security Teams, 'FIRST Trainings', 2026, https://www.first.org/education/first-training.

63 Center for Internet Security, 'CIS Controls', 2026, https://www.cisecurity.org/controls/.

64 Center for Internet Security, 'CIS Benchmarks', 2026, https://www.cisecurity.org/cis-benchmarks/.

their own risk appetite.[65] CIS's view is that this is a failed model.[66] Instead, it maps common attack classes utilising the MITRE ATT&CK framework and converts them into specific prescriptive actions, such as "mitigate here, block here, prevent here".[67]

CIS also operates the Multi-State Information Sharing and Analysis Center (MS-ISAC), the only ISAC dedicated solely to U.S. state, local, tribal, and territorial governments, schools, and election offices.[68] In an interview, CIS described it as a watch centre that pulls together, analyses, and shares anything relevant across its membership.[69]

CREST, founded in the United Kingdom in 2006, tackles a related but distinct problem. Where CIS tells organisations how to secure their own systems, CREST quality-assures the companies and individuals hired to do security work on their behalf. As a not-for-profit accreditation body, CREST sets quality standards for cybersecurity service providers, assesses them against those standards, and gives buyers a basis for confidence in who they hire.[70] It accredits over 500 member companies and has certified 6,000 individual cybersecurity professionals.[71] In an interview, CREST claimed that in a market where any firm could claim expertise in penetration testing or incident response, buyers had no independent way to evaluate those claims.[72] A body that awarded a quality mark to providers who met the standard and withheld it from those who did not gave buyers something to go on. In an interview, CREST noted that its penetration testing standard is, as far as it knows, the only global standard for quality in that service area, and its incident response standard is the only independent one.[73]

Organisations with limited resources, technical expertise, or institutional infrastructure lack the knowledge, skills, and tools needed to protect themselves against even basic threats.

For providers not yet ready for full accreditation, CREST developed a Pathway to Accreditation: a structured route that starts with a commitment to a set of ethical principles, moves through self-assessment, and provides preparatory material along the way, replacing what had previously been a binary pass-or-fail system.[74] CREST is self-funded through member subscriptions on a cost-recovery basis and takes no donor or government money for its core functions (e.g., the development of its standards or certifications).[75] CREST does, however, have government-initiated projects that receive government support.

Capacity Building and Technical Assistance

Organisations with limited resources, technical expertise, or institutional infrastructure lack the knowledge, skills, and tools needed to protect themselves against even basic threats. Chapter 3 demonstrated that this capacity deficit is most acute among SMEs, where 35% of security personnel in 2025 believed their cyber resilience was insufficient to address the threats they faced, up from just 5% in 2022, a trajectory that runs directly opposite to that of larger organisations. In a fourth domain, non-profit organisations address this capacity deficit

65 Center for Internet Security, 'Interview between Center for Internet Security and HCSS', 4 March 2026.

66 Center for Internet Security.

67 Center for Internet Security.

68 Center for Internet Security, 'MS-ISAC', 2026, https://www.cisecurity.org/ms-isac.

69 Center for Internet Security, 'Interview between Center for Internet Security and HCSS'.

70 CREST, 'Who Is CREST?', CREST, 2026, https://www.crest-approved.org/about-us/who-is-crest/; CREST, 'Interview between CREST and HCSS', 3 March 2026.

71 CREST, 'What We Do', 2026, https://www.crest-approved.org/about-us/what-we-do/.

72 CREST, 'Interview between CREST and HCSS'.

73 CREST.

74 CREST.

75 CREST.

through training, technical assistance, tool development, and the provision of free resources for organisations below the cyber poverty line.

The ***Cyber Readiness Institute*** (CRI), launched in July 2017, takes a narrower and more targeted approach. Its premise is that the biggest vulnerability in global supply chains is not large enterprises, which typically have the resources for sophisticated security programmes, but small and medium-sized businesses.[76] CRI's free, self-paced online programme covers four areas: multifactor authentication and passwords, software updates, phishing awareness, and secure storage and sharing.[77] In an interview, CRI explained what sets it apart: the focus is on human behaviour and internal policy, not technology.[78] Organisations buy tools, and then a person makes an error. CRI's program designates a cyber leader within an organisation to raise standards among other staff.[79]

Though designed for SMBs, CRI noted in an interview that the programme has found traction with large manufacturers with thousands of employees and government ministries in developing countries.[80] Trust in this programme is built on how the programme is funded and structured. Backing from Mastercard, Microsoft, T-Mobile, and ExxonMobil, rather than the US government, matters in regions where a government-affiliated programme would meet resistance, according to CRI.[81] Local coaches matter too; when CRI used US-based coaches abroad, the cultural gap showed in completion rates. Shifting to local coaches trained in the CRI method made a measurable difference.[82]

Digital Security Support for At-Risk Communities and Civil Society

Civil society organisations, journalists, human rights defenders, political dissidents, and minority communities that face targeted surveillance or attacks by state-sponsored actors cannot realistically or consistently turn to commercial cybersecurity firms or government cybersecurity agencies, which may be neutral at best and hostile at worst. At the same time, they face the same threats as governments and large corporations, yet are equipped with even fewer resources to protect themselves.[83] These groups thus depend disproportionately on dedicated non-profit organisations for their digital security. This list includes:

Access Now, founded in July 2009 in response to digital repression during Iran's contested presidential election, provides an assistance programme for at-risk communities.[84] Its Digital Security Helpline operates as a free 24/7 service in ten languages, providing real-time technical assistance to civil society organisations, activists, journalists, and human rights defenders worldwide.[85] In an interview, Access Now described the helpline as handling

76 Cyber Readiness Institute, 'Interview between Cyber Readiness Institute and HCSS', 19 March 2026.

77 Cyber Readiness Institute, *Cyber Readiness Program*, 2026, https://cyberreadinessinstitute.org/cyber-readiness-program/.

78 Cyber Readiness Institute, 'Interview between Cyber Readiness Institute and HCSS'.

79 Cyber Readiness Institute, 'The Cyber Leader Certification Program', 2026, https://cyberreadinessinstitute.org/cyber-leader-certification-program/.

80 Cyber Readiness Institute, 'Interview between Cyber Readiness Institute and HCSS'.

81 Cyber Readiness Institute.

82 Cyber Readiness Institute.

83 Munk School of Global Affairs & Public Policy, *Communities @ Risk: Targeted Digital Threats Against Civil Society* (2014), 2, https://citizenlab.ca/wp-content/uploads/2025/12/2-Extended-Analysis-Full.pdf.

