



Cyber Threat Reporting Platform

D2.1 Report on NGO Threat Landscape

Document Summary Information

Grant Agreement No	101111844	Acronym	UnderServed
Full Title	UnderServed Cyber Threat Reporting Platform		
Start Date	01/06/2023	Duration	24 months
Project URL	https://UnderServed-project.eu/		
Deliverable	D2.1 Report on NGO Threat Landscape		
Work Package	WP2		
Contractual due date	M8	Actual submission date	14.10.2024
Nature	R	Dissemination Level	PU
Lead Beneficiary	CyberPeace Institute		
Responsible Author(s)	Adrien Ogee (CPI), Murielle Abi Akar (CPI), Miles Collins (CPI) GPT-4 was employed for editorial purposes.		
Contributions from	Cormac Doherty (CCI UCD)		



Co-funded by the
European Union

This project has received funding from the European Union's ISF 2022 fund, under grant agreement No 101111844. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v0.1	18.01.24	75%	Initial Deliverable Structure	Murielle Abi Akar, Miles Collins, Adrien Ogee (CPI)
v0.2	18.03.24	80%	First peer-review	Cormac Doherty (UCD CCI)
v0.3	03.04.24	85%	Second peer-review (including changes from first peer-review)	Cormac Doherty (UCD CCI)
v0.4	04.04.24	90%	Including changes from second peer-review	Murielle Abi Akar, Florent Bitschy, Miles Collins, Stéphane Duguin, Adrien Ogee (CPI)
v0.5	10.04.24	95%	Including placeholder for LEA/CERTs surveys to be conducted before M15 as per T2.2	Murielle Abi Akar, Florent Bitschy, Miles Collins, Stéphane Duguin, Adrien Ogee (CPI)
v0.6	11.09.24	98%	LEA/CERTs survey analysis added	Murielle Abi Akar, Adrien Ogee (CPI)
v0.7	24.09.24	99%	Third peer-review	Cormac Doherty (UCD CCI), Mark Sedman (WaterAid)
v0.8	11.10.24	100%	Including changes from third peer-review	Murielle Abi Akar, Adrien Ogee (CPI)

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority, the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the UnderServed consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the UnderServed Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the UnderServed Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© UnderServed Consortium, 2023-2025. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of contents

Executive summary	8
Introduction	10
1.1 Mapping UnderServed outputs	12
1.2 Why this report?	12
1.3 Deliverable overview and report structure	13
1.4 Research methodology	13
1.5 Limitations.....	15
2. NGO cyber maturity	17
2.1 Average cybersecurity maturity scores.....	17
2.2 Assets and data protection	18
2.3 Backup and disaster recovery	18
2.4 Incident response and disaster recovery plan	19
2.5 Digital perimeter security	19
2.6 Next-Gen endpoint protection.....	20
2.7 Authentication practices	20
2.8 Simulated phishing and training	20
2.9 Password management.....	20
2.10 Threat awareness and monitoring.....	21
2.11 Threat posture of NGOs as reported by LEA/CERTs	21
2.11.1 Reporting from NGOs to CERTs/LEAs.....	21
2.11.2 Frequency of interactions	21
2.11.3 Measuring the impact of CERTs/LEAs interventions.....	22
2.11.4 Receiving data from NGOs about cyberattacks	22
2.11.5 Channels of communication	22
3. NGO vulnerabilities	23
3.1 Network and infrastructure security	23
3.2 Application and data security	24
3.3 Known vulnerabilities and compliance	25
4. NGO cyber incidents	28
4.1 Publicly reported incidents	28

4.2 Incident data gathered on research group	30
4.3 Leaked credentials	35
4.4 Case studies	36
4.4.1 Case 1: Spear-phishing attack against Belgian NGO	37
4.4.2 Case 2: Active directory compromise in a Swiss NGO	39
4.4.3 Case 3: EU-based NGO targeted by ransomware attack	44
4.5 Key cyber incidents prioritised and managed by LEAs/CERTs	46
4.5.1 Types of cyber incidents managed.....	47
4.5.2 Prioritisation of cyber incidents reported by NGOs.....	47
5. Platform requirements for NGO cyber incident reporting to LEAs.....	48
5.1 LEA/CERTs platform requirements	48
5.1.1 Challenges faced when managing incidents for NGOs	48
5.1.2 Types of data received from NGOs	48
5.1.3 Success stories or positive outcomes from collaborations.....	48
5.1.4 Cyber threat reporting platform	49
5.1.5 Use of data provided by NGOs.....	49
5.1.6 Benefits of a dedicated threat reporting platform for NGOs	50
5.1.7 Specific data to be prioritised on a dedicated threat reporting platform	51
5.1.8 Useful features for a cyber threat reporting platform	52
5.1.9 Specific support and resources for NGOs	53
5.2 NGO platform requirements.....	54
5.3 Platform modules proposals.....	56
5.3.1 Organisational information module.....	56
5.3.2 Incident notification module	56
5.3.3 Technical data upload module.....	56
5.3.4 Legal support interface	56
5.3.5 Recovery assistance hub	57
5.3.6 Volunteer support coordination	57
5.3.7 Optional requirements.....	57
Conclusion.....	58
References	59

Appendices.....	63
Appendix I - Survey questions.....	63
Appendix II: NGO-led shareable cyber threat intelligence	66
1 Contextual intelligence	66
2 Incident-specific intelligence	66
Appendix III: Glossary	68

List of tables

Table 1: Adherence to UnderServed GA deliverable & tasks descriptions.....	12
Table 2: CISA KEV listed CVE's present in NGO environments	26
Table 3: Infected device statistics.....	32

List of figures

Figure 1: Average cybersecurity maturity scores of humanitarian NGOs in the EU and in Switzerland	17
Figure 2: Survey responses: Insights on EU NGOs from the GSA.....	18
Figure 3: GCSA results from NGOs on website vulnerability assessment deployment	19
Figure 4: Risky services detected in EU NGOs.....	24
Figure 5: Risky services detected in CH NGOs	24
Figure 6: Number of CVEs detected in EU NGOs grouped by severity.	25
Figure 7: Number of CVEs detected in EU NGOs, grouped by severity	26
Figure 8: Heat map: malicious traffic detection count within 3 victims.....	33
Figure 9: EU Count of infection traffic by category	34
Figure 10: EU infection origin locations	34
Figure 11: Call-home duration counts	35
Figure 12: Spear phishing email received by EU Disinfo Lab in 2022	38
Figure 13: Sample email (sanitised)	40
Figure 14: Message prompting the user to enable the execution of the malicious script	41
Figure 15: The QBot infection process	42
Figure 16: How the exchange server is compromised.....	43
Figure 17: Ransom note received by NGO.....	45
Figure 18: Negotiation communication logs.....	46

Abbreviations used

Abbreviation	Description
CVE	Common Vulnerabilities and Exposures
EU	European Union
DDOS	Distributed Denial-of-Service
DNSSEC	Domain Name System Security Extensions
GCSA	General Cybersecurity Assessment
ICRC	International Committee of the Red Cross
NGAV	Next Generation Endpoint Protection
MFA	Multi-Factor Authentication
MiTM	Man-in-the-middle attack
NGO	Non-Governmental Organisation
HTTP	Hypertext Transfer Protocol

Executive summary

In an era characterised by the rapid digitalisation of society, Non-Governmental Organisations (NGOs) play a pivotal role in addressing a myriad of humanitarian crises, human rights issues and social cohesion initiatives within the European Union (EU) and beyond. However, this increased reliance on digital technologies exposes these organisations to a spectrum of cyber threats, necessitating urgent and targeted responses to safeguard their operations and the sensitive data they handle.

