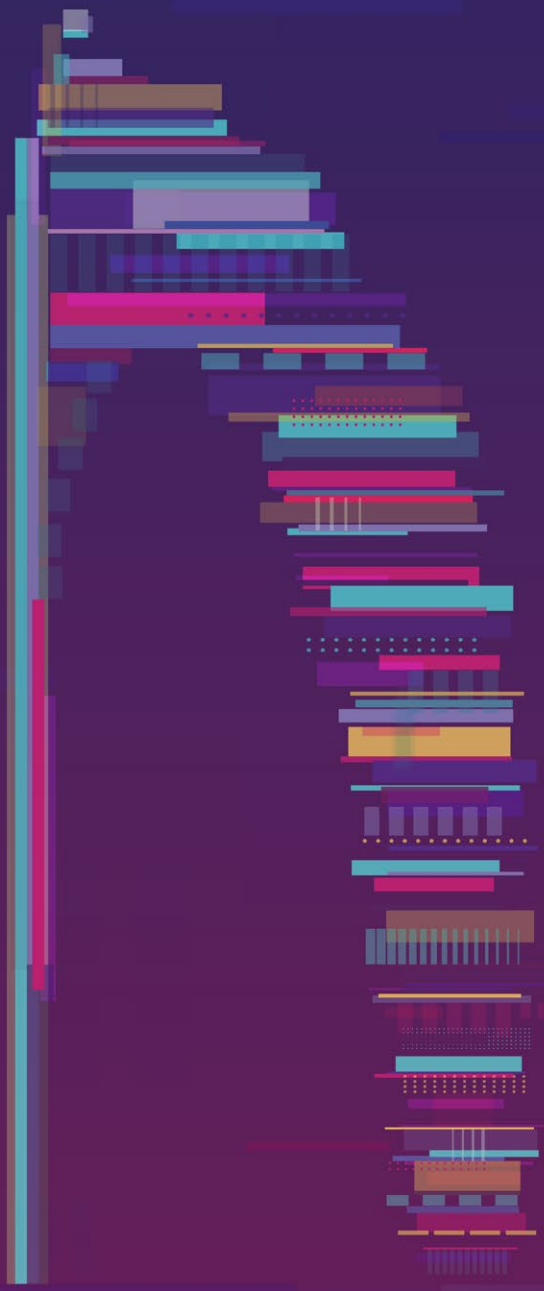
CyberPeace Institute



CYBERPEACE ANALYTICAL REPORT

NGOs SERVING HUMANITY AT RISK: CYBER THREATS AFFECTING INTERNATIONAL GENEVA

With the support of:

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

In a world in crisis, protecting NGOs is an emergency.

Foreword

Stéphane Duguin,

Chief Executive Officer, CyberPeace Institute

Despite 25 years spent collecting evidence at crime scenes, gathering testimonies, tracking down perpetrators of crimes and being confronted with the worst that the human mind can imagine, I am still stunned by criminals lack of shame.

Before becoming Chief Executive Officer of the CyberPeace Institute, I admit I never looked into the situation of non-governmental organizations (NGOs), and did not understand the precarity within which they operate in cyberspace. These last few years have introduced me to a shocking reality, that those who are first on the front line of armed conflicts, in natural disasters and climate crises, are targets, and often victims of cyberattacks. These are attacks against those who invest their hearts, expertise and time to the provision of essential services to people in all parts of the world - from access to drinking water, assistance to refugees, to safeguarding children.

This report bears witness to the cyber reality of NGOs, and supports a conviction: I firmly believe that we can all do more to support NGOs. Civil society, public authorities, philanthropies, academia, media, can collectively enable the urgent support that NGOs need and deserve.

This report is published on the fourth anniversary of the founding of the CyberPeace Institute. Since our creation, we have been providing free cybersecurity support to those who need it most, analysing the threat landscape and advocating for responsible behavior in cyberspace.

This report is a further contribution to this work, and another building block in the construction of collective action to protect those - the NGOs - who help to protect us.

Part 1
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 greater humanity, peace and justice. NGOs are the unsung heroes, responding in 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 the 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.

With the leadership and support of the Republic and Canton of Geneva, this 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.

This report builds on technical analysis conducted by our cyber analysts and a comprehensive survey with 27 Geneva-based NGOs.

The sample size of 27 NGOs allowed for a detailed examination of each participating NGO, providing an understanding of their unique contexts, challenges, and practices. This depth of analysis can yield nuanced insights that may be obscured in larger samples. These organizations have been selected because they embody the diversity of Geneva NGOs: some conduct their activities in Geneva whilst others operate across the world. Some are small and under-financed, others are well established. They operate in sectors including healthcare, justice, human rights, peace and education and humanitarian relief. Together, these NGOs bring vital aid and services to tens of millions of beneficiaries.

If you are an NGO looking for help with your cybersecurity, we encourage you to reach out to us. We are here to support and protect your vital work in our increasingly digital world.

The CyberPeace Institute is an independent and neutral non-governmental organisation (NGO) that strives to reduce the frequency, impact, and scale of cyberattacks, to hold actors accountable for the harm they cause, and to assist vulnerable communities.

The Institute is based in Geneva, works in close collaboration with relevant partners to reduce the harm from cyberattacks on people's lives worldwide, and provide assistance. By analysing cyberattacks, it exposes their societal impact, the ways that international laws and norms are being violated, and advances responsible behaviour to enforce cyberpeace.

At the heart of the Institute's efforts is the recognition that cyberspace is about people. It supports providers of essential services to the most vulnerable members of society, ultimately benefiting us all.

Why this Analysis? From Data to Action

The aim of this analysis project is to increase understanding of the cyber threat landscape affecting NGOs and aims to provide actionable recommendations.

These recommendations address the following areas:

1. How NGOs can better defend and protect themselves from cyberattacks and their associated impact and harm. A separate technical report is also provided to NGOs with more specificities on technical findings from this project.
2. How donors, policymakers, and companies can contribute to safeguarding NGOs in the face of cyber threats.

Although the focus of the current report is on Geneva-based organizations, this methodology will be replicated in other contexts and serve as a blueprint for future reports on cyber threats against NGOs.

This report is part of the CyberPeace Institute's broader mission, offering free cybersecurity services to NGOs which includes:

- Mapping the threat landscape for NGOs.
- Delivering actionable, free cybersecurity services to NGOs (CyberPeace Builders program[1]).
- Producing threat intelligence and automatically alerting NGOs about suspicious cyber activity.
- Building capacity amongst donors to understand the cybersecurity risks of NGOs.
- Providing data-driven evidence to regulators.

Acknowledgements and assistance

The CyberPeace Institute acknowledges and thanks the important contributions from the NGOs that participated in this project. These NGOs from International Geneva conduct their activities across a range of sectors, including humanitarian, health, justice, human rights, peace and education. They bring vital assistance and services to tens of millions of beneficiaries across the globe. These NGOs operate internationally across various regions, particularly Europe, Africa, the

Middle East and Asia. A number of the organizations also operate in North America, Oceania, Latin America and the Caribbean.

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 project but they have not been requested to endorse them.

NGOs concerned by or encountering any of the issues detailed in this report can contact the Institute for advice and support through its CyberPeace Builders program. The CyberPeace Builders[1] is composed of regional advisors and experts working and/or volunteering for the CyberPeace Institute, and managing a network of corporate volunteers from local and international companies developed specifically to support NGOs. This program helps NGOs by providing them with pre-incident, post-incident and support services to build their cyber resilience. NGOs can build their resilience by accessing tailored assistance, such as awareness training, dark web monitoring, phishing simulations and website vulnerability scanning.

Part 2
Key Findings

Key Finding 1

NGOs in International Geneva are targeted by cyberattacks.

• 41% of NGOs report having been victim 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 Information Technology (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. For instance, 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.

Part 3

Recommendations

Strategic Recommendations for NGOs

NGOs should follow guidance and advice provided by the National Cyber Security Centre (NCSC). The NCSC website provides information and advice on topics including, cyberthreats and incidents, technology considerations, awareness-raising and prevention. NGOs can also use the website to report cybersecurity incidents and vulnerabilities.

NGOs should report cyber incidents to the relevant Swiss law enforcement agency and to the NCSC.

NGOs should join the CyberPeace Builders to benefit from actionable and free cybersecurity resources, including skilled experts, adapted technology, and support in developing their digitization strategy.

Technical Recommendations for NGOs

The CyberPeace Builders provides free cybersecurity support to NGOs, including for the following recommendations:

NGOs should organize simulations to test their cybersecurity policies and practices. NGOs should also regularly run security awareness and training programs for all staff members, including board members and senior leadership teams. Specialized training on social engineering attacks, such as phishing exercises, should also be conducted. NGOs should also conduct vulnerability scans of their digital assets and

ensure they follow the latest security recommendations.

NGOs should maintain official documents outlining their cybersecurity policies and procedures, with a particular emphasis on software management. Regularly updating software, removing unsupported or unused software, and disabling unnecessary user accounts should be documented as best practices.

NGOs should establish clear processes and procedures for the identification and implementation of cybersecurity tools. This includes Multi-Factor Authentication (MFA), Next-Generation Anti-Virus (NGAV) software, firewalls, password managers, Virtual Private Networks (VPNs), and Data Loss Prevention (DLP) systems.

NGOs should develop robust backup procedures to mitigate the impact of cyberattacks, infrastructure failures, outages, or unexpected events. These procedures should be documented and regularly tested.

To protect their web services effectively, **NGOs** should document processes for safeguarding backend admin interfaces with reverse proxy masking IP addresses and secure query processing. Additionally, they should implement Domain Name System (DNS) and network proxy solutions offering DDoS protection and certificate issuers for website protection.

NGOs should provide clear guidance to their users on checking whether their private and professional email accounts have appeared in known data breaches. They should also establish documented procedures to follow in the event of a breach.

NGOs should schedule regular security audits conducted by external third-party experts, documenting the audit process and results.

NGOs should establish documented naming conventions with consistent rules for account naming, facilitating cybersecurity management.

NGOs should document processes for the regular review and verification of security for external accounts.

To reduce security risks, **NGOs** should maintain official documents outlining procedures for restricting administrative privileges to a minimal number of trusted users.

NGOs should document security measures that ensure all ports are secured with SSL encryption to prevent unauthorized users from intercepting data.

NGOs should follow documented best practices for email security, including DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).

Recommendations for the International Geneva

While the key findings shed light on the critical challenges that NGOs in International Geneva face in the realm of cybersecurity, the following recommendations provide a concrete roadmap for action. These recommendations are structured according to a cyber capacity building framework developed by the United Nations Institute for Disarmament Research (UNIDIR)[2], covering five key pillars: official documents, processes and structures, partnerships and networks, people and skills, and technology.