84 Access Now, 'About Us', Access Now, 2026, https://www.accessnow.org/about-us/.

85 Access Now, 'Digital Security Helpline', Access Now, 2026, https://www.accessnow.org/help/.

both preventative work (such as device hardening, secure communications, organisational security reviews) and reactive response.[86] Spyware cases are handled in high volume, and many move beyond purely technical remediation into legal support and litigation because they do not remain purely technical.[87] Access Now's advocacy has had some commercial platform-level results as well. According to the organisation, talks with Apple, Google, and WhatsApp contributed to Apple's Lockdown Mode, Google's Advanced Protection Programme for Android, and new protective features in WhatsApp.[88]

Beyond the Helpline, Access Now runs RightsCon, described as the world's leading summit on human rights in the digital age, provides funding to grassroots organisations, and leads the #KeepItOn coalition of 345+ organisations fighting internet shutdowns globally.[89] Their monitoring and advocacy help prevent or shorten internet shutdowns.

The ***CyberPeace Institute***, founded in September 2019 in Geneva with the support of Microsoft, Mastercard, and the William and Flora Hewlett Foundation, approaches the same broad challenge from a different angle. In an interview, the Institute described its work as organised around two pillars: one hands-on, one systemic.[90] The first is the CyberPeace Builders programme, which connects over 1,600 corporate volunteers from 456 companies with more than 600 non-profits globally, providing free cybersecurity assistance tools, knowledge, and workforce.[91] The Institute was direct about why this model works: cybersecurity companies volunteer because they know they are not giving up any commercial market, and NGOs simply cannot pay or attract cyber talent through normal mechanisms.[92] The second pillar is analytical: aggregating structured and unstructured data, along with open-source intelligence, to document the human impact of cyberattacks.[93] In an interview, the Institute noted the pillars are paired so that one secures organisations one at a time, the other builds the systemic picture needed to influence policy.[94]

Some of the most structurally significant actors in this space derive their value from breadth.

Organisations with Broader Mandates

Not all non-profit cybersecurity organisations fit neatly into one service category. Some of the most structurally significant actors in this space derive their value from breadth. For example, their role is to convene, coordinate, and enable activity across multiple functions, rather than to deliver a single specialised service. This breadth mirrors the expansive global cyber threat landscape set out in Chapter 3.

The ***Global Cyber Alliance*** (GCA), founded in 2015 by the Center for Internet Security, the Manhattan District Attorney's Office, and the City of London Police, works across threat intelligence, capacity building, and standards implementation. Its best-known technical product is Quad9, a free, privacy-preserving DNS resolver launched in November 2017 that now blocks an average of more than 670 million threats per day in more than 130 countries.[95] In

86 AccessNow, 'Interview between AccessNow and HCSS', 6 March 2026.
87 AccessNow.
88 AccessNow.
89 Access Now, 'About Us'.
90 CyberPeace Institute, 'Interview between CyberPeace Institute and HCSS', 16 March 2026.
91 CyberPeace Institute.
92 CyberPeace Institute.
93 CyberPeace Institute.
94 CyberPeace Institute.
95 Global Cyber Alliance, 'Quad9', 2026, https://globalcyberalliance.org/work/quad9/.

2021, Quad9 became an independent non-profit based in Switzerland. GCA's Cybersecurity Toolkits, built around CIS Controls and aligned with UK NCSC Cyber Essentials and Australia's Essential Eight, have drawn over 2 million visitors since launch; they target small businesses, election offices, journalists, individuals, and non-profits that commercial security vendors rarely serve. In an interview, GCA described its work as approaching the problem from both the infrastructure side and the end-user side.[96] On the infrastructure side, this includes MANRS, which now encourages routing security norms across more than 1,300 network operators worldwide, and Domain Trust, which facilitates the sharing of known malicious domain data with registrars and registries.[97] On the end-user side, the toolkits go a step beyond awareness training by pointing users to curated, vetted free tools they can actually install, on the basis that, as GCA put it, even cybersecurity experts will click the wrong link eventually.[98]

The ***Institute for Security and Technology*** (IST) is a non-profit in the San Francisco Bay Area. Similarly, as GCA, it does not fit primarily into one service category: its work runs from policy analysis and multi-stakeholder convening to developing incident reporting frameworks and defence blueprints. It organises this across three pillars: a Policy Lab, Tech Works, and a Network for Global Security.[99] IST does not just address cybersecurity, but a range of emerging global security issues, such as information warfare, nuclear security, and artificial intelligence.[100]

In the cybersecurity realm, one of its most prominent programmes is the Ransomware Task Force. It brought together sixty organisations from government, industry, law enforcement, and civil society, produced forty-eight recommendations, and then tracked implementation over three years.[101] IST reported progress on ninety to ninety-two percent of the recommendations across its 2022, 2023, and 2024 reports.[102] The outcomes it traces to that work include mandatory incident reporting under CIRCIA, the Joint Ransomware Task Force at CISA, and Treasury guidance on the legality of ransom payments.[103] In an interview, IST was direct about where it sits: non-profits do what government cannot and industry will not, because most of the necessary work in cybersecurity has no straightforward commercial model.[104] Its constituency spans small- and medium-sized businesses, civil society organisations, critical infrastructure operators, governments and their agencies, law enforcement, and industry partners.[105]

Foundational Support

The final category of NPO services can be most accurately described as the foundational support grouping. Indeed, this grouping, unlike the others, does not provide traditional cybersecurity services such as threat intelligence or incident response. Instead, this grouping

96 Global Cyber Alliance, 'Interview between Global Cyber Alliance and HCSS', 23 April 2026.

97 Global Cyber Alliance.

98 Global Cyber Alliance.

99 Cybil, 'Institute for Security and Technology (IST)', 2026, https://cybilportal.org/actors/institute-for-security-and-technology-ist/.

100 Cybil.

101 Institute for Security and Technology, 'Interview between Institute for Security and Technology and HCSS', 11 March 2026.

102 Institute for Security and Technology.

103 Institute for Security and Technology.

104 Institute for Security and Technology.

105 Institute for Security and Technology.

provides a service that underpins the entire non-profit cybersecurity ecosystem. A prime example of such a service is the one provided by the NPO NLnet Labs.