The UnderServed project, funded by the European Commission, emerges as a critical intervention designed to bolster the cybersecurity posture of NGOs. This initiative is predicated on the acknowledgement by the European Commission of the acute vulnerability of NGOs to cyberattacks—a reality starkly illustrated by recent high-profile breaches, including the compromise of the International Committee of the Red Cross's data. According to Microsoft data, the NGO sector is the second most targeted sector by nation states, after IT. This underscores the need for enhanced cybersecurity measures tailored to the needs and constraints of the NGO sector.

The UnderServed platform aims to provide a comprehensive suite of tools and resources to empower NGOs in their cybersecurity endeavours. This includes facilitating incident reporting, assistance, and access to support networks. The platform is conceptualised as a technological solution as well as a strategic enabler for NGOs to more effectively manage information security and maintain their critical humanitarian missions in a secure digital environment.

Through desktop research, surveys, interviews and technical analyses, this report presents the current state of NGO cybersecurity, revealing a diversity of preparedness levels and identifying prevalent vulnerabilities. For example, only 19% of NGOs surveyed in the EU have a formal incident response and disaster recovery plan in place, underscoring a critical gap in preparedness for cyber incidents. Out of 56 NGOs analysed, all exhibited misconfiguration and security weaknesses or vulnerabilities in the software they use, highlighting an urgent need for enhanced digital hygiene practices. For instance, out of the 56 NGOs, 93% lacked proper Domain Name System Security Extensions (DNSSEC), significantly heightening their susceptibility to domain spoofing attacks.

NGOs are at the mercy of cybercriminals and state actors; between January 2023 and January 2024, 70% of EU NGOs analysed had at least one user account compromised, underscoring the need for robust access management and the adoption of multi-factor authentication (MFA). Indeed, when nefarious actors are able to leverage these credentials to attack NGOs, the consequences can be dire.

Although NGOs do not typically disclose or report cyberattacks, several cases are discussed within this report, including a spear-phishing attack, an advanced persistent threat and a ransomware attack.

The findings in this report highlight the acute need for the UnderServed platform and the broader necessity of adopting a proactive, informed approach to cybersecurity within the NGO sector. This project represents a significant step towards enhancing the cybersecurity resilience of NGOs in the EU. By

providing a tailored incident reporting and information-sharing platform, the project not only addresses the immediate cybersecurity needs of NGOs but also contributes to the development of a more secure, collaborative cyber ecosystem for these vital organisations. The implementation of UnderServed thus stands as a critical initiative in safeguarding the indispensable contributions of NGOs to societal well-being against evolving cyber threats.

Introduction

Non-governmental organisations (NGOs) play a crucial role contributing significantly to various aspects of society. With over thousands of NGOs operating within the European Union (EU), these organisations are instrumental in addressing humanitarian crises, promoting human rights, and fostering social cohesion¹. European NGOs are at the forefront of responding to natural disasters, conflicts, and emergencies, offering lifesaving support such as food aid, medical care, and shelter to affected populations¹. Through their dedication, innovation, and collaborative efforts, humanitarian NGOs in the EU contribute significantly to alleviating suffering, protecting vulnerable populations, and advancing global solidarity.

The digital era has undeniably improved the work of NGOs on many levels; however, it has also brought a number of negative, often unrecognised, externalities. Cyber threats impacting individuals and organisations globally is a risk that poses serious challenges and necessitates urgent responses. The European Commission's Joint Research Centre and the EU Security Union Strategy (2020-2025) have acknowledged the pervasive nature of these cyber threats. Recognising that cybersecurity is no longer a niche issue but one affecting all sectors - from government entities to businesses and even NGOs. In response, the European Commission has initiated critical measures to bolster cybersecurity². These include substantial investments to strengthen cyber infrastructure and enhance cyber resilience. For instance, the European Network and Information Security (ENISA), the Cybersecurity Act, the Cyber Resilience Act and many more².

As efforts to build stronger cyber capacities and infrastructures progress, it's become apparent that the non-profit sector is often overlooked by governments, civil society organisations or private sector³. A study conducted by the United Nations University revealed that only 30% of NGOs worldwide received government support to comply with cybersecurity regulations and legal requirements³.

Microsoft's data reveals that cybercriminals frequently target NGOs and think tanks, ranking them as the second most targeted sector. These entities account for 31% of all notifications concerning nation-state attacks on organisational domains⁴. In 2022, the International Committee of the Red Cross (ICRC), a renowned NGO, faced cyberattacks resulting in the compromise of personal data belonging to over

¹ European Civil Protection and Humanitarian Aid Operations. "Humanitarian Partners". February 1st, 2024. [Online]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/partnerships/humanitarian-partners_en

² Shaping Europe's Digital Future. "Cybersecurity Policies," March 20th, 2024. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

³ United Nations University, Institute of Macau., "Civil society organizations' cyber resilience". 2021. [Online]. Available: https://collections.unu.edu/eserv/UNU:8262/Civil_Society_Organizations_Cyber_Resilience.pdf

⁴ Spelhaug, Justin. "Strengthening Cyber Defenses for Nonprofits." Microsoft on the Issues, December 13th, 2021. <https://blogs.microsoft.com/on-the-issues/2021/10/21/cyber-defenses-security-program-nonprofits/>

515,000 individuals worldwide in a sophisticated cyberattack⁵. Similarly, Philabundance, a charitable organisation, also experienced a cyber attack, resulting in a loss of \$1 million⁶.

Despite their crucial role, NGOs remain highly susceptible to cyber risks. Due to budget constraints that prevent them from allocating sufficient resources to manage their IT and cybersecurity, these organisations are particularly vulnerable. Their relationships with a wide range of wealthy donors and their increasing digital footprint create prime opportunities for cybercriminals to exploit cybersecurity loopholes. Consequently, NGOs face significant risks, including threats to their financial resources, operational effectiveness, and even their political stances. This vulnerability highlights the need for more inclusive cybersecurity strategies that protect all sectors, including them.

The UnderServed project, funded by the EU, has emerged to support this endeavour. The project aims to address these problems by creating an information-sharing and incident-reporting platform that is specifically designed to meet the requirements of a vulnerable sector. For the purpose of the project, this platform's primary focus will be the humanitarian sector, yet it will be built so that it can be expanded to other sectors in the future.

This report is the first deliverable in the WP2 'NGO threat landscape' of the UnderServed project. It provides a detailed description and analysis of the threat landscape of 30 humanitarian NGOs based in the EU.

⁵ International Committee of the Red Cross (ICRC), "Cyber attack on the ICRC: What we know". June 22nd, 2022. [Online]. Available: <https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know>

⁶ Pat Ralph, "Philabundance Falls Victim to Cyberattack, Loses Almost \$1 Million," PhillyVoice, December 1st, 2020, <https://www.phillyvoice.com/philabundance-cyberattack-theft-1-million-dollars/>

1.1 Mapping UnderServed outputs

The purpose of this section is to map UnderServed Grant Agreement commitments, both within the formal deliverable and task description, against the project's respective outputs and work performed.

Table 1: Adherence to UnderServed GA deliverable & tasks descriptions

UnderServed GA Component Title	UnderServed GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D2.1 Report on NGO Threat Landscape	Final fact-based pdf report in English and executive summary translated in 24 EU languages.	All	This report presents the threat landscape of NGOs based in the EU and Switzerland. Translation at a later stage.
TASKS			
T2.2. Research	The research will focus on collecting raw incidents data and conducting survey and interviews with NGOs, CERTs and LEAs	2 & 3	We conducted surveys and Interviews with NGOs and CERTs/LEAs.
T2.3. Interim analysis	Conduct an initial analysis of the data to establish how the data needs to be presented in the platform. Develop case studies.	4, 5 & 6	In the following sections, we provide several case studies along with an analysis of the data gathered and the requirements suggested for the platform.