Official Documents Related to Cybersecurity Matters:

• NGOs should be recognized as stakeholders with specific needs to which host authorities pay particular attention. Given the role of NGOs, promoting their cybersecurity should be integrated strongly into policies.

• Geneva-based NGOs should develop and implement cybersecurity governance policies and practices, including a cybersecurity policy, an incident response plan, and an asset inventory. The CyberPeace Institute, as a local partner, commits to help them do that.

• The CyberPeace Institute and its academic partners should enhance their efforts to document, track, and analyze cyberattacks against NGOs within the Geneva ecosystem and any subsequent accountability measures taken, including the prosecution of perpetrators.

Processes and Structures:

• Swiss Public authorities should recognize the specific needs of NGOs. In cases involving ransomware, investigations into the financial flow stemming from extortion schemes should be conducted to hinder the activities of threat actors. Public authorities should actively promote the position discouraging the payment of ransom, emphasizing that it directly finances organized crime and encourages further cyberattacks.

• Swiss Public authorities, together with the National Cyber Security Center (NCSC), should actively promote transparent reporting on cyberattacks against NGOs to inform policy-making. Robust

safeguards should be in place to protect the confidentiality and integrity of this information.

Partnerships and networks:

• Cybersecurity companies based in Geneva, and private companies who employ cybersecurity professionals, should join the CyberPeace Builders programme to volunteer their expertise to help Geneva-based NGOs. Private companies can benefit from the CyberPeace Builders program by showcasing social responsibility and fostering staff skill development in real-world scenarios. These collaborations also strengthen cross-sector relationships, offering insights into NGO cybersecurity challenges and improving companies' ability to address evolving threats.

• NGOs would benefit from a better understanging of the threat they are facing. Swiss public authorities could actively facilitate the study of existing and potential cyber threats faced by NGOs. Collaborative initiatives with academia and civil society organizations can be instrumental in building knowledge about cyberattacks and their impact on NGOs.

• The local ecosystem should engage with media organizations reporting on cyberattacks to highlight the human impact these attacks have on NGOs and the beneficiaries they serve.

People and Skills:

• Resources should continue to be allocated to enhance the knowledge and expertise related to cybersecurity within NGOs. This includes setting up cyber clinics to help NGOs in developing in-house capabilities through training, or outsourcing to external providers when necessary. Swiss public authorities and academics can play a particular role in this regard.

Technology:

• Local corporations and civil society in the Geneva ecosystem should collaborate to share in a secure manner threat information about attacks against NGOs and the vulnerabilities that threat actors exploit with ease.

• The CyberPeace Institute and its partners should continue to develop free cybersecurity products for NGOs, and develop partnerships with Geneva-based private companies to offer their solutions for free to local NGOs.

Part 4

Cyber Threats on NGOs : Analysis

Overarching Threat Landscape

For the past years, NGOs have been undergoing a rapid digital transformation which has increased their risks of cyberattacks. The technologies that allow their action to be more effective are being exploited by malicious actors who steal funds, exfiltrate data, including highly sensitive data on people, or disrupt the organizations' ability to operate. Additionally, there is the risk that cyberattacks and operations could exacerbate humanitarian needs. For example, targeting essential infrastructure could disrupt the provision of critical services including power supplies, healthcare and clean water, which are essential for the civilian population.

However, NGOs often lack cybersecurity capabilities to both understand their threat landscape and to put in place adequate measures to prevent, respond to and recover from cyberattacks. They may not have the resources and expertise to properly secure their ICT infrastructure and digital assets or to develop an adequate incident response system that could minimize the impacts of cyberattacks.

Types of Cyberattack

Destructive attacks designed to cause damage to systems and deletion of data.

Disruptive attacks that interrupt the functioning of organizations and systems.

Data weaponization attacks leading to the theft or exfiltration of data or the acquisition of data for espionage, surveillance or intelligence.

Disinformation attacks leading to the spread and circulation of false and/or malicious information.

Types of Threat Actors

Cyber threat actors, also known as malicious actors, are individuals and/or groups that intentionally cause harm to digital networks, systems and/or devices. Cyber incidents are carried out by a range of different threat actors including:

Nation-state actors:

- Threat actors that are part of a state apparatus.

State-sponsored threat actors:

- Threat actors which conduct cyber operations on behalf of a state's interests, including geopolitical objectives. The state may delegate authority for an actor to act on its behalf, or orchestrate an actor to act in pursuit of state goals, including by the provision of ideation or material support.
- Advanced Persistent Threat actors (APTs) are often included within the realm of state-sponsored threat actors due to the sophistication of their malicious cyber activities.
- "Proxies" are intermediaries that are available to, detached from, but mobilised by, a beneficiary - which may be a state - to carry out cyber activities in pursuance of its interests.

Hacktivist collectives:

- Threat actors conducting malicious cyber operations - primarily hacking - to bring attention to a cause. These threat actors are politically, socially, or ideologically motivated.

Cyber criminals:

- Individuals or groups of people who use technology with malicious intent to harm or otherwise obstruct activities on digital systems or networks.

Cyber terrorists:

- Threat actors belonging to, or affiliated with, a terrorist organization, who conduct malicious cyber operations - including threats of violence - to support that organization's objectives or activities.

Insider threats:

- Insider threat actors are individuals who use their authorized access to an organization, intentionally or unintentionally, to do harm to the

organization. No matter the intent, there is often a compromise to the confidentiality, availability and/or integrity of the organization's network, systems or data.

Competitors:

- Threat actors conducting malicious cyber activities against a competitor to gain advantage or cause reputational harm.

Individuals:

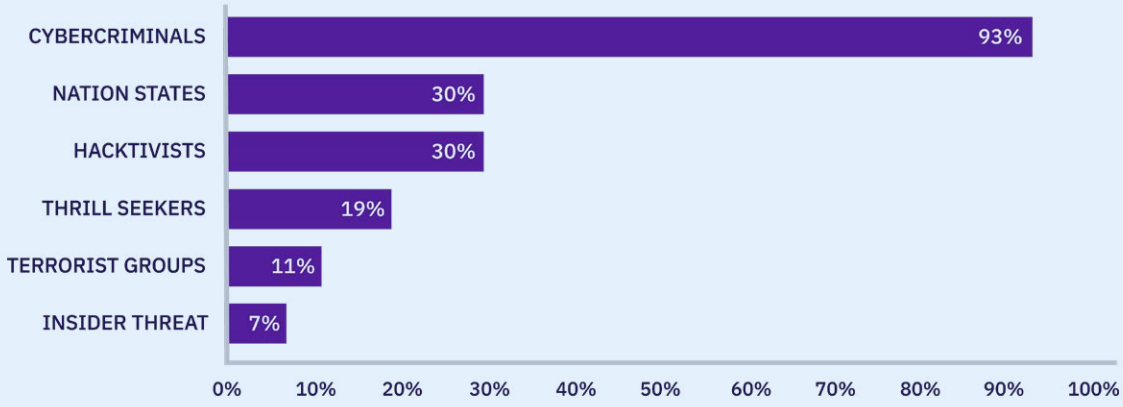
- Threat actors that attack computer and information systems primarily for fun or to advance their own skills (thrill seekers), or for their own personal gain.

Specific Threats and Vulnerabilities

The NGOs participating in the analysis were asked to identify the main cyberattacks/threats to their organization, the malicious actors behind these attacks, and any vulnerabilities that pose a serious risk to their organizations' cybersecurity. The results demonstrate a general awareness on the variety of potential threats and risks NGOs might encounter, as illustrated below.

- **93% of NGOs** identified cybercriminals as a significant threat actor, demonstrating widespread concerns about potential criminal targeting.
- Hacktivists and nation-state actors were jointly perceived as the next tier of threat actors, with **30% of NGOs** indicating concern over the potential threat.
- Other significant threat actors included, 'thrill seekers', and terrorist groups.

Significant Threat Actors (as perceived by NGOs)

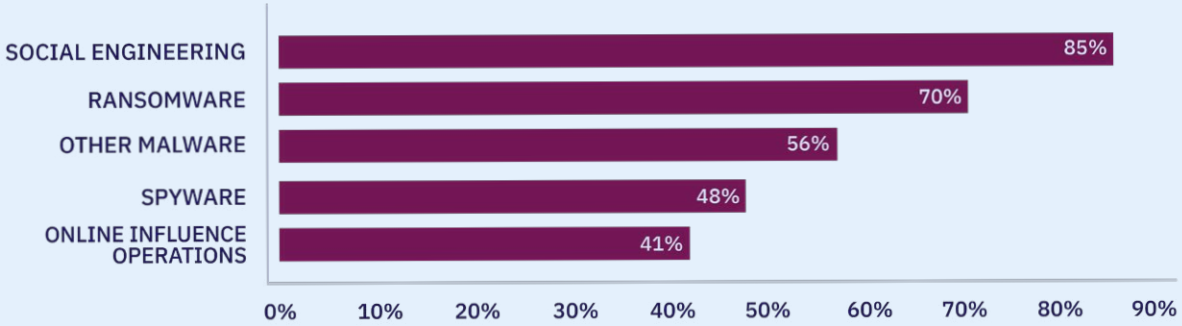


The NGOs were asked to identify the techniques/type of threat they perceive as posing a significant threat. Findings focused particularly on different types of disruptive attacks:

85% consider social engineering to be a significant threat.

41% consider online influence operations as an significant threat.

NGOs Threat Perception - Top 5 Cyberattack Types

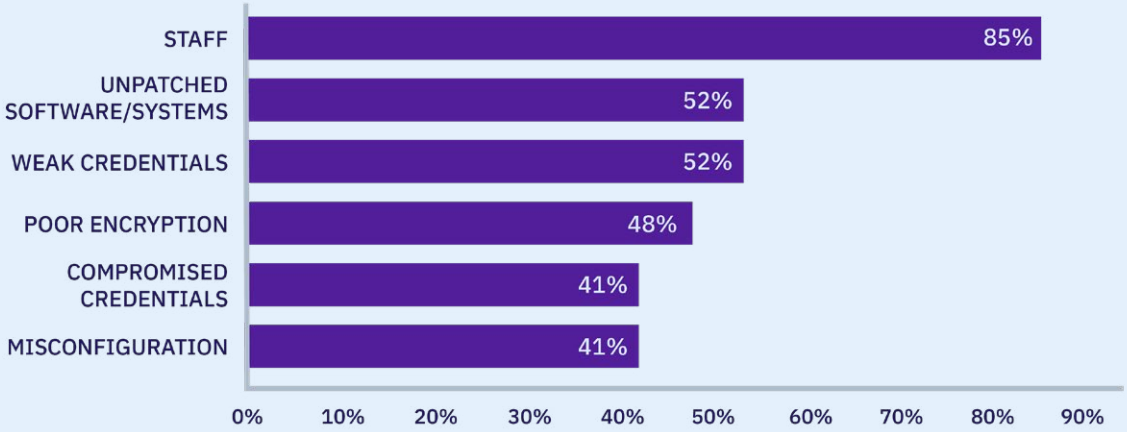


The NGOs were asked to provide their insights into what they perceive to be the main risk factors for their organizations. The findings were that:

85% think that their staff pose a significant risk.