NLnet Labs is a Dutch non-profit foundation established in 1999 that works at a lower layer of the stack than most organisations in this chapter. Rather than telling organisations how to secure their systems or quality-assuring the work of those hired to test them, NLnet Labs writes and maintains the open-source software that implements the protocols the internet runs on. Its "products" include NSD (Name Server Daemon), software that answers authoritative questions about who owns a domain, Unbound (software that looks up and caches those answers on behalf of users), and Routinator (software that checks whether internet traffic is coming from where it claims to). These are deployed across the entire internet hierarchy, from the root servers and country-level domain registries at the top, down to the home routers that ordinary consumers plug in and forget about.[106]

In an interview, NLnet Labs noted that roughly half of the 12 operators running the 13 DNS root letters use NSD, and that several of the world's largest cloud providers run Unbound.[107] Moreover, the organisation holds roughly 80% of the RPKI validator market through products like Routinator, a concentration that NLnet Labs finds uncomfortable.[108] They would rather see three or four high-quality implementations to choose from.[109]

All software is distributed for free. Revenue comes from support contracts with operators who want early notification of security issues and access to bug fixes. NLnet Lab claims this is less a product subscription than a mechanism to sustain infrastructure maintenance, with no meaningful commercial successor.[110] NLnet Labs also participates in the Internet Engineering Task Force, has co-authored standards on routing, and in an interview described its role there as representing the public interest in a forum where commercial actors dominate.[111]

The five pillars are the operational services non-profits provide, each addressing failure in the commercial and governmental cybersecurity ecosystem.

Conclusion

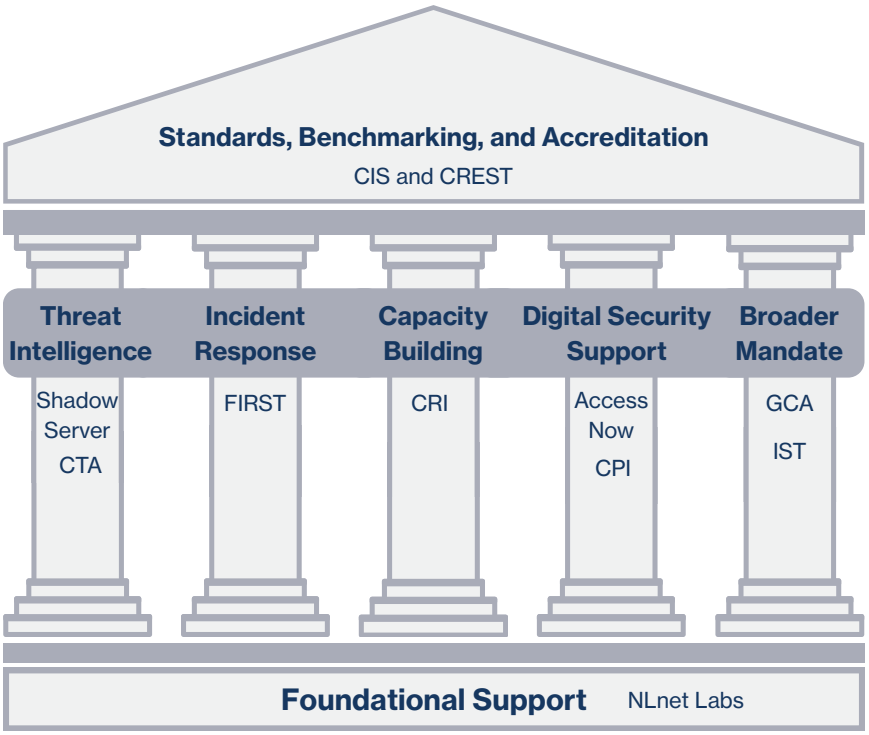
The categories set out above do not exist independently of each other. They form a layered architecture, represented in Figure 12 below as a classical portico: five functional pillars supported by a common foundation and topped by a shared roof. Together, they structure the non-profit cybersecurity ecosystem.

The five pillars (threat intelligence, incident response, capacity building, digital security support, and broader mandate) are the operational services non-profits provide, each addressing failure in the commercial and governmental cybersecurity ecosystem.

Threat intelligence closes the information gap for organisations that cannot afford commercial feeds. Incident response coordinates action across the jurisdictional and sectoral lines that individual governments and firms cannot easily cross. Capacity building raises the floor for organisations below the cyber poverty line. Digital security support reaches the civil society actors who neither the market nor the state is structurally positioned to protect.

106 NLnet Labs, 'Interview between NLnet Labs and HCSS', 2 March 2026.
107 NLnet Labs.
108 NLnet Labs.
109 NLnet Labs.
110 NLnet Labs.
111 NLnet Labs.

Figure 12: The Portico depiction of the non-profit cybersecurity ecosystem and how they interconnect.



The pillars also reinforce one another in practice. Threat intelligence feeds incident response. For example, Shadowserver's daily reports provide data that national CERTs need to act on unfolding incidents, and FIRST's community, in turn, can generate the operational experience that shapes how threat intelligence is scoped. Incident response reveals predictable phishing vectors, which capacity-building programmes like CRI's can then translate into training. Meanwhile, capacity building raises the baseline at which targeted digital security support becomes practical, and those within the broader mandate pillar fill any remaining service gaps. This interconnected nature ensures that an NGO that already follows basic cybersecurity practices is better positioned to be supported against a more sophisticated adversary by NPOs such as Access Now or the CyberPeace Institute. Some NPOs also provide services across multiple pillars. As such, the groupings shown in Figure 12 should be seen as illustrative examples of what each pillar entails, rather than as an exclusive categorisation of where these NPOs belong within the global cyber ecosystem.

Underneath sits the foundational layer, represented here by NLnet Labs, which develops and maintains the open-source implementations of the DNS and routing protocols that the pillars above depend on. Above sits the roof: the standards, benchmarks, and accreditation frameworks that give the whole structure coherence, allowing intelligence to be exchanged in common formats, response teams to be measured against a recognisable quality bar, and training and user-support programmes to align with tested practice.

Given this context, the non-profit cybersecurity sector should not be seen as a collection of individual initiatives but an ecosystem whose resilience depends on all its layers being adequately resourced. The next chapter takes up the question of the value this non-profit ecosystem provides, examining the economic and social value it generates for the users, sectors, and societies they serve.