1.2 Why this report?

The objective of this report is to increase understanding of the cyber threat landscape affecting NGOs in the EU, in order to inform the development of the UnderServed platform. The report illustrates the cybersecurity issues that affect EU NGOs, looking at their level of cybersecurity maturity, the weaknesses vulnerabilities in their digital infrastructure, and the cyber incidents that have impacted them. Additionally, we conducted surveys with LEAs and CERTs about their interactions with NGOs, as well as their requirements for the platform. This report will also provide a comparative analysis with Swiss-based NGOs, offering a comparative perspective from a country with a history of hosting humanitarian NGOs and advocating for their protection⁷.

⁷ Ville De Genève - Site Officiel. "International Institutions, Permanent Missions and Non-governmental Organisations," February 5th, 2024. [Online]. Available: <https://www.geneve.ch/en/themes/international-geneva/international-institutions-permanent-missions-non-governmental-organisations>.

1.3 Deliverable overview and report structure

This report is the first deliverable in the WP2 ‘NGO threat landscape’ of the UnderServed project. It provides a detailed description and analysis of the threat landscape facing NGOs based in the EU spread across three main sections. The first section looks at the level of maturity of NGOs across all cybersecurity domains and builds upon questionnaires and interviews held with 30 NGOs in the EU, and 30 in Switzerland. The second section builds upon vulnerability scans to evaluate the vulnerabilities in the digital footprint of all these NGOs. The third section examines the incidents that NGOs have faced, drawing data from open and closed-source intelligence, from passive scans and dark web monitoring as well as surveys conducted for LEA and CERTs. Building on this review of the cyber threat landscape affecting EU NGOs, a fourth section provides insights, particularly from the surveys, into the modules that could be required from the UnderServed platform.

1.4 Research methodology

This report is founded on data sourced and analysed by the CyberPeace Institute from two channels:

- Primary data through direct engagement with NGOs, LEAs and CERTs through surveys and interviews drawn from the CyberPeace Institute’s flagship services including the CyberPeace Builders program and Cyber Incident Tracers^{8,9}. The data has been aggregated and anonymised to respect the privacy and security of the participating NGOs.
- Secondary sources from open sources, collected through open source intelligence techniques, passive scanning of digital assets to identify any risks or vulnerabilities. It is as well gathered from a trusted network of partner cybersecurity companies - providing additional insights stemming from secondary datasets such as telemetry data, data breaches, leaks and cybersecurity ratings.

In order to identify NGOs readiness and cyber resilience levels, the methodology employs a mixed-methods approach. A mixed-methods approach is a procedure for collecting, analysing, 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.

For this report, a total of 30 EU NGOs filled a security maturity questionnaire comprising different questions across 9 categories of information security. Another 30 NGOs in Switzerland filled it as well and the results were analysed to offer a comparative perspective.

The CyberPeace Institute has developed the General Cyber Security Assessment (GCSA) to streamline and simplify NGOs’ cybersecurity assessment¹⁰. The GCSA is a comprehensive, self-assessment tool designed

⁸ CyberPeace Institute. “CyberPeace Builders.” CyberPeace Builders, n.d. <https://cpb.ngo/>

⁹ CyberPeace Institute. “Cyber Incident Tracers | CyberPeace Institute,” October 10, 2023. <https://cyberpeaceinstitute.org/cyber-incident-tracers>

¹⁰ CyberPeace Institute, “Measure to Improve: The GCSA’s Role in Nonprofit Cyber Resilience”. January 30th, 2024. [Online]. Available: <https://cyberpeaceinstitute.org/news/measure-to-improve-the-gcsas-role-in-nonprofit-cyber-resilience/>

to help NGOs evaluate their own cybersecurity maturity level, which builds on industry standards such as NIST's Cybersecurity Framework ¹¹. The self-assessment is written in English and takes less than 20 minutes to complete. As NGOs often lack a single point of contact for cybersecurity, the tool was designed in such a way that different staff members from the organisation could provide input. After completion, the organisation receives a two-page report of their current cybersecurity posture with suggested next steps.

The survey consists of 30 questions, covering 9 categories of information security activity:

- *Asset and Data Protection*: This category focuses on identifying critical assets and data, regulating access to systems and networks, and implementing targeted safeguards for sensitive information.
- *Backup and disaster recovery*: This category outlines the importance of regular data backups and verification, emphasising the 3-2-1 backup method.
- *Incident response and disaster recovery plan*: Distinctively from the previous category, this category examines the resilience of the organisation to bounce back as quickly as possible after a disaster.
- *Digital Perimeter Security*: Covers safeguarding an organisation's public-facing virtual accounts and digital platforms, like websites, emails, and social media, from cyberattacks, including data leak prevention strategies.
- *Next Generation Endpoint Protection*: Focuses on advanced security tools that proactively learn and counter malware in real-time, questioning the deployment of such antivirus solutions on organisational devices.
- *Authentication Practices*: Addresses implementing an additional security layer, often through a combination of something users have, know, and are, such as Two-Factor or Multi-Factor Authentication, including biometrics, across key organisational platforms.
- *Simulated Phishing and Training*: This category assesses the maturity of cybersecurity awareness within the organisation, focusing on regular user training, conducting phishing simulations, and implementing warning banners for external emails.
- *Password Management*: related to the use of software application or a hardware device that is used to store and manage an employee's passwords.
- *Threat Awareness & Monitoring*: Focuses on the monitoring of darknet activities to detect suspicious actions or identity theft, such as leaked user credentials, to enhance organisational security.

The targeted organisations are registered NGOs, apolitical, independent, which seek to improve lives and reduce suffering, with a focus on Humanitarian-Development and Peace endeavours. All of them operate from the EU or Switzerland and conduct their activities either at national, European or global level.

¹¹ NIST. "Cybersecurity Framework | NIST," March 8, 2024. <https://www.nist.gov/cyberframework>

Approximately 65% of the NGOs analysed were classified as small organisations. Small organisations are defined as those with 50 employees or fewer, while large organisations encompass those with 51 employees and above.

The internal team from the CyberPeace Institute interviewed 60 NGOs. These interviews gathered qualitative insights with regard to the human-centred understanding of their cybersecurity practice. The interviews were conducted in both French and English.

The sample size of 30 EU 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 might not capture the full range of cybersecurity preparedness and threat awareness across the entire EU humanitarian NGO community.

In addition to surveying NGOs, the CyberPeace Institute also conducted research on the collaboration between NGOs, Law Enforcement Agencies (LEAs), and Computer Emergency Response Teams (CERTs). This research was conducted to address the increasing frequency and sophistication of cyberattacks on nonprofit organisations. In this context, a survey was conducted to gather insights into how CERTs/LEAs interact with NGOs regarding cyberattacks, the challenges they face, and the potential solutions that could strengthen these partnerships.

This survey targeted professionals working in CERTs and LEAs, and 8 participants completed it. These respondents came from diverse roles, including Information Security Consultants, Detective Inspectors, and Senior Consultants in Digital Forensics and Incident Response (DFIR). The objective was to assess the current state of engagement between CERTs/LEAs and NGOs, with a focus on incident response, cyber threat management, and areas where collaboration could be improved.

The insights gained from this survey provide valuable perspectives on the operational realities of dealing with cyber threats, highlighting the need for improved communication, resource-sharing, and technical support platforms between CERTs, LEAs, and NGOs.

1.5 Limitations

While the findings of this study offer valuable insights of the threat landscape of EU based humanitarian NGOs, it is important to acknowledge some limitations that may have influenced the outcomes.

Beginning with the sample size, we have assessed 30 NGOs only in the humanitarian ecosystem. This number of NGOs may introduce some biases. Other NGOs may have other experiences and knowledge when it comes to cybersecurity controls, vulnerabilities and threats.

NGOs are generally reluctant to share detailed information about cybersecurity incidents: they have virtually no regulatory obligations to do so, no incentives to do so and generally lack the maturity to understand the risks and benefits associated with shaping the narrative around a cyber incident. Those are the very reasons why the UnderServed project came to be.