52% identified unpatched software, systems and weak credentials as significant risks.

Significant Vulnerability Risks (as percieved by NGOs)



Besides demonstrating a general awareness level amongst the NGOs participating in the current analysis, these figures indicate that cybersecurity has become a serious concern for NGOs.

Moreover, these concerns reflect findings detailed by the Swiss National Cyber Security Centre (NCSC), which details ransomware gateways as including poorly secured systems and emails with attachments.[3] This is also underscored by the UK National Cyber Security Centre in their Annual Review 2021, where it was observed that threat actors were increasingly exploiting vulnerabilities in virtual private networks (VPNs), unpatched software and using phishing emails specifically to deliver ransomware.[4]

Actual Incidents

In general, information about actual cyber incidents is rarely made public, thus the report survey asked NGOs if they had been the victim of a cyberattack. The findings in this regard are that:

41% of NGOs report that they have been the victim of a cyberattack within the past three years.

The most prolific attacks include social engineering (e.g. phishing), ransomware, Denial of Service Attacks (DDoS) and other malware. Other reported attacks included CEO fraud, website impersonation, spyware, Man-in-the-Middle (MITM) and brute-force attacks.

Of those that had experienced cyber incidents, **100%** reported that these attacks were not isolated events, with some experiencing cybersecurity incidents daily while others face them on a monthly or annual basis.

The attacks led to a range of adverse impacts on the NGOs, including financial losses, compromised financial data, disruptions to external engagements, disruptions to staff activities and to staff time, and the necessity to revise procedures.

In order to gain a better understanding of the actual impact of cyberattacks, three case studies are presented later in this report. The case studies are based on interviews with three of the surveyed NGOs and look into the specific circumstances of the cyberattacks they experienced. These case studies provide valuable insights into the threat landscape faced by NGOs and the need for effective responses.

Resilience and Incident Response

Findings show that **70% of NGOs** don't think, or aren't sure whether, they have an adequate level of resilience to recover from a disruptive cyberattack. When asked about their capacity to monitor cyber risks and respond to incidents:

- **70% of NGOs** do not have any incident response, analysis or investigative in-house capabilities in the case of a cyberattack.
- **63% of NGOs** do not monitor the clear or dark web for leaked credentials or compromised accounts/infrastructure.
- **37% of NGOs** do not believe they have the capability, or are uncertain about their capacity, to detect potential security incidents or suspicious activity.
- **15% of NGOs** indicated that they never conduct security assessments or audits of their cybersecurity infrastructure.
- **33% of NGOs** indicated that they have acquired, or plan to acquire cyber insurance.

Organizational Readiness

Human Resources

The report survey aimed to gauge the distribution of different IT and cybersecurity expertise roles (people and skills) within the organizations. This is crucial for understanding the capacities and capabilities of the NGOs in managing and mitigating cyber threats.

NGOs were asked to identify which of the following roles existed within their organization: IT support; systems administrator; data protection officer; cyber security expert; information security officer; other.

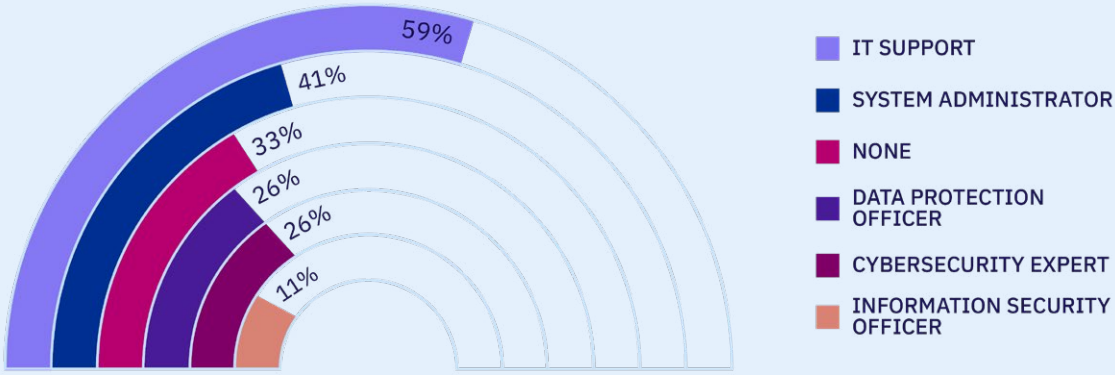
The results demonstrate a range of cybersecurity and IT expertise across the surveyed NGOs.

33% of NGOs overall report having no IT support or technical expertise.

15% of NGOs have cybersecurity experts.

- IT Support is the most commonly reported expertise, identified in **59% of NGOs**, indicating at least a foundational level of IT capability.
- System administrator expertise is reported by **41% of NGOs**, demonstrating a structure in their approach to IT and cybersecurity.
- **26% of NGOs** have a data protection officer in their organization.
- Only **15% of NGOs** have cybersecurity experts, and **11% of NGOs** have an information security officer.

Organisational readiness (Human Resources)



Organizations lacking such support are likely to have considerable difficulty managing their cybersecurity posture, and mitigating or responding to cybersecurity incidents. Without a dedicated cybersecurity team, NGOs may struggle to conduct regular risk assessments, identify potential weaknesses in their systems, and implement robust security measures. Moreover, the absence of IT and cybersecurity experts hampers the organization's ability to stay abreast of evolving threats and industry best practices. In the event of a cybersecurity incident, such as a data breach or a ransomware attack, the absence of specialized personnel can exacerbate the impact, leading to prolonged downtime, data loss, and reputational damage.

IT and cybersecurity professionals play a crucial role in proactively implementing preventative measures, monitoring for anomalies, and responding promptly to mitigate the effects of an attack. NGOs without cybersecurity staff face a higher risk of falling victim to cyber threats and may struggle to recover without the necessary expertise to navigate the complexities of the digital landscape.

- Reviewing the results by organizational size, **88% of NGOs**, which are classified as micro-size enterprises by the OECD (defined as businesses with fewer than 10 employees), report having no dedicated IT or cybersecurity expertise. In contrast, larger organizations tend to possess broader expertise, suggesting a relationship between organization size and technical capability.

  However, one organization within the medium-sized enterprise category, which the OECD defines as having between 50 and 249 employees, also reports having no IT support or cybersecurity expertise, which represents a significant exposure given the size of the organization. This emphasises that a shortage of expert staff, whether due to budgetary constraints or lack of recognition of the necessity for such expertise, is not confined solely to smaller organizations.

Financial Capacity

Investing in cybersecurity ensures that an NGO can keep its systems and software up-to-date, by implementing the latest security measures to defend against evolving cyber risks. Allocating financial resources to enable the necessary people, skills, policies, processes, and tools in cybersecurity is an investment in safeguarding the organization's confidentiality, availability and integrity. In particular, ensuring operational resilience, and upholding the trust of beneficiaries, staff, donors and partners.

- **56% of NGOs** report not having a budget allocated for their cybersecurity needs, which is consistent with the low levels of technical and cybersecurity capacities found in many of the surveyed organizations.

Processes

Developing robust cybersecurity processes is a crucial step towards protecting sensitive data, preparing for and defending against evolving threats, and upholding the trust of different stakeholders.

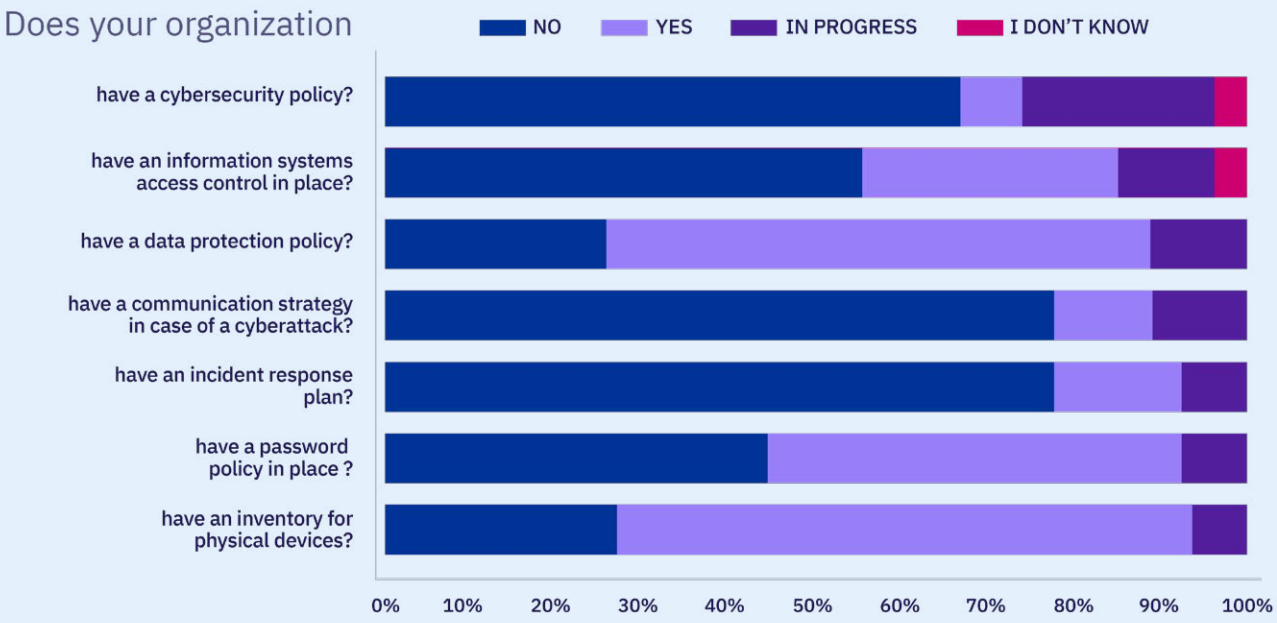
- Only **4% of NGOs** report currently having a cybersecurity policy. A cybersecurity policy outlines how an organization safeguards itself against and responds to cyber threats. It serves as a vital framework that encompasses various aspects of cybersecurity, including systems access control, incident response, inventory procedures,

password management and data protection. An effective policy can help organizations to comply with regulatory requirements and reduce their risk of falling victim to cyberattacks.