Chapter 5: Counterfactual Assessment: The Economic and Social Value Generated by Non-profits

The internet economy generates trillions of dollars of value annually.[112] As highlighted in the previous chapter, much of the infrastructure that keeps it secure and functioning is maintained by non-profits that provide their services at no cost. This chapter aims to establish the economic and social value of non-profit cybersecurity organisations. While this value can be understood holistically, it is often difficult to quantify because their services are frequently offered for free or at below-market rates.

To address this, the chapter presents an approach for estimating value ranges, particularly in economic terms. These estimates are based on interviews with organisations and draw on company data, illustrative examples, and publicly available information. They are not intended to be exhaustive, but rather to provide a generalised overview of the types of value these non-profits generate.

The analysis focuses on a subset of organisations rather than the entire sector. As such, the total value of the broader non-profit cybersecurity ecosystem is likely to be significantly higher. The values presented here are at the lower end and should be considered incomplete and conservative estimates of the actual value generated by these organisations.

In order to estimate the economic value that non-profit cybersecurity companies generate, this study employs a set of value calculations, organised into three main value categories:

1. **Market equivalent value**: the cost of services delivered in the for-profit sphere.
2. **Cost avoided value**: the decrease in an organisation's losses due to a non-profit organisation's intervention.
3. **Facilitated value**: the economic value generated through services underpinned by the non-profit sector.

[112] 'Global Digital Economy Report (2025) | IDCA', accessed 16 April 2026, https://www.idc-a.org/insights/qUi9XgvyrzSkyDUy9Tqr.

This chapter starts by outlining examples for each cost calculation method. The examples are grouped based on the type of service provided, as established in Chapter 4. After this, a final assessment of the value generated will be provided, and the broader implications of these findings will be outlined.

Table 2: Overview of Value Estimates of Case Studies by Value Category

	Value Estimation Method		
Cybersecurity Domain	**Market Equivalent Value**	**Cost Avoided Value**	**Facilitated/Supported Value**
Foundational Support	USD 10–13M (NLnet Labs)	USD 1–10B (NLnet Labs, GCA)	USD 150–800B (NLnet Labs, GCA)
Threat Intelligence	USD 830M–980M (ShadowServer)		USD 14.6B (CTA)
Incident Response		USD 800M–1.2B (CTA)	
Capacity Building	USD 17.5M (CRI)		FIRST (see breakdown on page 37)
Digital Security Support	USD 15M (Access Now), USD 1.9M–6.4M (CPI)	USD 1.23B (Access Now)	
Broader Mandate		USD 2.3M (IST)	
Standards, Benchmarks and Accreditation	USD 354M (CIS) USD 78M (CREST)		

Table 2 provides an overview of examples of economic value calculations gathered through desk research and interviews. Together, they represent several billion dollars of economic value generated, derived from different calculation methods. Non-profits can generate economic value across calculation methods, such as NLnet Labs and Access Now, both spanning more than one category. The total value should therefore be considered indicative rather than precise. The section below describes the calculations and the rationale behind our findings for the three value estimation methods.

Market Equivalent Value

Market Equivalent value assesses the services these non-profits provide and what it would cost to replace them on a one-to-one basis at market rates. This can take the form of the amount of code required to write, as well as the costs of rebuilding a platform or a standard. Moreover, non-profits often provide services at no cost or drastically reduced costs compared to market alternatives. The economic value provided can thus be inferred from prevailing market rates. These estimates provide insight into the value these organisations deliver and the costs companies would incur if they sourced the same services from a commercial party.

Rebuilding platforms

Reconstructing NLnet Labs' software from scratch would require substantial investment even before accounting for the institutional capital that has been built up over the years.

Building and nurturing digital platforms and services often requires considerable time and effort. The services delivered by organisations such as NLnet Labs are a key example of critical infrastructure in the digital domain. NLnet Labs builds and maintains the core software that keeps the internet's address book (Domain Name System) working. Its tools handle how domain names get looked up (NSD and Unbound) and how internet traffic gets routed safely to the right destination (RPKI).[113] All of it is free and open source. According to NLnet Labs, half of the 12 operators translating domain names into addresses use NSD.[114] Several operators have reportedly concluded it is cheaper to contribute code back to NLnet Labs than to copy it and build their own version.[115]

Reconstructing NLnet Labs' software from scratch would require substantial investment even before accounting for the institutional capital that has been built up over the years. Applying the COCOMO II embedded-systems mode calculation (the appropriate standard for security-critical, constrained network software) to the approximately 324,000 source lines of code across NSD, Unbound, and Routinator yields a codebase reconstruction cost of 10-13 million euros (USD 11.7 – 15.3 million) at Amsterdam senior-engineer consultancy rates (150 euros per hour).[116] That figure covers code alone. Other costs, including personnel and maintenance, increase the total cost.

Organisations that provide security and threat services would also be costly to rebuild. For example, the Center for Internet Security (CIS) runs the Security Operations Centre (SOC) for U.S. state, local, tribal and territorial governments. These governments include roughly 50 states, more than 3,000 counties, approximately 19,000 municipalities, and hundreds of tribal and territorial entities. All these organisations receive IT-system monitoring and threat detection from CIS through the Multi-State Information Sharing and Analysis Centre (MS-ISAC). Without CIS, these organisations would have to use market alternatives. Using a very conservative assumption that the MS-ISAC substitutes for only 500 outsourced, mid-sized SOCs, and applying the average market cost of USD 220,000 per SOC per year

113 RPKI provides a verification and authentication framework to secure routing on the Internet, adapting and specifying the fundamentals of a conventional Public Key Infrastructure (PKI) to address specific security issues.

114 NLnet Labs.

115 NLnet Labs.

116 Lucas Pereira dos Santos and Maurício Ferreira, 'Applying COCOMO II for a DO-178C Safety-Critical Software Effort Estimation', *Journal of Aerospace Technology and Management* 11 (2019): e1819, https://doi.org/10.5028/jatm.v11.1031.
'COCOMO II - Constructive Cost Model', accessed 15 April 2026, https://softwarecost.org/tools/COCOMO/.

for a medium-sized enterprise, the service CIS provides represents at least **USD 110 million** in avoided annual security costs.[117]

Developing effective standards can also deliver substantial economic value that is not easily replicated. For example, CREST has created a regulatory framework for assessing the quality of cybersecurity organisations and has made it freely available. Governments that want to regulate the quality of cybersecurity services could either develop their own national quality standard or adopt an existing one, such as CREST's. Assuming building such a standard takes one year, based on the development of the Cybersecurity Framework by the National Institute for Standards and Technology, and a consultancy rate of 150 euros per hour with a team of 15 specialists, this would cost USD 3.9 million.[118]

Across 20 jurisdictions, the implied avoided cost to governments would be USD 78 million, delivered by a non-profit that makes its standards publicly available for free.