Additionally, although the digital footprint of NGOs has been growing in the last decade¹², their limited IT resources constrain their ability to set up and maintain their own digital infrastructure such as autonomous systems, making it challenging to comprehensively assess their cybersecurity posture without more direct or active engagement methods, which were outside the scope of this research.

Last, the small sample size of CERTs and LEAs surveyed may not fully capture the diversity of experiences and operational contexts across different regions and organisations.

¹² Al Achkar, “Achieving Safe Operations Through Acceptance: Challenges and Opportunities for Security Risk Management”. [Online]. Available: https://gisf.ngo/wp-content/uploads/2021/12/Digital_Risk_how_new_technologies_impact_acceptance_and_raise_new_challenges_for_NGOs.pdf

2. NGO cyber maturity

Within the EU, humanitarian NGOs encounter a spectrum of challenges that affects their operations. The analysis below is not exhaustive in its coverage given that 30 NGOs were assessed. It is also important to mention that detailed information about participating NGOs is omitted to safeguard their privacy and security.

In order to better assess the level of cybersecurity maturity of EU NGOs, interviews were conducted and the GCSA was filled, either directly by the NGO or by the interviewer.

The following subsections present the survey results for each question in order.

2.1 Average cybersecurity maturity scores

After assessing NGOs, and as per the assessment, results were divided into 9 categories. In the Figure below the scores of each category are represented.

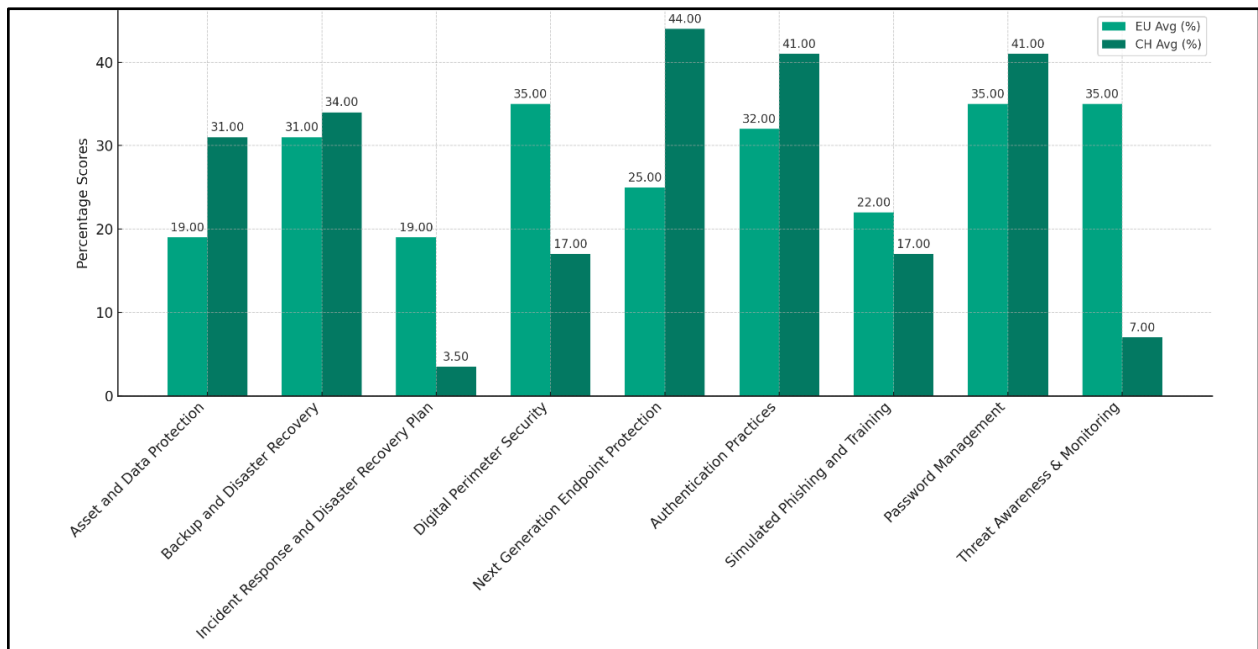


Figure 1: Average cybersecurity maturity scores of humanitarian NGOs in the EU and in Switzerland

The cybersecurity maturity of EU NGOs illustrates a mixed landscape. A considerable number of NGOs have been working on their backup procedures, password management, authentication practices, and the implementation of digital perimeter security. They are also actively monitoring threats and cyber risks to enhance overall cybersecurity measures. However, a majority of them lack essential cybersecurity measures such as cloud security, incident response, and other categories, required to uphold their operations. For instance, even though 19% of the NGOs have incident response and disaster recovery plans compared to only 3.5% for Swiss NGOs, more attention should be given to this category. Almost half

of the Swiss NGOs surveyed have been actively implementing Next Generation Endpoint Protection and authentication measures, in contrast to a lower adoption rate observed among EU NGOs. Let's dive deeper into each category.

2.2 Assets and data protection

In terms of assets and data protection, the situation among EU NGOs is concerning. Only 29% have both their physical and digital assets up-to-date and configured correctly. This low percentage is troubling given the importance of maintaining both hardware devices and software licences for security.

A mere 16% possess an up-to-date inventory of these assets. This step is critical for identifying and managing potential security risks, yet it is widely neglected. Just 32% practice effective patch management, which is essential to prevent the exploitation of vulnerabilities.

Moreover, there is a significant gap in cyber insurance coverage, with 84% of EU NGOs lacking this protection, compared to 31% of Swiss NGOs whose general insurance also includes cyber coverage in case of a cyber incident. Cyber insurance is key to reducing financial losses after a cyberattack, but it often requires documented policies, which are absent in many NGOs.

And indeed, only 27% have a formal data protection policy.

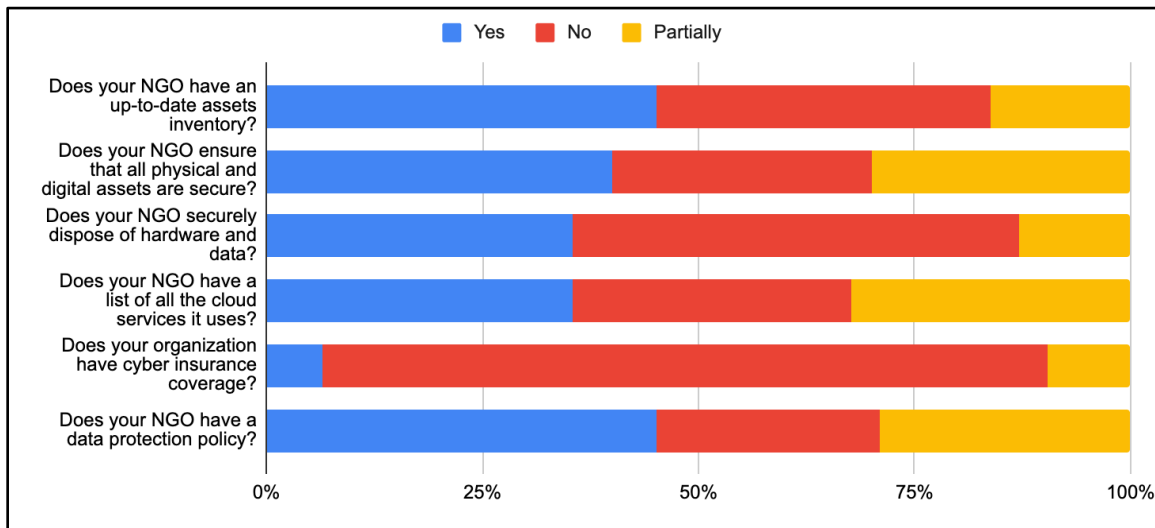


Figure 2: Survey responses: Insights on EU NGOs from the GSA

2.3 Backup and disaster recovery

This category outlines the importance of regular data backups and verification, emphasising the 3-2-1 backup method: 3 copies of one's data stored on 2 different media types with 1 copy off-site. Both EU and

Swiss NGOs share similar maturity scores when looking at their backup and disaster recovery strategies: only 29% of them reported backing up their data and storing them somewhere safe, so they can immediately recover from an incident.