• Components of such a policy are being implemented to a varying degree across the organizations. For example, **48% of NGOs** indicate the presence of a password policy, **63% of NGOs** have established a data protection policy and **30% of NGOs** report having an information systems access control policy.

78% of NGOs report that they do not have an incident response plan (IRP).

• **26% of NGOs** report that they do not keep an inventory of physical ICT assets. The foundational security of any organization's cybersecurity environment relies on knowing what assets they own and manage, what their status is, where they are located, and who is responsible for them.



Hosting Environment and Data Location

Cloud-based and on-premise hosting are both ways to store and manage digital resources including data, websites and emails. On-premise hosting involves storing, controlling and maintaining servers within an organization's own physical infrastructure. For example, an organization may decide to deploy a mail server within their own network environment. Cloud-based solutions instead rely on the use of external infrastructure belonging to a third party. For example, an organization may use a cloud based email management solution that does not require them to update, manage or maintain the mail server. On-premise hosting is typically less cost-effective and scalable than cloud-based hosting, but can provide higher levels of control and security if configured and maintained according to best practice recommendations. Taking these factors into consideration, organizations may decide to use one, or a combination (hybrid) of the two solutions, in order to cater to their specific requirements.

Whether using on-premise, hybrid or cloud storage solutions, NGOs must ensure that access control is properly configured, activity is logged and user accounts are managed to mitigate unauthorized access to sensitive data. The report survey findings show that:

- **92% of NGOs** host sensitive data either in the cloud (**44%**), or in a mixture of cloud-based and on-premise solutions (**48%**).

82% of NGOs use a cloud-based email server.

89% of NGOs use external hosting for their main domain/website.

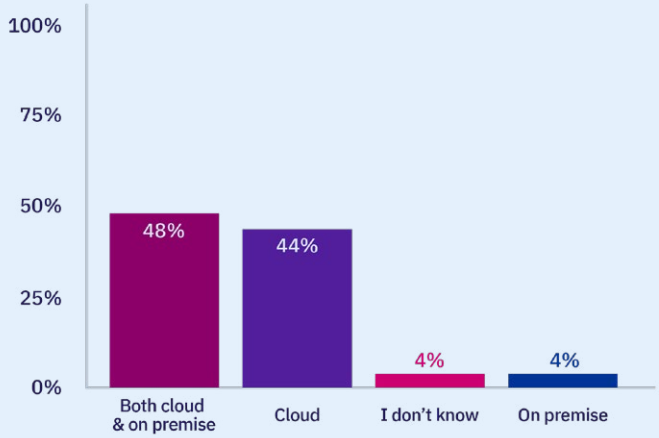
- Among external domain/website hosting users, **42% of NGOs** opt for a shared hosting solution, **13% of NGOs** have dedicated hosting and **4%** use a combination of both. The remaining organizations were unable to confirm which type of external domain/website hosting they use.

It is important to note that the global distribution of an organization's assets such as web servers, may not be limited to the country in which an organization is physically located. Organizations may choose to use servers hosted at data centres in various countries depending on factors such as costs, latency, service providers, the nature of data they are handling, regulations and service delivery requirements.

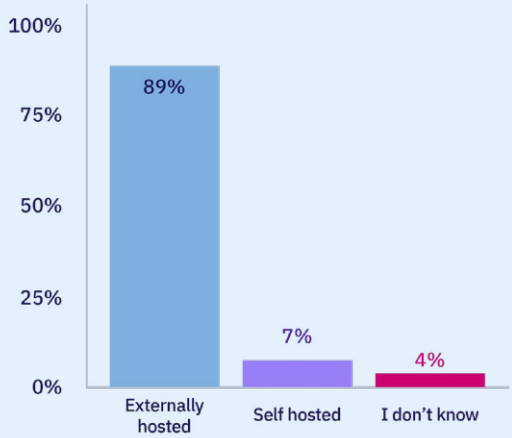
Organizations may also rely on the distributed infrastructure of parent and partner organizations, or require temporary deployments of networking devices and servers for remote satellite offices.

Understanding where an organization's internet facing assets are located is fundamental for the successful implementation of any organizational security setup. Knowing the location of assets can also provide insights into how organizations may be exposed to certain types of other risks, for instance, those stemming from geopolitical and geographical factors. For example, if servers are hosted in countries engaged in an armed conflict, prone to natural disasters or with power supply constraints, there may be additional controls and processes required to mitigate potential server downtime.

Sensitive Data Storage Location



Website Hosting



Technical Analysis

As part of this study, the surveyed NGOs were asked to take part in a technical analysis of their organizations' internet-facing assets, to assess if there were identifiable cyber threats and vulnerabilities.

The participating NGOs shared details about their infrastructure, including their use of web, email and database servers. By using the organizations' domain and IP information, passive scan data was gathered from partner platforms and from open source tools. This data provides an additional perspective on the visibility and variety of internet-facing assets used by the organizations. Importantly, these are the same devices that potential adversaries can also detect when scanning a target's environment.

The analysis of this technical information was carried out by the Institute experts but is not included in this report in order to avoid

exposing vulnerabilities. The NGOs that participated in the analysis are being supported by the CyberPeace Builders program to have the results of their technical analysis reviewed and appropriate responses put in place.

The analysis evaluates key security components of the NGOs' internet-facing assets, including exposed user credentials, email authentication and security, Common Vulnerabilities and Exposures (CVEs), Domain Name System (DNS) configurations, TLS/SSL certificates, open ports, and server software versions:

Tackling the Threat

The appropriate management and protection of data and ICT systems is essential for any organization but can hold even greater importance for NGOs, given the sensitive nature of the information they hold on highly vulnerable people and other stakeholders, such as donors.

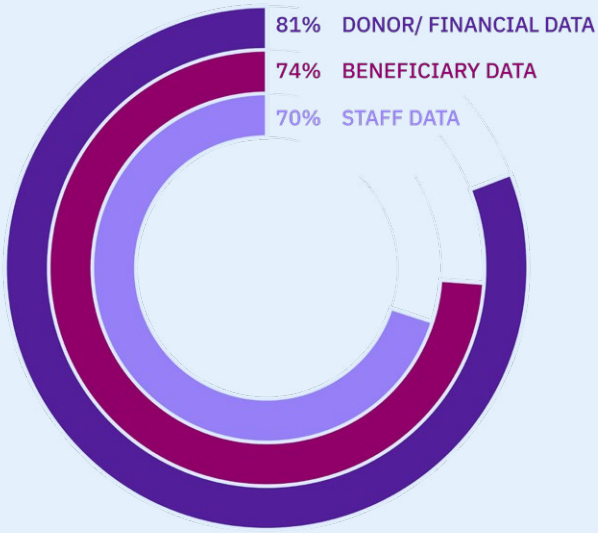
A data breach could result in the loss of data concerning their staff and operations, and also potentially sensitive information related to beneficiaries. NGOs must also be aware of their legal and regulatory obligations with regard to the protection of data in the jurisdictions in which they are hosted and operating.

The survey explored the types of data NGOs consider as being critical and requiring protection.

- 81% of NGO indicated Donor/Financial Data
- 74% of NGOs indicated Beneficiary Data
- 70% of NGOs indicated Staff Data

Given that NGOs hold sensitive data, employing measures and procedures designed to safeguard an organization's critical assets is essential.

Active cybersecurity measures can be used by organizations to mitigate threats. Organizations can implement active cybersecurity measures at a variety of levels across their ICT systems. In terms of infrastructure this may include anti-virus protection, regular backup procedures, enforced use of a VPN and the use of active firewalls, among others.



Account and Software Management

Organizations can immediately mitigate threats by keeping key systems and software updated, removing software that is no longer used or supported, and by removing/disabling unnecessary user accounts.

22% of NGOs do not update key software.

52% of NGOs do not require IT approval for software installations.

41% of NGOs do not remove software if it is no longer supported.

96% of NGOs report that they remove or disable unnecessary user accounts.

Managing user accounts is a fundamental aspect of maintaining a secure digital environment. By regularly reviewing and eliminating unnecessary accounts, NGOs demonstrate a proactive approach to reducing the attack surface and minimizing potential vulnerabilities.

Unused or outdated accounts can become vectors for unauthorized access, making them potential targets for malicious actors. Removing or disabling these accounts helps organizations prevent unauthorized access, data breaches, and other security incidents. This practice aligns with the principle of least privilege, ensuring that individuals

have only the necessary access rights for their roles. Overall, the high percentage of NGOs engaging in this security measure reflects a conscious effort to enhance their cybersecurity posture, safeguard sensitive information, and mitigate the risk of unauthorized access or exploitation of their systems.

Backup Procedures

By regularly keeping data backed-up in a safe environment, organizations have the ability to restore systems to a working condition in the event of infrastructure failure or disruptions. Examples of common scenarios that can lead to such a failure include systems and devices failing or crashing, cyberattacks (e.g. ransomware or DDoS attacks), and natural disasters (e.g. floods, fires and earthquakes). Even if the organization is not directly affected by these events, it may still experience downtime if its cloud or managed service provider is affected.[5]

82% of NGOs indicated they have a regular backup procedure in place.

While regular backup procedures are essential for protecting data, organizations also need to have a plan for restoring their data in

the event of an incident, such as a data breach or other emergency. Disaster Recovery (DR) exercises can help organizations to assess and refine their backup plans during simulated scenarios. Running such exercises can improve the reliability and functionality of backup plans and enhance organizational preparedness in the event of an actual disaster.

NIST Special Publication 800-84[6] is a guide on testing, training, and exercise programs for IT plans and capabilities. The publication guides organizations through creating and evaluating training, testing and exercise events with the objective of helping personnel prepare for adverse situations involving IT. This guide is a valuable resource for organizations of all sizes looking to improve their disaster recovery preparedness.

Other Active Cybersecurity Measures

Anti-virus solutions can detect, contain and remove potentially malicious applications from computers in an environment. Next Generation Endpoint protection (NGAV) anti-virus is particularly important, as it monitors for behavioural indicators commonly associated with active malware infections. NGAV provides users with enhanced protection within their organizational environment, ensuring safety even when networked devices are compromised and malicious entities attempt to propagate across the networks.

41% of NGOs report either not having next generation anti-virus protection software on all their organization's devices or are uncertain about its use.

Firewalls are virtual or physical devices/programs that control the flow of network traffic between networks or hosts to employ differing levels of protection.[7] They can serve as an important layer of security for organizations, whatever their size, protecting networks against unauthorized access. Every operating system, whether it's Windows, Mac OS or Linux, comes with its own built-in firewall, and it's crucial to have it activated. Additionally, it is crucial to have a cloud-based Web Application Firewall (WAF) in place to protect web services.