CREST's standards are now embedded in the regulatory frameworks of at least 20 jurisdictions, including the UK, the EU through DORA, Australia, Singapore, and countries in the Middle East and Africa. Across 20 jurisdictions, the implied avoided cost to governments would be USD 78 million, delivered by a non-profit that makes its standards publicly available for free. Again, building such a standard could take longer or require more labour, potentially increasing the total value to over USD 100 million.

These examples illustrate that rebuilding infrastructure now provided by non-profits would cost governments and organisations hundreds of millions of dollars. The next section examines the value generated by benchmarking services against market rates.

Provision of free or discounted services

Non-profit cybersecurity organisations frequently deliver services either free of charge or at heavily discounted rates, particularly to public-interest and under-resourced communities. As a result, the prices paid for these services significantly understate the true economic value of the work being performed. A more realistic way to assess impact is to compare the services delivered with their commercial or market equivalents, such as the cost of providing security training, providing incident response or cybersecurity standards.

Global benchmarks developed by non-profits can generate substantial value for users. For example, CIS makes its controls and benchmarks freely available to any organisation that chooses to adopt them. Roughly 25,000 organisations use CIS's free self-assessment tooling to increase the quality of their cybersecurity operations.[119] ISO 27001 certification, the closest commercial equivalent for a structured information security management programme, costs a typical small to medium-sized organisation between USD 10,000 and USD 75,000 over a three-year cycle, with an average of approximately USD 42,500.[120] Across 25,000 users, the commercial equivalent of the standards guidance CIS provides for free amounts to over USD 354 million in avoided certification and preparatory consultancy costs per annum.

---

117 Total Assure, 'Outsourced SOC Cost in 2025', 22 December 2025, https://totalassure.com/blog/outsourced-soc-costs-2025.

118 'NIST Marks Fifth Anniversary of Popular Cybersecurity Framework', *NIST*, 12 February 2019, https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework.

119 Company Interview

120 'How Much Does ISO 27001 Certification Cost?', accessed 15 April 2026, https://drata.com/learn/iso-27001/certification-cost.

Threat intelligence services can also generate substantial value. The most notable example would be Shadowserver, a non-profit that scans the global internet for vulnerabilities, malware, and active threats, and alerts affected organisations and governments. An estimate of the counterfactual commercial cost of Shadowserver's services can be based on the estimated values of the separate intelligence-sharing contracts. Our methodology uses the Netherlands, which represents 1.16% of global GDP, as the pricing anchor, with a basic government contract for equivalent threat intelligence data costing roughly USD 1 million annually.[121] Scaling that figure across the 201 national CERTs Shadowserver currently serves, weighted by each country's share of global GDP, yields approximately USD 83 million for basic government contracts alone.[122]

Governments that receive ShadowServer data typically redistribute it to national companies, which would require separate redistribution licences in a commercial arrangement. For the Netherlands alone, this cost is estimated at USD 20 million annually. If scaled across major economies, this would contribute a further USD 250 to USD 400 million in market-equivalent value. Non-government subscribers, numbering over 10,000, such as hospitals, banks, universities, and critical infrastructure operators, represent an additional USD 702 million at an average commercial-intelligence pricing of USD 70,200 per subscriber per year.[123] The total counterfactual commercial value lands at roughly USD 1.0 billion to USD 1.2 billion annually. Shadowserver delivers this at an operating cost of USD 5.5 to 6 million per year: a leverage ratio of approximately 170 to 200 USD of economic value per dollar spent.[124]

The total counterfactual commercial value lands at roughly USD 1.0 billion to USD 1.2 billion annually.

Elsewhere, several non-profits provide free assistance and training that, in the commercial market, would command substantial fees. One such NPO is the CyberPeace Institute, which provides free cybersecurity assistance, including threat assessments, incident response and capacity building to NGOs and humanitarian organisations that lack the resources to protect themselves. In total, about 645 organisations were supported in 2025.[125] That service is something a commercial vendor would price at USD 3,000 to USD 10,000 per organisation for a basic assessment alone.[126] With 645 organisations supported in 2025, that is USD 1.9 million – USD 6.4 million worth of services delivered.[127]

Another example includes the Cyber Readiness Institute (CRI), which provides cybersecurity training at no cost to users. Similar training courses are typically priced at approximately USD 36 per user per year in the commercial market.[128] If an estimated 500,000 individuals were to use this training, the implied economic value of this service could be calculated as at least USD 17.5 million worth of cybersecurity training per year.

Non-profits also provide incident response services; mitigating cyberattacks at low or no cost. Most notably, Access Now's Digital Security Helpline has handled more than 10,000 individual

121 Shadowserver.

122 Shadowserver

123 'Recorded Future Software Pricing & Plans 2026: See Your Cost', accessed 3 May 2026, https://www.vendr.com/marketplace/recorded-future.

124 CyberPeace Institute

125 CyberPeace Institute

126 'How Much Does a Cybersecurity Assessment Cost? Navigating', Atlant Security, 17 August 2023, https://atlantsecurity.com/blog/how-much-does-a-cybersecurity-assessment-cost-navigating-the-price-landscape.

127 CyberPeace Institute, 'CyberPeace Builders Annual Report 2025', *CyberPeace Institute*, 18 December 2025, https://cyberpeaceinstitute.org/news/cyberpeace-builders-annual-report-2025/.

128 'Security Awareness Training Cost (2025): Real-World Pricing', accessed 3 May 2026, https://www.consilien.com/news/how-much-does-security-awareness-training-cost-in-2025-a-complete-pricing-guide.

security cases, providing incident response, threat analysis and advice to individuals and organisations worldwide.[129] These services are comparable to commercial incident response and cybersecurity consulting, which typically charge USD 150 per hour or more in the private sector. Applying a conservative average of 10 hours per case at USD 150 per hour, the Helpline's work represents an estimated USD 1,500 in value per case.[130] Multiplied across 10,000 cases, this results in a minimum estimated market value of approximately USD 15 million in security services delivered.