With that said, 79% of EU NGOs reported that they have identified their critical functions related to the delivery of essential services to vulnerable populations. This is a good start. Unfortunately, more than half of them reported not backing up the data associated with these critical services.

2.4 Incident response and disaster recovery plan

When it comes to incident response and disaster recovery planning, only 3.2% of NGOs based in Switzerland and 19% of those based in the EU have that already in place. This alarming statistic highlights a critical gap: the limited implementation of incident response and disaster recovery plans in NGOs. This situation underscores the urgent need for an accessible incident reporting platform.

2.5 Digital perimeter security

Digital perimeter security is crucial for protecting an organisation's public-facing virtual assets, such as websites, emails, and social media platforms, from cyberattacks. This encompasses strategies for preventing data leaks. While 35% of EU NGOs have reported securing their networks, which is twice the rate observed among Swiss NGOs, there remains a significant area of concern. In the EU, a substantial 68% of NGOs do not perform website vulnerability assessment scans. In contrast, in Switzerland, only 17% of NGOs neglect to conduct website vulnerability scans. This stark difference highlights a critical gap in the digital security practices of EU NGOs, underlining the need for more rigorous and consistent cybersecurity measures.

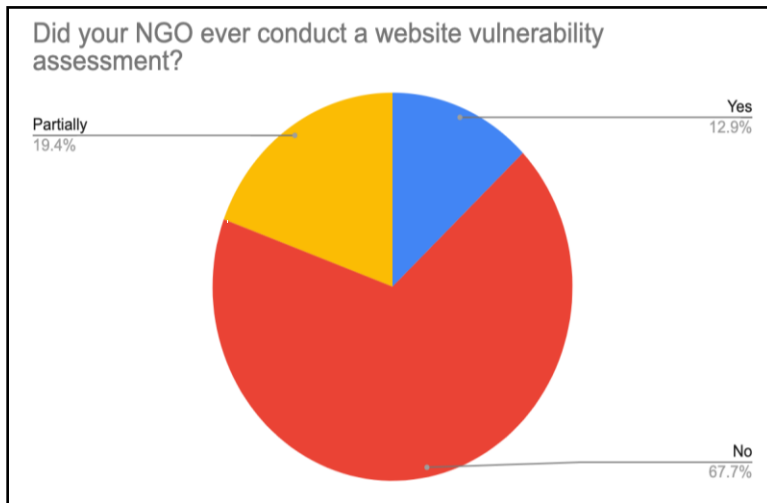


Figure 3: GCSA results from NGOs on website vulnerability assessment deployment

2.6 Next-Gen endpoint protection

Anti-virus solutions, including Next Generation Endpoint Protection, are vital in detecting, containing, and eradicating potentially harmful applications on computers. Such protection is particularly important as it tracks behavioural indicators associated with active malware infections, providing enhanced security in organisational settings. However, it's concerning that only 35% of EU NGOs' endpoints are safeguarded against malware and other cyber threats with up-to-date security software. This low percentage indicates a significant gap in basic cyber defence measures, leaving a majority of these organisations dangerously exposed to increasingly sophisticated cyberattacks.

2.7 Authentication practices

Identity and Access Management is a core part of a cybersecurity programme. Yet the adoption of practices such as Multi-Factor Authentication among EU NGOs is not as widespread as it should be. Only 54% of these organisations use MFA for accessing sensitive data or systems. Furthermore, just 45% follow a process to allocate access privileges based on user roles and responsibilities, which is essential for maintaining secure and efficient access control. Additionally, only 42% ensure adequate management of user accounts, particularly for individuals joining or leaving the organisation. This shortfall in robust authentication practices highlights a significant area of vulnerability.

2.8 Simulated phishing and training

This category evaluates the level of cybersecurity awareness within an organisation, emphasising the importance of regular user training, phishing simulations, and the implementation of warning banners for external emails. Alarming, 65.5% of NGOs in both regions lack initiatives for simulated phishing and awareness training. This is particularly concerning given that phishing incidents are a leading cause of cyberattacks, yet NGOs appear to underestimate the importance of enhancing awareness and strengthening training to prevent such incidents.

Further, 58% of EU NGOs do not offer cybersecurity training to their employees and volunteers, and a significant 71% do not conduct phishing simulations for all staff. This lack of comprehensive training and preparedness exposes these organisations to heightened risks and demonstrates a critical need for improved cybersecurity education and practice.

2.9 Password management

Regarding the adoption of password management solutions, either through software applications or hardware devices for secure storage and management of employee passwords, there is a notable deficiency. Approximately 36% of NGOs in both the EU and Switzerland do not actively manage their passwords.

In terms of specific practices, only 35% of EU NGOs use a password manager to securely store and handle passwords. Furthermore, a mere 19% of these organisations actively educate their employees on the importance of creating unique and complex passwords.

2.10 Threat awareness and monitoring

This area of focus evaluates the monitoring of dark web and logs activities to detect security breaches, anomalies, or unauthorised activities. More precisely, dark web monitoring is the process of actively tracking and analysing online activities and content within the encrypted and hidden layers of the internet to identify potential security threats, illicit activities, or stolen information. Logs monitoring involves the continuous examination and analysis of system-generated logs, capturing events and activities, to identify and respond to security incidents, anomalies, or potential threats within a network or IT environment. As such, the available data indicates that 35% of EU-based NGOs conduct threat awareness and monitoring activities, in comparison to a lower percentage of Swiss NGOs. However, further breaking down this global figure shows that 81% of EU NGOs still do not monitor the dark web, while 61% of them do not have the capacity to monitor their log activities.

2.11 Threat posture of NGOs as reported by LEA/CERTs

Due to their specialised expertise, LEA and CERT assessments and commentary on policies are vital. Their evaluations provide critical insights into the effectiveness of security practices, and recommend adjustments to mitigate risks. These assessments ensure comprehensive security reviews, legal compliance, and readiness to respond to security incidents. In this context, and building on the surveys conducted, we examined the nature of interactions between these entities and NGOs, with a particular focus on cyberattack reporting and response.

2.11.1 Reporting from NGOs to CERTs/LEAs

When asked whether their organisations have interactions with NGOs regarding cyberattacks, respondents were evenly split, with only half reporting having such interactions. This suggests that while some CERTs and LEAs are actively involved in supporting NGOs, others may not have established formal channels of collaboration, or NGOs may choose not to report incidents to CERTs/LEAs.

2.11.2 Frequency of interactions

For CERTs/LEAs that do engage with NGOs, the frequency of interactions varied:

- Weekly interactions: 25%
- Monthly interactions: 25%
- Infrequent interactions (e.g., one or two times a year): 50%

This spread indicates that while some CERTs/LEAs maintain regular contact with NGOs, others engage on a more sporadic basis. This variability may be influenced by the resources available within the agency or the volume of reported incidents.

2.11.3 Measuring the impact of CERTs/LEAs interventions

When asked how they measure the impact of their interventions in cyber incidents reported by NGOs, respondents cited various methods:

- Reduction in Incident Frequency: Some agencies track the reduction in the frequency of reported incidents following their intervention as a key metric.
- Speed of Recovery: Others measure the impact by how quickly NGOs are able to recover and resume normal operations after an incident.
- Feedback from NGOs: Several respondents noted that they rely on feedback from the NGOs themselves to gauge the success of their interventions.

2.11.4 Receiving data from NGOs about cyberattacks

Respondents were asked whether they receive data from NGOs regarding cyberattacks:

- A majority of respondents indicated that they do receive some data, although the quality and consistency of this data vary widely.
- Lack of Data: Some respondents noted that they do not consistently receive relevant data from NGOs, which makes it challenging to provide timely and effective support.