41% of NGOs report they either lack an active firewall on all their organization's devices or are uncertain regarding their usage.

Password managers help users generate and store multiple passwords for their online accounts. Password managers encrypt this information in a secure 'vault', only accessible to those with rights access.

37% of NGOs report either not using a password manager, or are uncertain about its use.

Virtual Private Networks (VPNs) create a secure tunnel that can access internal resources, safeguarding online activities by encrypting data and providing a level of anonymity by masking an organization's IP address.

- **19% of NGOs** report that VPN use is partially enforced.

56% of NGOs report that their organizations either do not enforce the use of a Virtual Private Network (VPN), or are uncertain about its use.

Multi-Factor Authentication (MFA) is a security process that requires using two or more different factors for authentication and can be an effective method to prevent password and identity theft.

- **7% of NGOs** report that they use MFA partially across their key platforms.

33% report either not having MFA activated across key platforms used in their organization's daily work, or are uncertain about its use.

Data Loss Prevention (DLP) is a security solution that protects sensitive data from unauthorized sharing, transfer, or use. DLP can help organizations monitor and secure sensitive data across on-premises systems, cloud based locations, and endpoint devices. DLP can also help organizations comply with regulations such as the General Data Protection Regulation (GDPR).[8]

78% of NGOs report either not having any DLP tools in place, or are uncertain about their use.

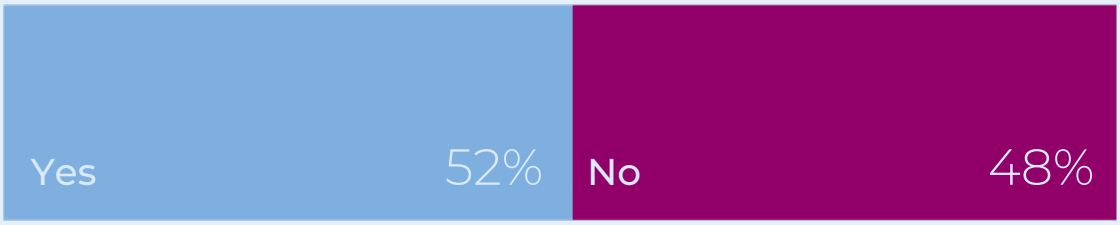
Training

Training is an essential tool for tackling cyber threats. Providing staff members with the knowledge and skills to recognise and take appropriate action against cyber incidents vastly improves the cybersecurity posture of any organization.

85% of NGOs think that their staff poses a significant risk in terms of cybersecurity.

52% of NGOs conduct regular cybersecurity awareness training.

Do your employees receive regular cybersecurity awareness training?



Security awareness and training programs can teach staff members about common cyber threats (e.g. phishing and ransomware), security best practices (e.g. password hygiene), how to report incidents and organisational policies.

Social Engineering

Despite the high rate of concern cited by NGOs that social engineering and staff members pose significant risk, only **52% of NGOs** report conducting regular cybersecurity awareness training. Furthermore, only **48%** report carrying out phishing exercises for staff members.

78% of NGOs consider social engineering to be a main threat.

48% of NGOs conduct phishing exercies for all staff.

Social engineering attacks can range from generalised schemes, aimed at wide audiences, to highly crafted campaigns trying to exploit the particular vulnerabilities of a specific target. Cybersecurity awareness sessions can play a key role in educating staff members about the various social engineering tactics employed by malicious actors. Specific exercises, focused on phishing attacks, can further improve an organization's readiness by simulating real-life phishing scenarios that encourage vigilance and train staff to recognise suspicious communications.

In Case Study #1, we provide an example of a ransomware attack against an NGO, which was initiated through a phishing email.

As described in NIST Special Publication 800-123, "making users and administrators aware of their security responsibilities and teaching the correct practices helps them change their behaviour to conform to security best practices. Training also supports individual accountability, which is an important method for improving information system security".[9]

Part 5

Case Studies

Case Study #1: Ransomware attack on an NGO

1. Overview

An NGO based in Geneva that provides services to other local and international associations faced a ransomware attack in the winter of 2020, which resulted in over a week's worth of operational data being lost. This case study delves into the details of what happened during the attack, the organization's response, the impact on its operations, lessons learned, and recommendations for future cybersecurity preparedness.

2. What happened?

In January 2020, a staff member was checking their emails and accidentally opened a PDF file containing malware, leading to the complete encryption of their data, by a threat actor. The perpetrators used a generic email with the PDF in attachment to launch the attack. The NGO does not believe it was specifically targeted by the attackers.

The infection initially started on one workstation and subsequently spread to the organization's server. The server stored crucial data, including booking information, financial and accounting data, and personal data of staff members. The attackers demanded a considerable sum of money, in bitcoin, for the decryption of the data.

The attack involved a ransomware referred to as REvil (Ransomware Evil). This ransomware was first discovered in April 2019 and has been responsible for numerous high-profile cyberattacks. REvil encrypts files on the victim's computer or network, making them inaccessible, and REVIL ransomware operators demand a ransom payment from their victims in exchange for the decryption key.

Malware is a malicious software. These are pieces of code designed to damage, destroy, or subvert computer systems. Malware includes viruses that can replicate and stop systems from working.

Ransomware is a type of malware designed to extort money by encrypting/blocking access to files or the computer system until a ransom is paid.

The NGO had never previously dealt with a cybersecurity incident like this. At a personal level, the employee who opened the link was both alarmed by what had happened and also angry about being deceived. As described by the Director of the NGO, *"My colleagues got scared when confronted with this. The colleague who opened the email containing the malware started to feel guilty. We all did our best to reassure them. But there was this feeling of vulnerability, of being exposed."* All colleagues and management were supportive, promoting a strong "no blame" culture.

What is a ransomware attack?

A ransomware attack is a type of malicious cyberattack in which a perpetrator encrypts a victim's data or files, rendering them inaccessible, and then demands a ransom payment from the victim in exchange for a decryption key or a promise to restore access to the data.

- Ransomware typically gains access to a victim's computer or network through various means, such as malicious email attachments, infected software downloads, or exploited vulnerabilities in software or systems.
- Once the ransomware infiltrates the victim's system, it begins encrypting files, making them unreadable without a decryption key. This encryption process can affect a wide range of files, including documents, images, databases, and more.
- After encrypting the victim's files, the attacker displays a ransom note on the victim's screen or leaves a text file with instructions on how to pay the ransom. The note typically includes the ransom amount, the cryptocurrency (e.g. Bitcoin), wallet address for payment, and a deadline for payment.

3. Response

The NGO contacted its IT provider for guidance as it did not have an internal person in charge of cybersecurity or IT. The NGO was advised to immediately disconnect the server from the network until a technician arrived in person. Hoping that its backup would restore

its systems and operations, the NGO chose not to engage with the cybercriminals or to pay the ransom demanded. However, while the backup was successful, it had not been updated with the last weeks' worth of operational data, which was lost as a result.

Recommendations to deal with a ransomware attack

Technical recommendation

- Implement automated and regular data backups of critical systems and data. Regularly test backups to ensure their integrity and reliability.
- Ensure backups are stored in an offline or offsite location, disconnected from the network.
- Deploy advanced endpoint security solutions that include behavior-based detection mechanisms to identify ransomware activity in real-time.
- Use email filtering solutions to detect and block malicious email attachments and links.

Strategic recommendations

- Develop a robust backup and recovery strategy as part of the organization's business continuity plan.
- Develop and enforce a cybersecurity policy that includes employee training on identifying phishing emails and maintaining strong password hygiene.
- Ensure key stakeholders, including IT personnel, legal counsel, and management, are aware of their roles and responsibilities in the event of an attack.
- Establish communication channels and contact information for external entities such as law enforcement and cybersecurity experts.

Ransom payments

The NCSC recommends that organizations not pay ransom demands, as there is no guarantee the criminal party will uphold their terms and paying ransoms encourages future attacks. For any Swiss organisations faced with a demand for a ransom payment, the NCSC urgently recommends discussing this with the cantonal police.[10]

4. Impact

This ransomware attack had several notable impacts on the organization:

i. **Data recovery:** Some data was lost. The organization managed to recover a part of its data, but it required a significant amount of time and effort.

ii. **Financial impact:** The attack disrupted the organization's budget planning and led to unexpected expenses, such as purchasing additional security measures and conducting employee training.

iii. **Operations:** The attack temporarily disrupted the organization's server and one employee's computer, in addition to losing one week's worth of operational information and data.

iv. **Cybersecurity awareness:** The incident highlighted the organization's vulnerability to cyberattacks, prompting them to take cybersecurity more seriously. They made the decision to invest in cybersecurity insurance shortly after this attack.

v. **Harm:** Distress on the employee and his colleagues.

5. Lessons Learned

Some of the key lessons learned by this NGO after this incident include:

i. **Training and awareness:** Regular cybersecurity training and awareness programs for employees are essential to protect against future attacks.

ii. **Data backup and recovery:** Ensuring proper data backup and recovery procedures are in place are crucial to safeguard against data loss during an attack.

iii. **Cybersecurity insurance:** Investing in cybersecurity insurance can help mitigate financial losses in the event of a cyberattack.

Case Study #2: **Attack on an NGO website**

1. Overview

This case study is about a small NGO based in Geneva whose mission is to provide professional and independent services to assist humanitarian and development organizations in their work. The organization's website serves as a central platform for communication with partners and clients.

In early 2020, this NGO experienced a cyberattack resulting in the compromise of their website, causing significant disruption to their operations. This case study explores the details of the attack, the organization's response, the impact on their operations, lessons learned, and recommendations.

2. What happened?

In early 2020, the organization fell victim to a website attack. When trying to connect to the website, they discovered that they were automatically redirected to a Chinese language marketplace website. The exact timing of the attack remains uncertain, as it was discovered during a period of reduced monitoring.

Unfortunately, the organization did not have a backup of their website, requiring a full reconstruction of the site which took nine months to complete. While the organization does not believe that they were deliberately targeted by the cyberattack, it appears the attackers were aiming to generate traffic to the marketplace website. The identity of the threat actor remains unknown, and there is no attribution or evidence linking any individual or group to the attack.

What is a website attack?

A website attack refers to a malicious activity or series of actions aimed at compromising the security, functionality, or availability of a website or web application. These attacks target vulnerabilities in websites to gain unauthorized access, steal data, deface web pages, disrupt services, or carry out other malicious activities. Website attacks are typically orchestrated by cybercriminals, hackers, or other threat actors.