When evaluated in terms of service delivery rather than price paid, non-profit cybersecurity organisations generate substantial economic value. By comparing their services to commercial market equivalents, it becomes clear that these organisations provide billions of dollars in economic value. The next section considers how non-profits help organisations avoid costs that result from cyber threats.

Costs avoided economic value

A one-third reduction in such incidents could generate hundreds of millions, if not billions, in annual savings.

The cost-avoided economic value looks at how much safer organisations and the internet have become due to interventions by non-profit cybersecurity organisations. This could take the form of enhanced phishing prevention or shorter periods of malware infection. These types of interventions create a safer internet ecosystem and thus significantly reduce costs for different types of organisations.

Cybersecurity training can lead to fewer cybersecurity losses through a 40% reduction in phishing clickthrough rate after three months of training.[131] In 2024, the average cost of a cyberattack on a small business ranged from USD 120,000 to USD 1.24 million, and 41% of US small businesses experienced at least one attack.[132] A one-third reduction in such incidents could generate hundreds of millions, if not billions, in annual savings.

Safe, trusted foundational software can also help reduce costs. DNS resolvers, which block queries to malicious websites, have prevented USD 10 billion in cybersecurity-related losses over five years, according to the 2019 DNS Cybersecurity Report.[133] Translating that to one-year yields USD 2 billion in avoided losses through trusted DNS for the study's sample population. Organisations such as the Global Cyber Alliance (GCA) and NLnet Labs provide these types of solutions for free.[134] Meanwhile, Quad9, a Swiss non-profit public DNS resolver co-founded by the GCA, blocks an average of 670 million malicious domain lookups daily

129 Access Now.

130 Dimitri McKay, 'The High Cost of Security Investigations', Splunk, 16 April 2025, https://www.splunk.com/en_us/blog/security/reduce-security-investigation-costs.html.

131 'KnowBe4 Report Reveals Security Training Reduces Global Phishing Click Rates by 86%', Security Info Watch, 14 May 2025, https://www.securityinfowatch.com/cybersecurity/press-release/55290389/knowbe4-knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86.

132 U. S. Small Business Administration, 'In Today's Economy, Cyber Safety Is Critical to Small Business Success | U.S. Small Business Administration', 23 October 2024, https://www.sba.gov/blog/2024/2024-10/todays-economy-cyber-safety-critical-small-business-success.
Alexis Porter, 'Impactful Big or Small: A Cost Comparison of Data Breaches', *BigID*, 19 February 2025, https://bigid.com/blog/a-cost-comparison-of-data-breaches/.

133 'Report: Measuring the Economic Value of DNS Security', *GCA | Global Cyber Alliance*, n.d., accessed 16 April 2026, https://globalcyberalliance.org/report-measuring-the-economic-value-of-dns-security/.

134 'Government Internet Shutdowns Cost $19.7B in 2025', 5 January 2026, https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

across 200 locations in 90 countries.[135] GCA's own research has shown that DNS firewalls of this type could mitigate one-third of all cyber incidents, estimating that on a global scale, protective DNS could prevent between USD 150 and USD 200 billion in losses annually.[136]

Rapid incident response can also significantly mitigate costs for affected organisations. One of the beneficiaries of the Institute for Security and Technology (IST) told them that by following the recommendations in their report, specifically the recommendation to work closely with law enforcement and report the incident, they were able to recover most of the ransom payment they made to the attackers.[137] From the initial USD 4.4 million ransom payment, the DOJ recovered approximately USD 2.3 million.[138] Given that nearly 80% of organisations that pay a ransom are attacked again, close cooperation with law enforcement and these non-profits will also ensure that victims do not incur future costs related to ransomware attacks.[139]

The avoided cost attributable to the intervention could amount to roughly USD 800 million to USD 1.2 billion for this particular incident for CTA's members/ beneficiaries.

Another example was the rapid response to the notorious WannaCry cyberattack in 2017. The CTA's Intelligence Sharing Working Group helped identify WannaCry's propagation mechanism roughly 48 hours sooner.[140] WannaCry caused an estimated USD 4 billion in global economic damage, with the bulk of losses concentrated in the first days.[141] Assuming that the coordination by CTA helped cut short the final 48 hours of active propagation, which represented an estimated 20 to 30 percent of total damage, the avoided cost attributable to the intervention could amount to roughly USD 800 million to USD 1.2 billion for this particular incident for CTA's members/beneficiaries.

Finally, preventing internet shutdowns can also prevent significant economic damage. Across 28 countries in 2025, documented shutdown costs totalled USD 19.7 billion.[142] Access Now's campaigning helped to prevent exactly these types of events in a few instances through advocacy, legal intervention, and public pressure on both governments and internet service providers.[143] Kazakhstan, Gambia, and Sudan, countries that Access Now helped prevent from going offline. If only Kazakhstan is considered, the country's five-day internet shutdown cost USD 410 million.[144] Therefore, a prolonged internet shutdown would pose an even more significant economic concern for the world's 48th- 50th-ranked economy based on nominal GDP.[145]

This section highlights how non-profits help avoid costs that run into the billions of dollars for organisations. Beyond the direct costs avoided, they also underpin the broader economic value generated by the digital economy, as explored in the following section.

135 'Quad9', *GCA | Global Cyber Alliance*, n.d., accessed 3 May 2026, https://globalcyberalliance.org/work/quad9/. 'Quad9 | A Public and Free DNS Service for a Better Security and Privacy', Quad9, accessed 3 May 2026, https://quad9.net/.

136 Quad9, 'Quad9 | A Public and Free DNS Service for a Better Security and Privacy'.

137 IST

138 IST

139 Anthony M. Freed, 'Majority of Organizations Who Paid Ransom Demand Attacked Again', Halcyon, 3 June 2025, https://www.halcyon.ai/blog/majority-of-organizations-who-paid-ransom-demand-attacked-again.

140 CTA

141 '"WannaCry" Ransomware Attack Losses Could Reach $4 Billion - CBS News', accessed 3 May 2026, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

142 'Government Internet Shutdowns Cost $19.7B in 2025'.

143 Access Now

144 'Central Asia's Government-Ordered Internet Blackouts Costing Millions | Eurasianet', accessed 16 April 2026, https://eurasianet.org/central-asias-government-ordered-internet-blackouts-costing-millions.

145 'GDP, Current Prices', International Monetary Fund, 2026, https://www.imf.org/external/datamapper/NGDPD@WEO/KAZ.