2.11.5 Channels of communication

CERTs/LEAs that reported having interactions with NGOs were also asked about the channels through which these communications occur. The responses indicate a preference for digital communication tools, with the following distribution:

- Email: 50%
- Multiple Channels (e.g., email, phone, meetings): 25%
- All Available Channels: 25%

While email is the predominant means of communication, some respondents noted using multiple methods to stay connected with NGOs, highlighting the need for flexible communication strategies depending on the urgency and nature of incidents.

The authors of this report acknowledge that the above data points are not exhaustive. Nonetheless, they provide a pertinent summary of the limited cyber capabilities of EU NGOs in the humanitarian sector, and highlight the need for systematic and standardised collection, analysis and sharing of information to provide better responses and facilitate international collaboration.

3. NGO vulnerabilities

In order to keep up with the rapid advancements in digital technology, NGOs established a robust online presence. Although this has undoubtedly made their work easier and enabled them to spread their word globally, it has increased their attack surface and made them more susceptible to cyberattacks. This is evidenced by the number of vulnerabilities that were uncovered when researching all NGOs in the research group. Of the 60, 56 were analysed (3 NGOs in the EU have too small a digital footprint to get picked up in our passive scans, and 1 in Switzerland). Among the 56 NGOs analysed, misconfiguration and security weaknesses and vulnerabilities¹³ on software they use have been found for all of them.

We looked at the following types of weaknesses and vulnerabilities:

- Network and infrastructure security
- Application and Data Security
- Known Vulnerabilities and Compliance

3.1 Network and infrastructure security

Network and infrastructure security configuration weaknesses among NGOs in the EU and Switzerland are multifaceted, ranging from encryption issues to inadequate security protocols. For instance, the implementation of Domain Name System Security Extensions (DNSSEC) was found to be severely lacking, with 93% of both EU and Swiss NGOs not having adequate DNSSEC due to misconfigured or missing records. This leaves them potentially vulnerable to domain spoofing attacks.

In the past year, 8 NGOs in the EU had expired SSL certificates, and 6 had self-signed certificates, leading to vulnerabilities in data transmission and exposing sensitive information to potential interception and attacks. Additionally, the use of outdated protocols like TLS v1.0, found in 14 NGOs in the EU and 14 in Switzerland, increases susceptibility to MiTM attacks (e.g. poodle, beast, etc.)

When it comes to open ports, while these may be necessary for running business applications and services, it is essential to ensure that insecure or sensitive services are not directly exposed, or if they have to, that they are adequately monitored and behind security appliances such as firewalls and WAFs. Unfortunately, 24% of EU NGOs and almost half of the Swiss NGOs had potentially risky services exposed on open ports, as highlighted in figures 4 and 5.

¹³ “Common Vulnerabilities and Exposures,” CVE, <https://cve.mitre.org/>

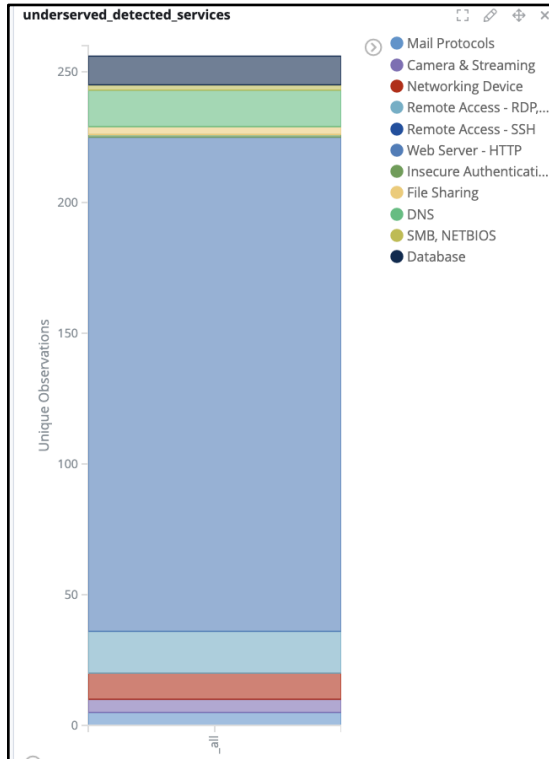


Figure 4: Risky services detected in EU NGOs

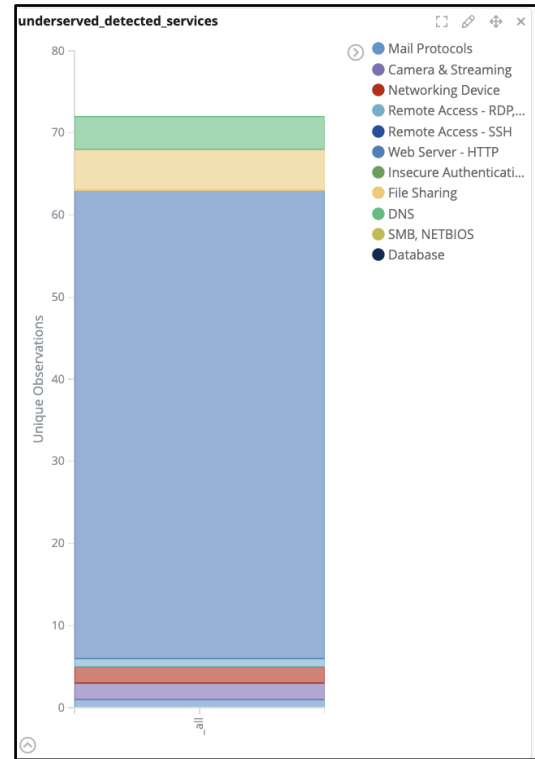


Figure 5: Risky services detected in CH NGOs

Our findings revealed that while the majority of open network ports were standard and commonly used for secure internet services, there was a notable prevalence of insecure HTTP web server ports in both groups. This could potentially pose risks, especially when these insecure ports are used in conjunction with authentication portals, making organisations susceptible to Man-in-the-middle (MitM) attacks.

It is noteworthy to mention the exposure of ports used for networking devices and cameras, as well as commonly exploited ports used in ransomware campaigns¹⁴:

- Remote Desktop Protocol (RDP)
- File Transfer Protocol (FTP)
- Server Message Block (SMB)
- Virtual Network Computing (VNC)

3.2 Application and data security

NGOs often rely on web applications for essential functions like information sharing. However, misconfigured HTTP headers and insecure application settings can leave these organisations open to web-based attacks. This issue is widespread, with 27 out of 29 EU NGOs and 25 out of 27 Swiss NGOs having either missing or misconfigured HTTP security headers. Moreover, web application weaknesses were

¹⁴ Misconfigurations and Weaknesses Known to be Used in Ransomware Campaigns | CISA," Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/stopransomware/misconfigurations-and-weaknesses-known-be-used-ransomware-campaigns>

identified in 25 EU NGOs and all Swiss NGOs, with Cross-Site Request Forgery being the most common vulnerability detected. These findings highlight a critical need for better web security practices.

Email security is another critical area of concern. A considerable 83% of EU NGOs and 70% of Swiss NGOs do not implement essential email security measures such as SPF or DKIM, making them more susceptible to email domain spoofing. This is compounded by the issue of misconfigured certificates, with hostname mismatches affecting about a third of NGOs in the EU and almost half of those in Switzerland. These mismatches, where the SSL certificate's domain name does not align with the website's domain, result in security warnings in web browsers, undermining website credibility and signalling potential vulnerabilities.

