COMMON GOOD CYBER

# Advancing Cybersecurity by Design for the Global Digital Infrastructure

December 2024

www.commongoodcyber.org

# Executive Summary

This paper outlines the critical relationship between Common Good Cyber and the ongoing policy efforts around Cybersecurity by Design, also called Security by Design or Secure by Design. It argues that achieving a secure digital environment requires collective action to not only build security into the design of digital products but also into the Internet infrastructure to ensure that the most vulnerable in society benefit from these protections. The paper highlights key policy areas where alignment and collaboration are needed and provides recommendations for policymakers, industry stakeholders, and civil society actors.

# Acknowledgements

This paper was prepared by the Global Cyber Alliance, with Ms. Kayle Giroud, Director of the Common Good Initiatives, as lead author. The paper benefited from contributions by Mr. Michael Daniel, Cyber Threat Alliance, and the thorough review of Mr. Tod Eberle, Shadowserver Foundation, Mr. John Todd, Quad9, Ms. Kinsey Yow, Cyber Readiness Institute, and Mr. Phil Reitinger, Ms. Komal Bazaz Smith, Ms. Marina Calvo Leyva and Ms. Megan Kruse, Global Cyber Alliance.

We extend our sincerest gratitude to the Secretariat of Common Good Cyber for their unwavering dedication and commitment to advancing the cause of cybersecurity for the common good. This initiative, coordinated by the Global Cyber Alliance, is being made possible through the collaborative efforts of a Secretariat of numerous organizations who have contributed their expertise, resources, and passion towards this noble endeavor: the Cyber Threat Alliance, the CyberPeace Institute, the Forum of Incident Response and Security Teams (FIRST), the Global Forum on Cyber Expertise (GFCE), the Institute for Security and Technology (IST), and the Shadowserver Foundation.

# Introduction

The rise in cyber threats poses an increasingly complex challenge to individuals, organizations, and governments alike. While cybersecurity by design policies seek to integrate security into the products and softwares used by many, they alone cannot address the full spectrum of risks. This paper advocates for a comprehensive approach that combines cybersecurity by design policies with broad-based technical efforts aimed at making the Internet and digital services safer by default for all users, especially vulnerable communities. For digital security to be truly effective, it must be a collective good—an inherent feature of the global digital commons, rather than a service that only the well-resourced can afford.

# I. The Concept of Common Good Cyber

Common Good Cyber aims to protect critical efforts designed to enhance the overall security of the Internet and the digital ecosystem, and to provide direct technical assistance to vulnerable communities. These efforts are intended to:

- Improve the security of the Internet for the common good, removing the burden from individual users and organizations.
- Support the cybersecurity nonprofits, to enhance threat data collection, collaboration, protective services and response capabilities to emerging threats.
- Coordinate efforts to protect vulnerable communities, ensuring that digital security resources and training are available to all.

# II. Cybersecurity by Design: A Policy Imperative

Cybersecurity by design refers to the practice of embedding security into the architecture and development of digital products and services from the outset. This approach is increasingly being adopted:

### 1. European Union

The EU's Cybersecurity Act and regulations like the NIS2 Directive and the Cyber Resilience Act emphasize that digital products and softwares must adhere to strict security guidelines. The EU's regulatory framework places significant emphasis on ensuring security by default for critical sectors, and for consumers.

### 2. United Kingdom

The Product Security and Telecommunications Infrastructure (PSTI) Bill mandates that manufacturers meet specific security standards, such as disallowing default passwords and ensuring products receive security updates.

### 3. United States

The Biden administration's cybersecurity strategy emphasizes Secure by Design as a cornerstone for reducing vulnerabilities in critical infrastructure and consumer-facing products leading to the launch of a Secure By Design Pledge led by the Cybersecurity & Infrastructure Security Agency (CISA) with over 200 software manufactures committing to take measurable actions in line with the cybersecurity by design principles. The National Institute of Standards and Technology (NIST) has also developed frameworks to encourage organizations to adopt Secure by Design principles.

# III. The Intersection of Common Good Cyber and Cybersecurity by Design

Despite growing evidence of the harm caused by digital security incidents, there has been limited progress towards a comprehensive global approach to digital security for the common good. Instead, the focus has been on individual institutions securing themselves, leaving others outside their "borders" vulnerable. This fragmented approach is insufficient given how interconnected we are in the digital age. High-risk communities are particularly disadvantaged, as they lack the resources to implement digital security measures. Although cybersecurity by design and the Common Good Cyber principles are complementary, their integration remains uneven. Policies centered on cybersecurity by design address the supply side by securing products and services before reaching consumers, but a truly secure digital ecosystem requires collective action, equipping all users, from ISPs to the most vulnerable, with the tools needed to stay secure. The absence of clear responsibility only reinforces the cycle of individual security efforts, leaving everyone else at risk in an increasingly Internet-dependent world.

The public-interest cybersecurity solutions mapped under the Common Good Cyber mapping address this gap by providing a set of services and initiatives that:

- Support technical interventions at the ecosystem level such as securely routing information and stopping the spread of ransomware through industry-wide collaboration.
- Provide free resources for vulnerable communities at end-users level, including training, digital security toolkits, and incident response coordination for under-resourced organizations.

## Existing Resources: Providing Free Cybersecurity to Empower Businesses

| Name and Organization | Description | Actionable Impact |
|---|---|---|
| **Five-part series on using outside firms to reduce your cybersecurity risks** by Cyber Readiness Institute | Most small businesses need to get some outside support for IT and cybersecurity. The Cyber Readiness Institute provides support in navigating cybersecurity contracts and vendors so they don't fall into traps. | CRI's series has been widely accessed, with **258 downloads on whether to get outside support**, 160 on available support options, 155 on vendor contracts, 126 on selecting support levels, and 96 on managing vendor relationships. |
| **GCA Cybersecurity Toolkit for Small Business** by Global Cyber Alliance | A comprehensive toolkit tailored for small businesses that includes resources, guidance, and tools to protect against cyber threats like phishing, malware, and more. | Empowers small businesses with essential cybersecurity measures, enhancing resilience against common threats with accessible tools removing the financial barrier to cyber hygiene. To date the toolkits have received **more than two million views from across 200 countries**. |
| **Quad9** by Quad9 | A global public DNS resolver that blocks access to known malicious websites, protecting users from malware, phishing, and other cyber threats. | Beyond **blocking 670 million cyber attacks per day to protect more than 100 million users worldwide**, Quad9 also analyzes vast amounts of data on cyber threats, building the resilience of global Internet infrastructure. |
| **Free cyber threat intelligence and public Dashboard** by Shadowserver | Free, daily cyber threat intelligence network reports tell organizations across all sectors (including small businesses and the Internet service providers who serve them) about exposed, misconfigured, vulnerable and compromised devices on their networks in need of patching to enhance network security. The public Dashboard provides high-level aggregated statistics about cybersecurity threats affecting a given country or region. | **Serving nearly 10,000 organizations across more than 175 countries**, Shadowserver's network reports and public Dashboard allow users to identify existing threats and track remediation efforts over time to measure progress in securing vulnerable networks. |

To date, the Common Good Cyber mapping identified 334 solutions that work in the public interest at various levels of implementation. Together, they create a robust framework that strengthens the digital environment for all users, particularly those with fewer resources.

Some solutions are immediately actionable by a small business or an entity with no in-house technical expertise, while others enable the technical community to build a more resilient Internet infrastructure so the everyday Internet user doesn't have to worry about it. While cybersecurity by design policies are emerging as global standards, the need for a secure Internet for future generations remains. By incorporating a whole-of-ecosystem approach and the need for a secure by design infrastructure as opposed to only secure by design products, the burden for technical assistance and capacity building at the end-user level could decrease.

---

**Policy Recommendations**

1. The cybersecurity by design mandate could extend beyond product and service manufacturers and include digital infrastructure providers, such as ISPs, which play a crucial role in securing the Internet ecosystem.
2. Governments and industry should collaborate to support the distribution and analysis of free actionable threat intelligence, ensuring that all stakeholders, including smaller and vulnerable organizations, get both the awareness and the guidance needed to respond to threats. This requires creating a structured framework for collaboration between government, private sector, academic institutions, and civil society organizations.
3. Governments should not only fund and promote initiatives that provide cybersecurity training, tools, and services tailored to high-risk communities, ensuring equitable access to digital security, but also solutions fixing systemic vulnerabilities and ensuring we all operate on a secure and resilient Internet infrastructure.

---

**Good Practice: The New European Framework**

The European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), is Europe's new framework to support the capacities of the cybersecurity technology community. The ECCC was established in 2021 to pool expertise, including from outside industrial and research contexts. The non-commercial and pre-commercial projects, referred to as 'civic tech' within the ECCC regulatory framework, are defined as projects which "make use of open standards, open data, and free and open source software, in the interest of society and the public good" and are mentioned several times in the mandate of the ECCC.

The ECCC provides a structured framework for cybersecurity investments in the interest of society. Each Member State sets up a National Coordination Centre (NCC) which acts as a national hub for the ECCC framework. States might set up the NCC under an existing ministry or agency. In the example of Belgium, the Centre for Cyber Security Belgium, the national cybersecurity agency, has been designated as the future NCC. This means the cybersecurity agency will now coordinate investments from the EU and will be able to directly support, with funding, 'civic tech' projects. This new European framework stands out because it enables

governments to directly support a diverse range of cybersecurity stakeholders, including nonprofits, through targeted funding. This approach is both unique and valuable, as it departs from the more conventional model where government funding typically flows to other government entities.

---

# Conclusion

To build a more secure digital future, we must go beyond traditional regulatory approaches. Cybersecurity by design approach is a vital policy initiative, but without the complementary efforts, many vulnerabilities will persist. Policymakers should adopt a holistic approach, and loop in the variety of actors involved in securing the digital commons and the high-risk communities by integrating Common Good Cyber principles to ensure that the Internet is secure for everyone—not just those who can afford it.