Supported Underlying Value

In addition to the direct services they provide, non-profits facilitate the internet economy and the economic value it generates. The internet is a platform on which companies conduct business and generate trillions of dollars of value.[146] This economic activity is underpinned by services that, if absent, would severely disrupt the market transactions and economic value generated on the internet.

An example of this is the Domain Name System (DNS). DNS is the internet's address book, translating domain names into the IP addresses that make every online connection possible. The non-profit NLnet Labs has a DNS resolver used by internet service providers and network operators worldwide. In terms of supported value, one could look at the total value of the digital economy enabled by this service. With the digital economy valued at USD 16 trillion (15% of global GDP) in 2024, even accounting for many for-profit providers operating in this space, non-profit DNS infrastructure supports value generation in the hundreds of billions of dollars.[147] Understandably, this value cannot be directly attributed solely to these organisations. However, it shows the value these organisations facilitate.

With the digital economy valued at USD 16 trillion (15% of global GDP) in 2024, even accounting for many for-profit providers operating in this space, non-profit DNS infrastructure supports value generation in the hundreds of billions of dollars.

Other supportive non-profit services come in the form of standards. FIRST maintains the three open standards that harmonise reporting in the cybersecurity space; however, determining their economic value has proven difficult compared with other members of the category. The Common Vulnerability Scoring System (CVSS) is an industry standard that assigns a severity score from 0 to 10 to every discovered software vulnerability.[148] Also, the Traffic Light Protocol (TLP) tells the recipient of sensitive threat information exactly how widely they may share it, using four colour labels.[149] The White House has recognised it as a cybersecurity best practice.[150] The Exploit Prediction Scoring System (EPSS) estimates the probability that a vulnerability will actually be exploited, helping teams prioritise their cyber policies.[151] All three standards are free and widely adopted by organisations such as Google and national Computer Emergency Response Teams (CERTs).[152]

Despite issues in calculating the value of FIRST standards, FIRST's capacity training programme proved more straightforward. FIRST does not provide training itself; therefore, we cannot fully attribute the programme's economic value to FIRST. Instead, FIRST provides the platform and the opportunity for the training to take place. FIRST was unable to provide an estimate of the number of training sessions held via its platform per year. However, taking a baseline estimate of 500 trainings facilitated through their platform, a means to calculate FIRST's value in their process is to multiply the number of trainings by the average market

146 'Global Digital Economy Report (2025) | IDCA'.

147 'Global Digital Economy Report (2025) | IDCA', accessed 3 May 2026, https://www.idc-a.org/insights/qUi9XgvyrzSkyDUy9Tqr.

148 'Common Vulnerability Scoring System SIG', FIRST — Forum of Incident Response and Security Teams, accessed 3 May 2026, https://www.first.org/cvss/.

149 'Traffic Light Protocol (TLP)', FIRST — Forum of Incident Response and Security Teams, accessed 3 May 2026, https://www.first.org/tlp/.

150 'FIRST Drives Global Cybersecurity Progress Through Community-Led Innovation', FIRST — Forum of Incident Response and Security Teams, accessed 3 May 2026, https://www.first.org/newsroom/releases/20241205.

151 'Exploit Prediction Scoring System (EPSS) Special Interest Group (SIG)', FIRST — Forum of Incident Response and Security Teams, accessed 3 May 2026, https://www.first.org/epss/.

152 FIRST — Forum of Incident Response and Security Teams, 'FIRST Drives Global Cybersecurity Progress Through Community-Led Innovation'.

value of comparable cybersecurity trainings and then apply an attribution factor to reflect the extent that these trainings were dependent on and/or successful due to FIRST's participation.

Therefore, an illustrative example would include 500 training sessions per year (at USD 3,000 per training), with a conservative estimate that 40% of the training's value is attributable to FIRST's enabling role (e.g., ensuring localisation of the training), implying a value of around USD 600,000. However, if this estimate is further adjusted to account for FIRST's role as the platform operator, at a conservative rate of 500 euros per training session, the total would be around 850,000 euros. Again, this value should be understood as an indicative estimate based on several assumptions about the value FIRST supports or enables, rather than as a value created solely by FIRST.

Cybersecurity non-profits also play a key role in establishing effective cybersecurity service markets. The global cyber threat intelligence (CTI) market is valued at approximately USD 14.6 billion in 2023.[153] Although relatively small within the broader cybersecurity industry, it plays a critical role by informing detection, response, and strategic decision-making. CTA is a key enabling institution within this ecosystem. It operates as a reciprocal intelligence-sharing consortium in which members contribute and receive threat data. This structure enables members to promptly and effectively spot and protect against threats. Moreover, because CTA remain neutral and does not monetise the intelligence provided by its members (some of which are for-profit organisations), its members are more willing to share information with the organisation. This ensures that CTA has a deep well of actionable, timely intelligence that can help prevent or shorten recovery time for its members from critical cybersecurity incidents, due to the aforementioned collective efforts.

The non-profit cybersecurity sector is generating value in the order of tens, if not hundreds of billions of dollars, when considered across all organisations globally.

Together, these examples illustrate that non-profit standards and coordination mechanisms underpin markets and ecosystems worth hundreds of billions of dollars, a value that would be difficult, if not impossible, to replicate through commercial alternatives alone.

Conclusion

This chapter shows that non-profit cybersecurity organisations generate significant value across a range of domains and through different mechanisms. Based on our case studies, the support that non-profits provide would take hundreds of millions to replace, create billions in cost avoidance, and underpin hundreds of billions of economic value. This value is delivered across a multitude of domains, including foundational support, threat intelligence, incident response, advocacy, digital security, standards, and capacity building.

These figures reflect only the case studies examined and represent a relatively small subset of the total value, which is likely much higher. Taken together, the non-profit cybersecurity sector is generating value in the order of tens, if not hundreds of billions of dollars, when considered across all organisations globally. Based on the case studies examined, the economic value generated is often 10 times, and in some cases up to 100 or 200 times greater than the cost of operating these organisations. This underscores that non-profit cybersecurity organisations are among the most effective destinations for funding, delivering exceptional value for money and strong returns for governments, businesses and society.

153 'Threat Intelligence Market Size, Share & Growth Report 2030', accessed 15 April 2026, https://www.grandviewresearch.com/industry-analysis/threat-intelligence-market.