3.3 Known vulnerabilities and compliance

Common Vulnerabilities and Exposures (CVE's)

Based on the data gathered on NGOs' internet exposed assets, various organisations have been, and are currently, using insecure devices and services to perform their work. The use of unsupported software, and unpatched systems exposes NGO's to increased risk of exploitation from threat actors who leverage Common Vulnerabilities and Exposures (CVE's) to attack systems¹⁵. Between January 2023 and January 2024, a total of 637 Common Vulnerabilities and Exposures (CVEs) were detected in the region demonstrating the cybersecurity challenges NGOs are facing, with the majority concerning EU NGOs. CVEs were identified on internet connected devices for exactly a fifth of the NGOs looked at in the EU and about a third in Switzerland. More worryingly, 15% of EU NGOs have potentially had High and Critical severity CVEs (based on a CVSS base score of 7 or higher) on their infrastructure¹⁶. Looking at the last 2 months only, our data shows that 14% EU and 30% of Swiss NGOs are currently potentially affected by CVEs.

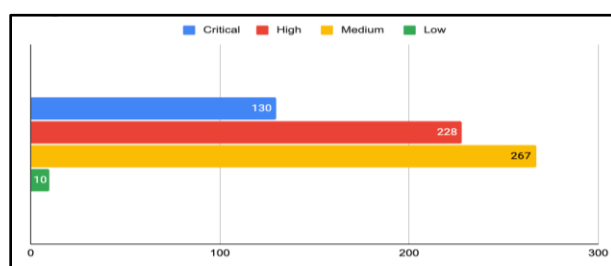


Figure 6: Number of CVEs detected in EU NGOs grouped by severity.

¹⁵ The Common Vulnerabilities and Exposures (CVE) Website. [Online]. Available: <https://www.cve.org/>

¹⁶ S. C. Leadership, "What is CVSS - Common Vulnerability Scoring System," Oct. 24, 2023. <https://www.sans.org/blog/what-is-cvss/>

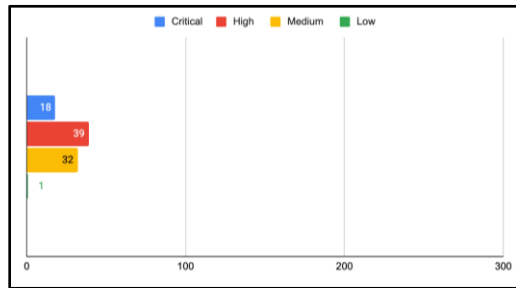


Figure 7: Number of CVEs detected in EU NGOs, grouped by severity

Even more worrying, we found that 2 NGOs in the EU (and 3 in Switzerland) have CVEs that are on CISA's Known Exploited Vulnerabilities list¹⁷. These are vulnerabilities that have recorded cases of exploitation, significantly increasing their risk to organisations.

Table 2: CISA KEV listed CVE's present in NGO environments

	EU	CH
CVE ID	CVE-2021-40438 (2 NGO's)	CVE-2021-40438 (2 NGO's)
	CVE-2019-0211 (1 NGO)	CVE-2019-0211 (1 NGO)
	CVE-2019-11043 (1 NGO)	CVE-2020-28949 (1 NGO)
	CVE-2012-1823 (1 NGO)	CVE-2020-13671 (1 NGO)

Of the CISA KEV listed CVEs, CVE-2021-40438, which is a critical-severity Apache server vulnerability, is most recurrent¹⁸. It affects 4 organisations - 2 in each group. This is followed by CVE-2019-0211, a high-severity Apache server vulnerability¹⁹.

One vulnerability on this list, CVE-2019-11043, has also been reported for known use in ransomware campaigns²⁰. This is a critical severity vulnerability affecting outdated PHP versions that may be exploited for remote code execution on target systems.

¹⁷ Cybersecurity and Infrastructure Security Agency CISA, "Known Exploited Vulnerabilities Catalog".

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1>

¹⁸ NVD - cve-2021-40438." <https://nvd.nist.gov/vuln/detail/cve-2021-40438>

¹⁹ NVD - CVE-2019-0211." <https://nvd.nist.gov/vuln/detail/CVE-2019-0211>

²⁰ CVE-2019-11043 Detail," NIST National Vulnerability Database. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2019-11043>

The identified vulnerabilities and security challenges facing NGOs underscore the critical need for enhanced cybersecurity measures. As NGOs increasingly rely on technology to further their missions and extend their global impact, it is imperative to prioritise robust network and application security protocols, maintain vigilance against known vulnerabilities, and adhere to cybersecurity best practices. Addressing these vulnerabilities is crucial not only for safeguarding sensitive data and ensuring operational continuity but also for preserving trust with stakeholders and donors. The risks posed by these vulnerabilities highlight the potential for cybersecurity incidents that can disrupt operations and compromise the integrity of NGOs' work. Therefore, proactive risk management, continuous monitoring, and swift remediation efforts are essential components of a comprehensive cybersecurity strategy to protect NGOs against evolving threats and mitigate potential impacts on their vital missions.

4. NGO cyber incidents

This section examines the cyber incidents affecting NGOs, including publicly reported cases, data gathered from research groups, as well as the leaked credentials registered. It highlights the challenges faced by NGOs and their responses to cyber threats, aiming to provide a comprehensive overview of the cybersecurity landscape within this sector. In order to provide a detailed and well-researched assessment of cybersecurity in NGOs, several case studies were included at the end.

4.1 Publicly reported incidents

The incidents below are based on open-source research and the victims are not necessarily part of the research group referred to elsewhere in this report.

Attack against SOS Children's Villages International, Austria, 2021

SOS Children's Villages International, an Austria-based global organisation, was the victim of a cybersecurity incident on September 18, 2021. The organisation took immediate action by implementing appropriate countermeasures, including notifying relevant authorities and seeking assistance from external cybersecurity experts. These measures enabled them to secure their servers swiftly and resume normal operations of all major systems by September 30, 2021. A thorough investigation followed, which fortunately indicated no evidence of personal data extraction, leakage, or unauthorised disclosure. The incident highlighted the significance of stringent cybersecurity practices, especially for organisations handling sensitive data of beneficiaries, donors, staff, and service providers. SOS Children's Villages International's prompt and effective response to the cybersecurity threat underlines their commitment to maintaining high standards of data security and privacy²¹.

Ransomware attack against Caritas, Germany, 2022

Caritas Germany became a victim of a ransomware attack on September 25, 2022, leading to significant disruptions in their IT systems. Despite the challenges, Caritas opted not to pay the ransom demanded by the attackers. Instead, they focused on establishing an alternative IT infrastructure, leveraging their existing data backups. The organisation emphasised the continuation of their services despite the setbacks, showcasing resilience and commitment to their cause²².

Cyberattack against ADAPT, Ireland, March 2022

ADAPT, a domestic abuse service based in Limerick, Ireland, was struck by a cyberattack on March 23, 2022. This attack caused significant disruptions to their IT systems and service operations. The organisation took immediate action by notifying law enforcement and data protection authorities and

²¹ SOS Children's Villages International, "Statement on Cyber Security Incident," October 6th, 2024. [Online]. Available: <https://www.sos-childrevillages.org/news/statement-on-cyber-security-incident>

²² B2B Cyber Security, "Ransomware Victim Caritas Refuses to Pay". September 25th, 2022. [Online]. Available: <https://b2b-cyber-security.de/en/ransomware-opfer-caritas-will-nicht-zahlen/>

sought external IT expertise to address the breach. Despite the challenges, ADAPT remained committed to continuing their essential services to those affected by domestic abuse²³.

Cyberattack against Rehab, Ireland, March 2022

The Rehab Group, an Irish organisation providing health and social care services, fell victim to a cyberattack in March 2022. This incident significantly impacted their IT systems, leading to service disruptions. In response, Rehab Group implemented their crisis management plan, which involved notifying relevant authorities and engaging cybersecurity experts. Despite these challenges, the organisation worked diligently to minimise the attack's impact on their services and clients²⁴.