There are different types of website attacks. Some of the most common ones include:

- **SQL Injection (SQLi)**: In an SQL Injection attack, an attacker injects malicious SQL queries into input fields on a website.
- **Cross-Site Scripting (XSS)**: XSS attacks involve injecting malicious scripts into web pages viewed by other users.
- **Cross-Site Request Forgery (CSRF)**: In CSRF attacks, attackers trick users into unknowingly executing actions on a website without their consent.
- **Distributed Denial of Service (DDoS)**: DDoS attacks flood a website's server with a massive volume of traffic, overwhelming its resources and causing it to cease functioning normally or to become unavailable to legitimate users. It is said to be distributed when the source of the attack is composed of a multitude of devices or systems.
- **Website Defacement:** The illicit or unauthorized modification of the appearance and content of a target's website or the act of redirecting traffic to other web pages.

3. Response

In the wake of the website attack, the organization's response was marked by an initial sense of panic, but swiftly transformed into a determined effort to address the situation. The organization embarked on reconstructing their website from the ground up, a process that demanded extensive time and resources. To mitigate the risk of future breaches and regain a sense of trust and security, the organization changed their web hosting provider. Throughout this incident response, the organization demonstrated transparency and accountability by promptly informing external stakeholders, and its board members, about the incident. The absence of backups meant that the organization lacked a vital component of an effective incident response strategy, underscoring the importance of preparedness in the face of unforeseen cybersecurity threats.

Recommendations to deal with a website attack

Technical recommendations

- Maintain frequent and up-to-date backups of the organization's website data and configurations. Implement an automated backup

system that includes both the website files and the associated database.

- Keep all website software, plugins, and themes up to date. Regularly apply security patches and updates to mitigate vulnerabilities that attackers may exploit.
- Deploy a Web Application Firewall (WAF) to filter and block malicious traffic, including common attack patterns like SQL injection and cross-site scripting (XSS).
- Implement Multi-Factor Authentication (MFA) for all administrators and users with access to the website's Content Management System (CMS) or backend.
- Security Headers: Implement security headers, such as Content Security Policy (CSP) and HTTP Strict Transport Security (HSTS), to enhance the website's resilience against various types of attacks.

Strategic recommendations

- Develop a comprehensive Incident Response Plan (IRP) that outlines the steps to take in case of a website attack. Assign roles and responsibilities, and conduct regular drills to ensure readiness.
- Train your staff and volunteers on cybersecurity best practices, such as recognizing phishing emails and maintaining strong passwords.
- Implement continuous website monitoring to detect suspicious activities or traffic anomalies promptly. Set up alerts for security incidents and respond swiftly to any anomalies.
- Enable Hypertext Transfer Protocol Secure (HTTPS) for your website to encrypt data in transit, protecting user information and enhancing trust.
- Establish a clear process for reporting security incidents both internally and, if necessary, to relevant authorities.
- Consider obtaining cybersecurity insurance to help cover potential financial losses in case of a security breach.
- Conduct regular security audits and risk assessments to identify and address emerging threats.

4. Impact

The ramifications of the cyberattack on the organization were wide-reaching and profound. Firstly, the attack had a detrimental impact on the organization's image and credibility, as their website remained unavailable for an entire month. During this period, the organization's stakeholders, including partners and clients, were left with a sense of uncertainty, eroding the trust they had previously enjoyed. Internally, the attack led to significant operational disruptions, with communication channels being severely affected, impacting the efficiency and effectiveness of the organization's day-to-day activities.

Furthermore, the attack disabled a contact form which hindered interactions with possible collaborators, potentially and temporarily impeding future partnerships with other NGOs. Lastly, the process of reconstructing the website imposed considerable financial costs on the organization, including expenses for web development, hosting, and security measures.

These multifaceted repercussions underscore the critical importance of robust cybersecurity measures and incident preparedness in safeguarding an organization's reputation, operations, and financial stability.

5. Lessons Learned

Some of the key lessons learned by this NGO after this incident include:

i. **Maintaining up-to-date backups** of their digital assets - a fundamental precautionary measure often overlooked until a crisis unfolds. The experience also underscored the necessity to regularly monitor and implement website updates and patches, reinforcing the imperative of proactive security maintenance.

ii. **Ensure robust relationships** with service providers, emphasizing the need to consistently verify the adequacy of their security measures.

iii. **Enhance staff awareness** within the organization regarding the ever present cybersecurity threats and vulnerabilities, reaffirming the importance of continuous education and vigilance in safeguarding against potential breaches.

Case Study #3: A Man-in-the-Middle cyberattack against an NGO

1. Overview

The organization in this case study is a medium-sized non-governmental organization (NGO) based in Geneva. In September 2019, this organization fell victim to a Man-in-the-Middle (MitM) cyberattack. A MitM is a type of cyberattack in which a malicious actor intercepts, with the potential of altering, the communication between two parties without their knowledge or consent. This case study explores the details of the attack, the NGO's response, the impact it had, lessons learned, and recommendations for other NGOs facing similar threats.

2. What happened?

In September 2019, shortly after the summer holidays, the NGO's finance department started following up on pending invoices. They noticed that they had not received payment from an overseas Foundation they worked closely with. The finance team followed up with the Foundation, mentioning that the payment had not been made. The Foundation responded to the NGO confirming that they had paid, with proof of payment. The NGO noticed that on these emails, the domain of the emails contained the characters “nn” in the place of “m” and that a spoof domain was being used. This is when the NGO realized that they were the victims of a MitM cyberattack.

Upon further investigation, the NGO realized that the Foundation had received a second email with the same invoice but with different banking details on the invoice. The attackers skillfully edited a PDF invoice and set up a spoof domain with an optically close name resembling the NGO’s real domain. This false domain was used to send a second email with the same email addresses in “to” and “cc” as the original email but all on the spoof domain.

This incident occurred during a period when many employees were on holiday, reducing the likelihood of immediate detection, and indeed the Foundation paid the invoice to the modified banking details. The NGO believes that the attackers intercepted an email either during its transmission from the NGO or upon reception at the Foundation. This

was probably done through compromised email boxes either at the NGO or the Foundation.

At the same time, the NGO received two similar emails with spoof domains and modified bank details, however the NGO noticed the spoof and did not pay the invoices to the modified banking details. In all three cases, the modified banking details referenced the same branch of an international bank.

What is a Man-in-the-Middle / email intrusion cyberattack?

In a MitM attack, the attacker secretly positions themselves between the sender and receiver of data, allowing them to eavesdrop on the communication, steal sensitive information, or manipulate the data being exchanged.

As a result of a MitM attack, cybercriminals can:

- **Create Email Forwarding Rules:** Attackers may create forwarding rules within an email account, which automatically forward copies of incoming emails to an external email address controlled by the attacker.
- **Access Sent Items:** Cybercriminals can access a victim's sent items to gather information on the emails the victim has sent, including any sensitive data or attachments.
- **Compromise Business Emails:** Business Email Compromise (BEC) attacks involve compromising the email accounts of high-level employees in an organization to impersonate them and authorize fraudulent transactions, such as wire transfers.
- **Steal Data:** Attackers may use email intrusion to steal sensitive data, such as personal information, financial data, intellectual property, or login credentials for other online services.
- **Invade NGO's Privacy:** Intruders may invade the privacy of individuals or organizations by accessing and reading their email correspondence.

3. Response

The NGO's initial response to the MitM attack was characterized by confusion and concern. An in-depth forensic investigation was initiated by the IT departments of the NGO and the Foundation,

which both revealed the same timeline. Within hours of the initial email with the attached invoice being sent, a dummy domain had been registered and the spoof email sent to the Foundation. The NGO began an internal investigation to determine the source and extent of the cyberattack. They identified that some unauthorized rules were set on the email accounts of some employees including that of the Finance Deputy Director. The NGO believes they were particularly targeted due to the size of the NGO and the industry it operates in.

The NGO received assistance to tackle this attack from their external IT provider, in addition to the efforts of their IT/cybersecurity team. After contacting the Serious Fraud Office in the UK, the NGO could not identify the cybercriminals, however they were able to provide the bank details used in the successful attack and the two unsuccessful attempts. A few months later the bank reimbursed the funds to the Foundation.

To prevent future similar attacks, the IT team in the NGO enacted policies that block any rules that forward information externally (outbound auto-forwarding block), as well as other technical measures. Additionally the finance department implemented supplementary controls, including that invoices are only sent from the finance mailbox to the recipient, without copying any NGO staff members on the email.

Additionally, the NGO finance department reaffirmed that the NGO will only make payments to the bank account provided by a vendor at the time of signing the initial contract. Changes in bank details must be provided to the NGO independently of invoicing.

Recommendations to deal with a MitM attack

Technical recommendation

- Implement strong encryption protocols (e.g. TLS/SSL) for data in transit, especially for web browsing, email, and sensitive communications.
- Implement a Public Key Infrastructure (PKI) system to securely manage and distribute digital certificates for websites and services.
- Implement email security measures, such as SPF, DKIM, and DMARC, to prevent email spoofing and phishing attempts. Use end-to-end encrypted email solutions when handling sensitive information.

- Employ intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious activity indicative of MitM attacks.
- Require MFA for accessing critical systems and sensitive data to prevent unauthorized access even if credentials are compromised.
- Keep all software, including operating systems, web browsers, and security software, up-to-date with the latest security patches.

Strategic recommendations

- Train employees and users to recognize the signs of MitM attacks and practice safe browsing and email habits. Encourage reporting of any kind of suspicious activity.
- Implement the principle of least privilege (PoLP) to restrict user access to only the resources necessary for their roles.
- Assess the security practices of third-party vendors, especially those providing critical services or software that could be vulnerable to MitM attacks.
- Consider adopting a Zero Trust Network Access (ZTNA) approach, which assumes that no entity—whether inside or outside the network—is trusted by default.
- Evaluate the need for cybersecurity insurance to provide financial protection in case of a MitM attack or other security incidents.

4. Impact

This MitM attack had several significant impacts on the organization:

i. **Financial Loss:** Both the Foundation and the NGO incurred a financial loss due to the fraudulent payment. This was later recovered but the NGO was not expecting the recovery.

ii. **Operational Disruption:** The attack disrupted the NGO's internal operations and caused confusion at the Foundation and the NGO as neither initially understood what had happened.

iii. **Reputation Damage:** The incident had a potentially negative impact on the NGO's reputation, raising concerns amongst management and the board.

iv.. **Awareness:** Staff members felt both concern and guilt, and there was a need for increased awareness of cybersecurity threats.

5. Lessons Learned

The cyberattack taught the organization several valuable lessons:

i. The importance of **verifying and cross-checking payment details**, especially for invoices involving significant amounts.

ii. The need for enhanced **staff awareness** and training to recognize and respond to phishing attacks.

iii. The implementation of **rules and processes** for handling financial transactions securely.

iv. The importance of taking swift action to secure email accounts and applying **Multi-factor Authentication** (MFA) to enhance email security.

Appendices

Appendix A: Detailed recommendations

Organizational recommendations

■ NGOs should have a specific cybersecurity policy tailored to their organization. A cybersecurity policy outlines how an organization safeguards itself against and responds to cyber threats. It serves as a vital framework that encompasses various aspects of cybersecurity, including systems access control, incident response, inventory procedures, password management and data protection. A cybersecurity policy should involve the senior leadership, as its main goal is to protect the organization's strategic assets. Without the backing of senior management, cybersecurity policies and rules are less likely to be effective.

- An effective policy can help an organization to comply with regulatory requirements and reduce the risk of falling victim to cyberattacks.
- Consolidating the applicable aspects of an organization's cybersecurity into a single, comprehensive policy can ensure consistency, accessibility for staff, and ease of management.
- Ensuring policies are constructed, utilised and properly documented may enhance an organization's eligibility for cyber insurance coverage.

➔ The CyberPeace Institute has created a cybersecurity policy template, which is provided as a free resource for participants in the CyberPeace Builders program. NGOs can adapt this template to their specific organisational profile and needs. Policy topics include; responsibilities, data classification, authentication and access, travel, infrastructure, devices, systems and software policy.

➔ The NIST Cybersecurity Framework and ISO/IEC 270001 are frameworks that can help organizations develop and implement their cybersecurity policy.[11] [12]

■ An inventory of physical assets is the foundational security of any organization's ICT infrastructure and relies on knowing what assets are owned and managed, what their status is, where they are located, and who is responsible for them. The process of keeping a list of devices is important for multiple reasons, including:

- providing the number and type of devices, including servers (web servers, database servers, email servers etc.), users' computers/ phones/tablets, networking equipment (routers, switches, firewalls, etc.), Internet of Things (IoT) devices (security cameras, door locks etc.), printers, and other network-connected devices.
- shows whether the devices are internal or external.
- provides awareness of the location, status and responsible party for each device, allowing for faster identification and mitigation of threats.

➔ The Canadian Centre for Cyber Security (CCCS) publication "Using Information Technology Asset Management (ITAM) to Enhance Cyber Security" provides guidance on the ITAM process - including steps on how to identify, track and manage IT assets.[13]

■ The global distribution of an organization's assets such as web servers, may not be restricted to the country an organization is physically located. Understanding where an organization's internet facing assets are located is fundamental for the successful implementation of any organizational security setup. Knowing the location of assets can also provide insights into how organizations may be exposed to certain types of other risks, for instance those stemming from geopolitical and geographical factors.

■ Ensuring an Incident Response Plan (IRP) is in place is essential for all NGOs. This is a written document, approved by the senior leadership team, that helps organizations before, during, and after a confirmed or suspected security incident. An IRP should clarify roles and responsibilities and provide guidance on key activities. Additionally, an IRP should also include a cybersecurity list of key people who may be needed during a crisis.[14]

➔ NIST's 'Computer Security Incident Handling Guide' is a valuable resource for any organization looking to establish or improve its IRP. The publication provides guidance on establishing incident response capabilities and handling incidents efficiently and effectively. The guidelines are adaptable and can be used regardless of specific operating systems, protocols or applications.[15]

■ NGOs should run security awareness and training programs for all staff members. By teaching users about security risks and how to prevent them, organizations can greatly reduce their risk of compromise.

➔ NGOs can use the NIST Cybersecurity Framework to improve cyber preparedness and increase resilience against cyberattacks. The Framework provides a comprehensive approach to cybersecurity management and can be adapted to the requirements of organisations of any size. The Framework is organized by five key Functions: Identify, Protect, Detect, Respond, and Recover.[16]

➔ Follow guidance and advice provided by the National Cybersecurity Centre (NCSC). The NCSC website is a valuable resource for both individuals and organisations. It provides information and advice on topics including, cyberthreats and incidents, technology considerations, awareness-raising and prevention. NGOs can also use the website to report cyber security incidents and find specific help to address them.[17]

Technical recommendations

Basic Cybersecurity Measures:

- Implement strict account and software management - regularly update software, remove unused software and disable unnecessary user accounts.
- Establish backup procedures to mitigate infrastructure failure from cyberattacks, outages or other unexpected events.
- Identify and use cybersecurity tools, such as Multi-factor Authentication (MFA), Next-Generation Anti-Virus (NGAV) software, Firewalls, Password Managers, VPNs and Data Loss Prevention (DLP) systems.
- Protect websites by using a reverse proxy[18] or cloud-based security service. These solutions can protect websites against a range of threats including Distributed Denial of Service attacks (DDoS).

  DDoS protection services safeguard websites and networks by absorbing or deflecting excessive internet traffic, ensuring that an organisation's online presence remains uninterrupted and secure.
- Encourage users to check if their private and professional email accounts appear in known data breaches using resources like HaveIBeenPwned.
- Schedule regular security audits, performed by external third-party experts.
- Establish Naming Conventions with consistent account naming

rules.

- Regularly review and verify security for external accounts.
- Restrict administrative privileges to a minimal amount of trusted users.
- Implement DomainKeys Identified Mail (DKIM) on mail servers.

➔ Apply to be a member of the CyberPeace Builders. As well as getting free access to the program's network of cybersecurity experts, the program offers free web monitoring services to detect compromised accounts or infrastructure.

Enhanced Cybersecurity Measures:

- Conduct disaster recovery (DR) exercises to identify areas of improvement in case of infrastructure failure from cyberattacks, outages or other unexpected events.
- Organise a Security Information and Event Management (SIEM). A SIEM solution helps organizations detect, analyse and respond to security threats. The technology collects logs from an organization's devices and systems and then analyses them for suspicious activity. As well as helping to stop cyberattacks before they happen, SIEM can also help organizations meet compliance requirements.[19]
- Use a zero trust security model. Zero trust is a cybersecurity approach that focuses on users, assets and resources instead of static network-based perimeters. It assumes no automatic trust based on physical location or asset ownership, requiring authentication and authorisation before granting access. Zero trust adapts to trends like remote working, bring your own device (BYOD) and cloud assets, emphasising individual resource protection.[20] As a final step, Zero Trust Network Access (ZTNA) is likely the most effective approach for achieving both secure and anonymous connections, though it does require substantial configuration.
- Use Domain-based Message Authentication, Reporting and Conformance (DMARC) to prevent spammers from using the domain to send emails without the domain owner's permission.

Appendix B
Methodological considerations

This report is founded on data sourced and analyzed by the CyberPeace Institute from three primary channels:

- primary data through direct engagement with Geneva-based NGOs, through surveys and interviews. The data has been aggregated and anonymized to respect the privacy and security of the participating NGOs.
- data from open sources, collected through open source intelligence techniques and the passive scanning of digital footprints/assets to identify any risks or vulnerabilities, and;
- data collected from a trusted network of partner cybersecurity companies - providing additional insights stemming from secondary datasets such as telemetry data, data breaches/leaks or cybersecurity ratings.

In order to identify the impact cyberattacks have on Geneva-based NGOs, as well as these organizations' readiness and cyber resilience-levels, the methodology employs a mixed-methods approach. A mixed-methods design is a procedure for collecting, analyzing, and mixing both qualitative and quantitative methods and data in a single study to provide a more comprehensive, fact-based solution to the analysis topic. This enables the analysts to learn from, adapt and apply the methodology to other geographical regions around the world, with the purpose of producing knowledge that respects the same analytical standards.

Project scope and participation of NGOs

In March 2023, a total of 44 Geneva-based NGOs were contacted to participate in the study. Out of the 44 NGOs, 27 agreed to take part in the different stages of the analysis, starting with a survey that was submitted by all participants within the timeframe of 3 to 4 weeks.

The NGOs taking part in this project conduct their activities across a range of sectors, including humanitarian, health, justice, human rights, peace and education. These NGOs bring vital aid and services to tens of millions of beneficiaries across the globe. The NGOs operate internationally across various regions, particularly Europe, Africa, the

Middle East and Asia. A number of the organizations also operate in North America, Oceana, Latin America and the Caribbean.

Based on OECD classifications[21] relating to employee count, 67% of NGOs participating in the project fall into the micro or small-size enterprise brackets, and 33% of NGOs are classified as medium or large-size enterprises:

- Micro enterprises, defined as those with fewer than 10 employees.
- Small enterprises, defined as those with 10-49 employees.
- Medium-sized enterprises, defined as those with 50 to 249 employees
- Large enterprises, defined as those with over 250 employees.

This report survey to NGOs encompassed multiple-choice and open-ended questions related to organizational size, sector, ability to detect cyber threats, strategies for protection against such threats, and methods for response and recovery following cyberattacks. An internal team of experts, from the CyberPeace Institute, consulted the NIST Cybersecurity Framework to ensure the surveys were designed according to industry standards, whilst being adapted to the operational needs and realities of NGOs. The survey also leveraged the experience of the Institute's team members who work directly with NGOs through the CyberPeace Builders program. The surveys were conducted in English.

Furthermore, from the 27 NGOs, 6 interviews were conducted with organisations that had direct experience of cyberattacks. These semi-structured interviews gathered qualitative insights with regard to the human-centered understanding of the consequences of cyberattacks. The interviews were conducted in both French and English.

Additionally, 19 of the NGOs participating in the project accepted the analysis team carrying out a technical analysis of their organization's internet-facing assets to assess if there were identifiable cyber threats and vulnerabilities. The NGOs that participated in this project are being supported by CyberPeace Builders program to have the results of their technical analysis reviewed.

The sample size of 27 NGOs allowed for a detailed examination of each participating NGO, providing an understanding of their unique contexts, challenges, and practices. This depth of analysis can yield nuanced insights that may be obscured in larger samples. However, the sample size, which constitutes approximately 6% of NGOs in Geneva,

might not capture the full range of cybersecurity preparedness and threat awareness across the city's NGO community. Additionally, the findings may not be easily extrapolated from the current sample size to other NGOs in different geographical areas, even though general trends can be observed.

Limitations

This report highlights the range of threats NGOs are facing in International Geneva, but does not aim to serve as a comprehensive guide for the issues discussed. Our analysis did not include questions in relation to the NGOs understanding of the legal and regulatory environment in Switzerland and/or the countries they operate in, which although of importance was not the focus. For example, data protection regulations are key considerations for NGOs managing data which must be respected, with reporting obligations in the event of data breaches.

The report purposefully omits detailed information regarding the NGOs that took part in this project. The analysis involved organisations disclosing sensitive information about their vulnerabilities and threat profiles. As such, this precaution is taken to protect the privacy and safety of all the organisations.

This report is not exhaustive and acknowledges that there are other threats, vulnerabilities and actors that come into play from those mentioned herein. There is little available analysis focused on the cyber threat and cybersecurity capacities specific to NGOs. A significant proportion of the analysis currently available is focused on threat actors and their tactics, techniques and procedures (TTPs) with very limited information on victims, targets and the societal impact of attacks. This report advocates systematic and standardized collection, analysis and sharing of information to provide better responses and facilitate international collaboration.

The CyberPeace Institute welcomes any feedback to develop this knowledge product. Any enquiries regarding the Project or interest in the analysis process are welcome, please visit the Institute's website to get in contact.

Appendix C
Glossary

Attack and Cyberattack: A disruptive cyber incident, data breach or a disinformation operation conducted by a threat actor using a computer network or system with malicious intent to cause damage (technical, financial, reputational or other) or extract / steal data without consent.

Backup: Copy of computer data that is kept in a safe environment, to be used in case of infrastructure failure to restore a system to a working condition.

Bitcoin: The first decentralized digital currency/cryptocurrency in which transactions can be performed without the need for a central bank.

Bring Your Own Device (BYOD): A policy allowing or encouraging employees to use their own computer or smartphone for professional activity.

CEO Fraud: Type of phishing attack where the threat actor usurps the identity of a CEO or another high-ranking individual of a targeted organisation.

Computer Emergency Response Teams (CERTs): CERTs are expert groups that handle cybersecurity incidents.

Cloud-based solutions: Refers to applications, storage, on-demand services, computer networks, or other resources that are accessed with an internet connection through another provider's shared cloud computing framework.

Cross-Site Scripting (XSS): XSS are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. Also known as HTML injections.

Cryptocurrency: Digital asset designed to be used as a trustworthy and non forgeable means of monetary exchange.

Cyberpeace: Cyberpeace exists when human security, dignity and equity are ensured in digital ecosystems.

Cybersecurity: The practice of protecting computer systems and networks from unauthorized information disclosure, theft of or damage to their hardware, software, or electronic data. Through the application of technologies, processes and controls, cybersecurity serves to reduce the risk of cyberattack and protect systems, networks and technologies.

Cyberspace: Digital systems and the online world make up cyberspace, which covers everything accessible through computer networks and the internet. This includes everything from corporate networks and social media platforms, to bank accounts and cloud services. It also includes all connected appliances, such as video surveillance cameras, gaming consoles, TV sets or robot vacuum cleaners.

Darknet or Dark web: A darknet is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization (e.g. TOR, Freenet, I2P or ZeroNet) intended to defend digital rights by providing security, anonymity, and censorship resistance. Though it is used for legitimate reasons, it has been heavily used by criminals and the term Darknet nowadays is generally associated with websites (also called onion sites) that are specifically used for criminal purposes.

Data breach: The exposure of confidential, sensitive or protected information to an unauthorised person. This could be accidental, such as a USB drive left on a train or an email attachment sent to the wrong person, but it can also be deliberate, as when malicious actors access a network and exfiltrate (target, copy and transfer) data.

Decryption: Converting encrypted (see definition 'Encryption') data into its original form. It is a process to reverse encryption and put data back into a human-readable form.

Decryption Key: Piece of information needed for the decryption process.

Disinformation: False or misleading information spread – often covertly – with the intention to deceive.

Distributed Denial-of-Service (DDoS): DDoS is an attack technique to flood a network, service or server with excessive traffic to cause it to cease functioning normally. It is said to be distributed when the source of the attack is composed of a multitude of devices or systems.

Domain: On a computer network, a domain is the name given to a computer resource or set of computer resources administered by one given entity.

DomainKeys Identified Mail (DKIM): is used to verify the integrity of an email message by generating cryptographic keys and signing outgoing email messages with a digital signature.

Encryption: Reversible process of converting information or data into an encoded format using mathematical computation algorithms. It is commonly used to protect sensitive information at rest or in-transit so that only authorized parties can view it.

Firewall: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

Hacktivists: Persons or groups that gain unauthorized access to computer files, systems or networks to further social, political or ideological ends.

Incident response: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Incident response plan (IRP): An incident response plan is a document that outlines an organization's procedures, steps, and responsibilities of its incident response program.

Internet of Things(IoT): Describes smart devices that are connected to the internet but are not personal computers or smartphones.

IP address: In the information technology context, Internet Protocol address.

Malware: Malicious software. These are pieces of code designed to damage, destroy or subvert computer systems. It includes viruses that can replicate and stop systems working; ransomware, which blocks systems until a ransom is paid; and spyware, which is hidden on the target system and spies on the device users.

Man-in-the-middle attack(MitM): Is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating.

Multi-factor authentication (MFA): Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/ personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Patch: A piece of software whose purpose is to fix a software bug or vulnerability.

Phishing: A fraudulent communication, purporting to be from a reputable source, with the aim to trick the recipient into giving away sensitive data or installing malware.

Port: Virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

Ransomware: A type of malware designed to extort money by encrypting / blocking access to files or the computer system until a ransom is paid.

Sender Policy Framework (SPF): Is used to check sender domain authenticity by checking which IP addresses are legitimate for mail sent from an organization’s domain.

Server: A computer or device on a network that manages network resources.

Social Engineering: Psychological manipulation of a person to make him/her perform an action or give away some information.

Software: Is a set of instructions, data or programs used to operate computers and execute specific tasks. It is the opposite of hardware, which describes the physical aspects of a computer.

Spoofing: Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system.

Spyware: Software designed to spy on the activity of a computer user.

Secure Sockets Layer (SSL): Is an encryption-based Internet security protocol.

The principle of least privilege (PoLP): Is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task.

Threat actors: Also known as cyber threat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems.

Traffic Light Protocol (TLP): The protocol requires that the person sending information assigns it a colour using a colour code. This colour indicates if and in what ways this information may be further disseminated. Someone who receives info, and believes that certain info can be disseminated on a greater scale, must first ask for permission from the sender.

Virtual private network (VPN): Encrypts your connection and anonymizes your IP address. It creates a secure tunnel that can access internal resources.

Virus: Software designed to replicate itself and propagate in a computer infrastructure.

Vulnerability: A vulnerability is an error in a piece of software that may be exploited to compromise a computer system.

Web application firewall (WAF): Helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

Web server: Computer system capable of delivering web content to end users over the internet via a web browser.

Zero trust: Cybersecurity approach that focuses on users, assets and resources instead of static network-based perimeters. It assumes no automatic trust based on physical location or asset ownership, requiring authentication and authorisation before granting access.

References

[1] The CyberPeace Builders program equips NGOs with guidance and cyber threat intelligence so they can detect upcoming cyberattacks, builds NGO cyber capacity to prevent cyberattacks against them or their beneficiaries, and engages with cybersecurity experts and NGOs through a volunteering platform and to foster community engagement. https://cyberpeaceinstitute.org/cyberpeace-builders/

[2] Dominioni, S. Persi Paolo, G. (2023). "Unpacking Cyber Capacity-Building Needs. Part II. Introducing a Threat-Based Approach". United Nations Institute for Disarmament Research (UNIDIR). Available at: https://unidir.org/wp-content/uploads/2023/09/UNDIR_unpacking_cyber_capacity_building_needs_part2.pdf (Accessed: November 2023).

[3] National Cyber Security Centre (NCSC).(2021). "Ransomware". National Cyber Security Centre. 4 December 2021. Available at: https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/ransomware.html (Accessed: October 2023).

[4] National Cyber Security Centre (NCSC). (2021)."Ransomware threat methodology". NCSC Annual Review 2021. National Cyber Security Centre (NCSC). 17 November 2021. Available at: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/ransomware-threat-methodology (Accessed: October 2023).

[5] Canadian Centre for Cyber Security. (2020). "Tips for backing up your information (ITSAP.40.002)". Canadian Centre for Cyber Security. October 2020. Available at: https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002 (Accessed: October 2023).

[6] Grance, T. et al. (2006). "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities". National Institute of Standards and Technology (NIST). September 2006. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf (Accessed: October 2023).

[7] Scarfone, K. and Hoffman, P. (2009). "Guidelines on Firewalls and Firewall Policy". National Institute of Standards and Technology (NIST SP). September 2009. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901083 (Accessed: October 2023).

[8] Microsoft. "What is Data Loss Prevention (DLP)". Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp (Accessed: October 2023).

[9] Scarfone, K., Jansen, W., & Tracy, M. (2008). "Guide to General Server Security". National Institute of Standards and Technology (NIST). July 2008. Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf (Accessed: October 2023).

[10] National Cyber Security Centre (NCSC). (2023). "A data leak - what next?". National Cyber Security Centre (NCSC). 1 September 2023. Available at: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/vorfall-was-nun/datenabfluss.html (Accessed: October 2023).

[11] National Institute of Standards and Technology (NIST). Cybersecurity Framework. https://www.nist.gov/cyberframework (Accessed Oct, 2023)

[12] International Organization for Standardization (ISO). ISO/IEC 27001: Information security management systems. https://www.iso.org/standard/27001 (Accessed Oct, 2023)

[13] Canadian Centre for Cyber Security. (2023). Using Information Technology Asset Management (ITAM) to Enhance Cyber Security. https://www.cyber.gc.ca/en/guidance/using-information-technology-asset-management-itam-enhance-cyber-security-itsm10004 (Accessed Oct, 2023)

[14] Cybersecurity and Infrastructure Security Agency (CISA). "Incident Response Plan Basics". Cybersecurity and Infrastructure Security Agency (CISA). Available at: https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf (Accessed: October 2023).

[15] Cichonski, P., Millar, T., France, T., Scarfone, K. (2012). "Computer Security Incident Handling Guide". National Institute of Standards and Technology (NIST). August 2012. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (Accessed: October 2023).

[16] National Institute of Standards and Technology (NIST). Cybersecurity Framework. https://www.nist.gov/cyberframework (Accessed Oct, 2023)

[17] National Cybersecurity Centre (NCSC). "Cyberthreats". https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen.html (Accessed Oct, 2023)

[18] Cloudflare. "What is a reverse proxy? Proxy servers explained". Cloudflare Available at: https://www.cloudflare.com/en-gb/learning/cdn/glossary/reverse-proxy/ (Accessed: October 2023).

[19] Microsoft. "SIEM Defined". Microsoft. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem (Accessed: October 2023).

[21] Scott, R. Borchet, O. Mitchel, S. Connelly, S.(2020). " Zero Trust Architecture". National Institute of Standards and Technology (NIST). Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (Accessed: October 2023).