Cybersecurity for the Common Good: The Imperative for Sustainable Mechanisms

Introduction

Common Good Cyber is inherently broad, and includes the set of available, accessible and deployed cybersecurity capabilities and activities that enable social and economic progress for everyone, beyond the investment that some might make to protect themselves. Common Good Cyber's key objectives include:

- **Global Collaboration:** Promote effective collaboration between governments, the private sector, academia, and civil society to collectively support core capabilities of the Internet.
- **Resource Mobilization:** Channel support towards nonprofit and public interest organizations dedicated to preserving the availability and security of the Internet.
- **Sustain Cybersecurity Capacity-Building:** Drive efforts to ensure the longevity and scalability of cybersecurity capacity-building initiatives on a global scale.

Unlike most other services that are a critical part of our lives, like roads and electric power, the Internet relies on people and nonprofits working on shaky ground and razor-thin budgets. This background paper focuses on a few illustrations of the challenges presented. The capabilities nonprofits provide form a significant part of the Internet, crucial for its availability, reliability, security, and scalability. However, the current funding and operational models for developing and maintaining these capabilities are unsustainable, posing risks to the Internet's availability and security. Despite their critical role, organizations involved in these activities face limited funding and resourcing models, hindering their ability to operate and putting their future existence in jeopardy.

The goal of Common Good Cyber is to change this paradigm. Key stakeholders in the Internet ecosystem need a common understanding of the challenges. This document explores these challenges by examining four illustrative categories:

A. Network Operation and Monitoring
B. Open Source Software
C. Operational and Support Organizations, and
D. Development and Delivery of Services and Tools

Sustaining the Internet and Building Capacity

For the Internet to work effectively, it depends on many components. These include, but are not limited to network operations and monitoring, naming and addressing, data routing, and protocols. In many cases, when these components were created to facilitate the Internet as we know it today, security was not top of mind. Addressing any issue that arises, like security, is further complicated by the range of stakeholders – businesses, governments and nonprofits – involved in maintaining these critical components and ensuring they can be used. The number of stakeholders, and their presence around the world, require that we also find and build the capabilities of the stakeholders at global scale.

A. Network Operation and Monitoring

The Internet relies on networks, connecting computers through cables or WiFi to transmit data. Many entities are involved in this effort, including for profit entities and nonprofit organizations. As one specific example, the Domain Name System (DNS) translates human-readable domain names into machine-readable IP addresses. Originally designed with minimal security, DNS servers are vulnerable to cyberattacks, posing risks to organizations, businesses, and governments.

Practical Example: Quad9

Quad9 is a nonprofit service founded by IBM, Packet Clearing House, and the Global Cyber Alliance. It provides a free DNS resolver service that protects users from cyber threats without compromising privacy. Quad9 blocks known malicious domains, preventing devices from accessing malware or phishing sites. It utilizes threat intelligence from leading cybersecurity companies to assess website safety in real-time. The system, deployed globally, automatically blocks access to known malicious websites, safeguarding user data. As of 2024, Quad9 operates with systems deployed in over 100 countries, preventing around 400 million malicious events per day.

Despite its positive impact, Quad9 faces challenges as a nonprofit relying on sponsorships and donations. End user protection is provided at no cost, which has proven to lead to wide adoption - Quad9 now estimates many tens of millions of end users utilize the no-cost protections against cyber-crime. However, there is not a direct relationship between this high usage and funding resources. Deployment to difficult technology regions (Africa, South America, central Asia) is costly and time-consuming. Legal issues, such as a case involving Sony Music Entertainment in Germany, have also impacted Quad9's financial reserves. The courts ultimately ruled in favor of Quad9, emphasizing the importance of protecting neutral nonprofit entities against arbitrary demands to block sites.

B. Open Source Software

Open source software is a crucial element in operating systems used by individuals, businesses, and governments. Developed collaboratively and available for examination, modification, and distribution at no cost, it has a far different support model than proprietary software, which is owned by a company, however, most modern software has open source components even if it is proprietary. Approximately

80-90% of software is estimated to be based on free open source software, making it a foundational component of the Internet and the global economy.

Practical Example: Log4J

Examples include Log4J and Linux, supporting applications like iCloud and operating systems like Android. Despite their widespread use, many open source projects, like Log4J, rely on volunteers for maintenance, making them susceptible to security vulnerabilities. In 2021, a Log4J vulnerability put millions of devices at risk, highlighting the challenges of relying on volunteer-driven projects for critical internet components. Talent retention is a significant issue due to the lack of compensation, with 41% of open source projects failing because contributors lose interest or have time constraints. The need for a new model to sustain open source software, crucial for both free and commercial tools on the Internet, is obvious. In addition, some Internet security software, like Suricata, is open source.

C. Operational and Support Organizations

Operational and Support Organizations help maintain the cybersecurity of the Internet by, for example, monitoring threats across networks and sharing information to protect networks and assets. The provision of cybersecurity services by Operational and Support Organizations at little to no cost to the customer fosters a collective defense approach, ensuring widespread accessibility and affordability. The support they provide can both aid the capability of more sophisticated stakeholders, empowering them to better protect everyone, or more specifically help the more vulnerable. This democratization of cybersecurity enables a broader user base, including small businesses and public agencies with limited resources, to fortify their digital environments. By removing financial barriers, these organizations promote inclusivity, enhance overall cyber resilience, and contribute to the creation of a safer and more secure digital ecosystem for everyone.

Practical Example: Shadowserver Foundation

The Shadowserver Foundation, a non-profit, conducts internet scans to identify vulnerabilities and serves as a hub for sharing cyber threat intelligence. Its impact includes providing free daily reports to 131 national CERTs, collaborating with law enforcement, and benefiting major businesses and governments. To continue providing essential public benefit services, Shadowserver's needs include: funds to maintain its costly data center; donated servers and other hardware to replace aging systems within its data center; communications expertise to increase awareness of Shadowserver’s available services; and introductions to key decision-makers in government and private industry who can create opportunities for Shadowserver to contribute to funded projects and help ensure its free services are being fully utilized across all sectors.

Practical Example: MITRE ATT&CK

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques. It started as a research project and has evolved into a resource maintained by over 400 contributors and used by thousands of organizations globally. ATT&CK is a means that enables security teams to understand and defend against critical threats. Despite global community support and reliance, ATT&CK is resource constrained with a significant backlog and annual funding uncertainty.

These examples highlight the critical role of non-profit organizations in cybersecurity and the challenges they face in sustaining their operations and contributions to the global community as many under-resourced security teams globally rely on threat data provided by ShadowServer and MITRE ATT&CK to take informed decisions and protect their systems and networks.

D. Development and Delivery of Services and Tools

Ensuring the security of the Internet involves developing and delivering services and tools accessible to all users, particularly those with minimal resources for cybersecurity. Non-profit organizations play a crucial role in lowering barriers by developing policies, tools and providing cybersecurity training. These efforts are essential for ensuring global cooperation and enabling cybersecurity for all Internet users.

Practical Example: FIRST

The Forum of Incident Response and Security Teams (FIRST) was formed in 1990 in response to the growing need for better communication and coordination across the quickly growing incident response community. FIRST's mission is to bring together incident response and security teams from every country across the world to ensure a safe internet for all, fostering coordination, establishing a common language for threats and responses, and developing good practices for incident response. Volunteer-driven, FIRST leverages the expertise of incident responders worldwide, allowing them to contribute their passion and knowledge to the community.

FIRST's impact has benefited numerous stakeholders in addressing cybersecurity incidents globally. However, as a primarily community and volunteer-led organization, providing sustainable support is a challenge as the community continues to grow rapidly and serve increasingly diverse contexts. Fundraising poses difficulties as FIRST’s role primarily is as a forum, facilitator, and enabler, making it challenging to fit into funding opportunities. Administrative burdens further complicate accessing funding opportunities and creates the risk of mission drift. FIRST adopts a member-focused business model where modest membership dues support a small full-time team, primarily focused on core activities, with a lack of dedicated staff for fundraising, communications, or administrative support. With a strong global network of operational experts and practitioners, the positive impact of the FIRST community to the global common good would benefit from increased resources to support volunteer and community driven initiatives, communications support, regional liaisons for more tailored and localized support and outreach, and dedicated resources for FIRST community and capacity building initiatives.

The Challenges Faced by Cybersecurity Non-Profits

Based on the above examples we can see that these organizations– that primarily work in the background of the Internet's operation– face several challenges to remain sustainable. These can be grouped into two broad categories: (1) limited and/or inconsistent funding; (2) reliance on small teams to advance technical and non-technical work.

Limited and/or inconsistent funding

Funding for nonprofit organizations focused on securing the Internet for all is insufficient or inconsistent. There are three main reasons for this:

1. **Available funding is often focused on specific key performance indicators that do not necessarily align with nonprofit missions**
   In many cases the majority of funding for cybersecurity is tied to key performance indicators determined by the funder. Often these are limited to specific program life-cycles or aimed at strengthening the cybersecurity of a specific community or country via national policies or capacity building. Therefore securing funding via this mechanism has the potential to lead to mission drift. Furthermore, applying for these available funds requires organizational capacity to respond to these opportunities, a luxury many cybersecurity nonprofits do not have. In cases where funding is successfully obtained via this method, projects are often limited to short life-cycles, meaning the funding is timebound. Key activities to sustain core capabilities of the Internet are also often started as a side project in spare time, and not by organizations that have the framework to even consider sustaining them in the long-run.

2. **Membership fee business models do not bring in enough funding to support these nonprofits operations.**
   Membership-based business models provide a way for nonprofits to secure funding. However, this approach falls short in providing sustained or adequate funding to fully cover operational costs. While the model offers a strategic avenue for engaging partners, they can be resource-intensive. In addition, membership models are most effective when the collective interests of the members reflect the actions that should be taken to protect the Internet, but there are where that isn't true or or economic challenges (including the collective action problem) reduce the effectiveness of member-driven efforts.

3. **Reliance on small teams or volunteers to deliver technical and nontechnical work**
   Many of these organizations rely on small teams or volunteers to advance both their mission-centric and operational work. Reliance on volunteers, for instance, limits an organization's ability to conduct its work based on the availability of its volunteer network. Sometimes these key activities started simply as a side project done in folks' spare time to address a gap that they identified that they knew no one else would address. In a sector, like cybersecurity, this can prove challenging as threats need immediate remediation. Furthermore, many of these organizations are primarily staffed by technical teams. This ensures they are able

to deploy cybersecurity expertise to their target communities. Nevertheless, it means they lack full-time support in areas like strategic communications, administrative functions, or stakeholder engagement. As such, these organizations are often juggling different responsibilities that do not necessarily mirror their skillset.

Conclusion

In conclusion, the security and reliability of the Internet are fundamental to our interconnected world but many organizations maintaining the Internet are unable to hire or maintain sufficient staff and secure the resources to meet their needs or procure the latest technology to maintain their services. By addressing the challenges faced by cybersecurity non-profits, we can collectively contribute to a safer digital future for individuals, businesses, and governments alike. It is time to recognize the crucial role these organizations play and take concerted action to fortify the backbone of our digital society.