Chapter 6: **Conclusion and Recommendations**

The digitalisation of the global economy is set to continue accelerating at an unprecedented pace over the coming decades, especially with the advent of technologies such as quantum computing. As such, the need to better secure our critical infrastructure and businesses will become increasingly important as cyber adversaries seek to utilise these new technologies for their own malicious purposes.

While for-profit organisations will undoubtedly play a pivotal role in ensuring that the global digital ecosystem remains secure in this new era, non-profit cybersecurity organisations also play an essential but insufficiently recognised role as well. Indeed, the central findings of this report highlight that these non-profits' contributions are neither marginal nor supplementary to those of their for-profit counterparts. Instead, they are foundational to the resilience, safety, and continuity of the global cyber ecosystem on which modern societies and economies depend.

The underappreciation of the value provided by these types of organisations appears to stem from the fact that what they offer is not adequately captured by conventional measures alone, given the breadth and depth of their services. Indeed, the contributions of these non-profits only become fully apparent when understood in a broader, more holistic manner. More specifically, in the context of the harm-reduced, resilience-strengthened, and collective cyber hygiene supported against the backdrop of an ever-evolving global cyber threat landscape.

Moreover, the work of non-profits encompasses multiple interconnected functions that, as shown in Chapter 4 and its portico shape, cannot operate effectively without the other pillars. Given that their responsibilities cannot be reduced to a single intervention type or category, their significance lies in how members of the sector both reinforce and support one another and in their overall goal of ensuring the freedom of the internet and a secure global cyber ecosystem.

Therefore, this study ultimately highlights that the appropriate question vis-à-vis non-profit cybersecurity organisations should not be "what value do they bring?" but rather "can we still provide a robust cybersecurity system in their absence?" Indeed, without these organisations, cyber service gaps would widen, cyber resilience would weaken, and the cyber threat landscape would become harder to manage for governments, SMEs, and even large corporations.

For that reason, this study concludes that there is a need for a more meaningful understanding of the value these organisations provide to ensure that governments and private-sector partners can support their work. Indeed, without this support, many non-profits will remain on rocky financial footing, limiting their capacity to provide critical services and potentially harming the global economy. To ensure that these critical services remain properly funded and robust, actors such as nation-states, industry leaders, and the non-profit sector itself could implement the following recommendations:

Recommendations for Government

1. **Establish dedicated public funding streams for non-profit's core operations:** Create permanent multi-year grant programme(s) or budget lines specifically for non-profit cybersecurity organisations. A certain percentage of this funding should be allocated to the organisation's core activities (e.g., maintaining DNS, threat hunting, developing standards and certificates, or cyber-related training) rather than to projects with limited scope. Such funding could be a part of the North Atlantic Treaty Organization's (NATO) new 5% defence expenditure commitment. This could, for example, fall under the 1.5% allocated for "security-related, dual-use infrastructure and resilience" areas, including cyber defence.[154]

   Initiatives like the Common Good Cyber Fund (CGCF) already operate along these lines. The CGCF pools donations from governments, philanthropies, and organisations to provide multi-year funding to cybersecurity NPOs.[155] In its 2025 pilot, it awarded USD 1.9 million and plans to distribute at least USD 3.5 million more through an open call in 2026. Governments should actively contribute to such funds, but these should not replace dedicated government grant programmes. Voluntary donations can dry up when donor priorities shift, or budgets tighten; a government budget line offers the predictable, recurring funding NPOs need.

   Indeed, due to the non-profit nature of these organisations, they often cannot fully bill for all the hours on a specific project, especially when they are inundated with multiple projects simultaneously, each with a very specific scope. This can result in organisations having 1) no or limited time to work on their core activities, which heightens the risk of the main value they generate eroding due to lack of time/funding; or 2) an inability to plan over multiple years, as they are constantly required to secure funds on a yearly basis. This funding should also be allowed to be used for activities globally, as cyber threats do not know national borders.

2. **Integrate non-profits into national cybersecurity strategies:** Formally recognise non-profit cybersecurity organisations in national cyber strategies, resilience plans, and critical infrastructure frameworks as a means to make their roles more visible, legitimate, and easier to provide funding for. This does not mean incorporating them into a country's government structure, as that would undermine their status as a neutral party and prevent them from serving as intermediaries among NGOs, industry, and government.

3. **Create a rapid-response funding mechanism:** Set up emergency funding mechanisms that non-profits can easily and quickly access for core activities and/or during major cyber incidents, geopolitical shocks (e.g., the Colonial Pipeline attack or SolarWinds incident). This mechanism would, for example, help ensure that SMEs can also survive such events despite not having the same level of funding as larger corporations.

---

154 Atlantic Council, 'NATO Defence Spending Tracker: How Are Allies Contributing to Collective Defense?', Atlantic Council, 9 April 2026, https://www.atlanticcouncil.org/commentary/trackers-and-data-visualizations/nato-defense-spending-tracker/.

155 Internet Society Foundation, 'Common Good Cyber Fund: A New Global Grant Program Supporting Cybersecurity Nonprofits', 24 February 2026, https://www.isocfoundation.org/2026/02/common-good-cyber-fund-a-new-global-grant-program-supporting-cybersecurity-nonprofits/.

Recommendations for Industry

1. **Commit a fixed percentage of revenue, profits, or philanthropy to the non-profit cybersecurity sector:** Adopt a formal industry/company norm that some level of support is provided to the non-profit sector. For example, this could be a "one per cent" norm for philanthropic giving, with a broad enough scope that non-profits can use the funds for both core functions and project-based work. Such funding could also be provided as membership fees, whereby for-profit entities receive certain "perks" (e.g., access to tailored threat intelligence) to further incentivise their continued financial support. However, this financial support should not infringe on non-profits' neutral status and/or detract from their ability to help underserved communities or organisations.

   To ease the financial burden on companies, this funding could be given in combination with national or regional governments. This funding should also be allowed to be used for activities globally, as cyber threats do not know national borders, and in addition to the membership fees or donations already provided to NPOs such as CREST or CTA.

Recommendations for the Non-profit Sector

1. **Take more ownership of the value provided by their services:** Through this project, it became apparent that for many non-profits, they had a hard time taking direct ownership of the economic or social value they generate because of the collective nature of their work. This has created an environment in which it is difficult for them to adequately highlight the importance of their work to potential funders. As such, these organisations need to develop clear, credible ways to spotlight their outcomes, including services delivered, communities supported, and, most importantly, risks reduced and harm avoided, as well as the cost that would have been incurred if a for-profit alternative had been chosen (if one exists).

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl