Cyberpeace Analytical Report

NGOs Serving Humanity at Risk: Cyber Threats Affecting International Geneva

Executive Summary

Introduction

In the heart of International Geneva, a diverse ecosystem thrives, housing 38 international organizations (IOs), 432 non-governmental organizations (NGOs), and several hundred associations active at an international level, all united by a shared mission: to make the world a place of peace and justice. NGOs are the unsung heroes, addressing armed conflicts, natural disasters, and humanitarian crises, championing human rights, and advancing the Sustainable Development Goals (SDGs). Like many other organizations, NGOs heavily rely on technology, which is critical for projecting their activities globally in real time. Yet, in today's digital landscape, this reality brings its own set of challenges.

While fighting for the greater good, NGOs must battle against all forms of cyberattacks, ranging from espionage and ransomware to fraud and disinformation. On one side, they are targeted by various threat actors - criminal groups, state actors, terrorist groups or hacktivists - seeking to disrupt their work, compromise data, and tarnish their reputation. On the other, they do not possess human or financial resources to protect themselves.

In Geneva, the CyberPeace Institute safeguards these heroes. Our cybersecurity services for NGOs include threat landscape mapping, volunteer-led consulting, alert notifications, and providing policy recommendations to donors and public/private decision-makers. All these services are free and tailored to the NGOs' operational reality.

The Report aims to provide actionable recommendations to build capacities and resilience to mitigate cyber risks. It provides insights on the organizational readiness of NGOs to prevent, respond to and recover from cyberattacks. Using data, including primary data from surveys and interviews, the Report looks at the threats NGOs face, the vulnerabilities they are exposed to, and examines their preparedness to mitigate these challenges. Its ambition is to reinforce NGOs' resilience in a sustainable manner, and for them to become the primary actors of their cybersecurity.

Key Findings

Key Finding 1

NGOs in International Geneva are targeted by cyberattacks

- **41% of NGOs** report having been victims of a cyberattack within the past three years.

- **All NGOs** that have experienced attacks report that these were not isolated events. The frequency of these incidents varies, with some NGOs facing incidents on a daily basis and others encountering them on a monthly or annual basis.

- **70% of NGOs** either don't think, or aren't sure whether they have an adequate level of resilience to recover from a disruptive cyberattack.

Key Finding 2

NGOs in International Geneva understand their exposure to cyber risks, but lack the support needed to implement mature cybersecurity strategies

- NGOs, unlike entities recognized as critical infrastructure, lack specific designation as a sector for particular protections in cyberspace.

- Funding for NGOs is generally earmarked for specific projects, often leaving cybersecurity without dedicated financial support.

- **33% of NGOs** report having no IT support or technical expertise, and **56% of NGOs** report not having a budget allocated for their cybersecurity needs.

- While NGOs generally recognize a variety of potential threats, such as social engineering, ransomware, and other malware, **only 4%** have an actionable cybersecurity policy.

- **85% of NGOs** recognize the importance of staff awareness in cybersecurity, yet **only 52%** provide regular cybersecurity awareness training to their personnel.

Key Finding 3

NGOs in International Geneva face challenges reconciling their operational models with the rapidly changing operational landscape and the needs for cybersecurity

· NGOs are confronted with a rapidly changing landscape of regulation, norms and laws related to the use of technology and obligations in the event of cyberattacks, such as data protection obligations in the case of a data breach.

· Freely available cybersecurity tools accessible to NGOs are not tailored to their specific operating and business models. Access to and awareness of these tools alone does not equate to sustainable cybersecurity.

· NGOs require more than tools and knowledge, they also require a cybersecurity workforce (people and skills).

Whilst NGOs have much more progress to make in their cybersecurity capabilities and capacities, acknowledging the very real threats posed to them and developing cybersecurity practices suggests concrete actions can be taken, paving the way for a more optimistic future.

Tackling the Threats - Strategic and Technical Recommendations

While the key findings shed light on the critical challenges that NGOs in International Geneva face in the realm of cybersecurity, the report details recommendations that provide a concrete roadmap for action.

Strategic and Technical Recommendations focus on the following categories in cybersecurity:

- Processes and Structures
- Partnerships and Networks
- People and Skills
- Technology
- Official Documents Related to Cybersecurity Matters

NGOs are also recommended to join the Institute’s CyberPeace Builders program to benefit from actionable and free cybersecurity assistance and support. The CyberPeace Builders program equips NGOs with guidance and cyber threat intelligence which enables them to detect upcoming cyberattacks, and build NGO cyber capacity to prevent cyberattacks against them or their beneficiaries.

Additionally it engages with cybersecurity experts and NGOs through a volunteering platform to foster community engagement.

The CyberPeace Institute acknowledges and thanks the important contributions from the NGOs that participated in this Project. The analysis, findings, and conclusions of this Report have been developed by the analysts and other experts of the CyberPeace Institute. They have been shared with the NGOs who participated in the research, but they have not been requested to endorse them.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15
1202 Geneva, Switzerland

cyberpeaceinstitute.org
@CyberPeace Institute
@CyberpeaceInst