Doctors Without Borders, February 2022

In February 2022, Médecins Sans Frontières (MSF), also known as Doctors Without Borders, was reportedly targeted by hackers. Unauthorised access to MSF's network was being sold, indicating a serious breach of cybersecurity. This incident highlighted the vulnerability of even large and well-established humanitarian organisations to cyberattacks. Such breaches are particularly concerning given the sensitive nature of the data held by organisations like MSF²⁵.

EU Disinfo Lab, Belgium, 2020

The EU Disinfo Lab, a non-profit organisation focused on analysing disinformation campaigns against the EU, suffered a Distributed Denial of Service (DDoS) attack on July 20, 2020. This cyberattack knocked their website offline for several hours. The NGO described the incident as a "brute force cyberattack," but staff members suggested it was DDoS-based. The attack highlights the increasing threats faced by organisations involved in digital information security²⁶.

Akadem, France, September 2023

Akadem, the digital platform of the Fonds Social Juif Unifié (FSJU), experienced a ransomware attack during the night of September 25 to 26, 2023. This cyberattack occurred on Yom Kippur, a significant Jewish holiday. The attack caused the Akadem website to become unavailable, marking a severe disruption in their services²⁷.

²³ Limerick Leader, "Limerick Domestic Abuse Charity Targeted in Cyber Attack," March 23rd, 2020. [Online]. Available: <https://www.limerickleader.ie/news/home/773188/limerick-domestic-abuse-charity-targeted-in-cyber-attack.html>

²⁴ The Irish Times, "Rehab Group Falls Victim to Cyber Attack," March 16th, 2022. [Online]. Available: <https://www.irishtimes.com/business/technology/rehab-group-falls-victim-to-cyber-attack-1.4828860>

²⁵ Forbes, "Hackers Sell Access to a \$2 Billion Nonprofit, a Californian Hospital, and Michigan Government" February 23rd, 2022. [Online]. Available: <https://www.forbes.com/sites/thomasbrewster/2022/02/23/hackers-sell-access-to-a-2-billion-nonprofit-a-californian-hospital-and-michigan-government/?sh=33a007dc5758>

²⁶ Tech Monitor, "EU Disinfo Lab in DDoS Attack," July 20th, 2020. [Online]. Available: <https://techmonitor.ai/technology/cybersecurity/eu-disinfo-lab-in-ddos-attack>

²⁷ L'Inform, "Les dessous de la cyberattaque contre Akadem, le site du Fonds Social Juif Unifié," [Online]. October 4th, 2023. Available: https://www.linforme.com/tech-telecom/article/les-dessous-de-la-cyberattaque-contre-akadem-le-site-du-fonds-social-juif-unifie_1051.html

Transparency International, Germany, 2019

In 2019, Transparency International faced a six-week long, sophisticated phishing attack. Detected through a surge in failed login attempts to their Microsoft Office accounts, the attack involved both mass login attempts and targeted spear phishing. Spear phishing emails mimicked senior management's writing style, raising suspicions that the attackers could view internal communications. Microsoft alerts indicated breaches in two staff accounts, despite multi-factor authentication. The IT team, supported by a cybersecurity firm, identified potential state-sponsored origins of the attack, involving domain spoofing and suspected use of sophisticated spyware. The attacks ceased unexpectedly after six weeks, leaving the organisation more aware of cybersecurity threats. Interestingly, at the time of the incident, the organisations debated whether or not to report the incident to law enforcement, and ended up deciding not to²⁸.

In Switzerland, even fewer NGOs have ever publicly discussed cyber incidents.

ICRC, Switzerland, January 2022

The International Committee of the Red Cross (ICRC) experienced a sophisticated cyberattack in January 2022, which compromised servers hosting personal data of over 515,000 people worldwide. The data breach included sensitive information of individuals aided by the ICRC, such as missing persons and their families, detainees, and others affected by conflicts and disasters. The attack was notable for its advanced nature, utilising specific hacking tools and techniques that evaded standard detection. The ICRC took immediate steps to address the breach, enhance security, and assist affected individuals²⁹.

Insecurity Insight, Switzerland, 2022

Insecurity Insight, a Swiss non-profit, experienced a significant cyber harassment incident after reporting on Russian attacks on Ukrainian hospitals. Their employees received numerous phishing messages and inappropriate content on their phones, which was unprecedented in scale for the organisation. Christina Wille, the director, believes this was an attempt to intimidate her team from continuing their documentation of the war's impact in Ukraine. Despite these attempts, the cyberattacks did not succeed in deterring their reporting efforts³⁰.

4.2 Incident data gathered on research group

Now specifically looking into the research group of 60 NGOs, detecting some cyber incidents could be done using measurable data obtainable first via sinkholed c2 traffic. Sinkholing is a cybersecurity technique used to redirect traffic from a network that is under attack or from malicious endpoints to a

²⁸ Solidarity Action Network, "Resisting Sustained Phishing Attacks," [Online]. Available: <https://solidarityaction.network/wp-content/uploads/resisting-sustained-phishing-attacks.pdf>

²⁹ International Committee of the Red Cross (ICRC), "Cyber attack on the ICRC: What we know," [Online]. Available: <https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know>

³⁰ CNN, "Humanitarian aid to Ukraine disrupted by cyberattacks". April 23rd, 2022. [Online]. Available: <https://edition.cnn.com/2022/04/23/politics/humanitarian-aid-ukraine-war-cyberattacks/index.html>

controlled server, the "sinkhole server." The primary purpose of sinkholing is to disrupt the threat posed by malware, botnets, and other malicious activities. Security researchers or network administrators identify malicious domain names or IP addresses that are being used to control compromised systems, such as a botnet's command and control (C&C) servers - they then configure DNS or IP routing to redirect traffic from those identified malicious endpoints to the sinkhole server. The sinkhole server does not respond to the requests in the way the malicious server would, effectively cutting off communication between the infected devices and the control servers. This prevents the infected devices from receiving malicious instructions, whilst allowing researchers to collect data about the compromised systems, such as IP addresses. These can be used to analyse the attack pattern, the extent of the infection, and potentially notify affected parties. This method allows for the identification of 2 NGOs in the EU, and 1 in Switzerland that have likely been infected by comparing the internet facing or external breakout IP addresses and user accounts attributed to these NGOs, to data coming from cyber threat intelligence platforms. Researching the dark web, we were also able to confirm that a significant number of NGOs have had credentials stolen from them. Let's take a closer look.

Malware infected devices

Many forms of malware rely on attacker-controlled domains or servers. These are commonly referred to as command-and-control infrastructure. Once malware is delivered to a device and executes, it is common for the malware to initiate connections to a c2 server or domain for further instructions, or to fetch an additional payload.

In this case we obtained data on suspicious outbound traffic originating from NGO environments to external locations associated with known command and control infrastructures indicating that a device attempted to make c2 communications or 'call home' - this data-gathering method is commonly referred to as sinkholed c2 traffic.

In total, c2 traffic indicating infected devices was recorded 83 times between January 2023-2024. It concerned 2 NGOs in the EU, only 1 in Switzerland. The traffic originated from a total of 13 external IPs located in 9 countries, as evidenced in table 3.

Table 3: Infected device statistics

	# Detected Traffic Events	# Malware Types	# NGOs	# Infected Assets	# Source Countries
EU	81	14	2	12	8
CH	1	1	1	1	1
Total	83	15	3	13	9

15 malware families were identified, as evidenced in figure 8. Each column represents the events seen at the organisation and the chart shows no overlapping malware strains across organisations. MewishID (adware) followed by PseudoManuscript (spyware). Mewishid is a type of riskware/adware that could potentially exploit system resources in a bothersome or undesirable manner, posing a potential security risk ³¹. PseudoManuscript is a type of spyware that allows an attacker to obtain remote access to an infected system and exfiltrate sensitive information such as VPN credentials ³². It is usually delivered via pirated software or fake installer files. Although it has not been attributed to a specific threat actor, the malware has largely affected industrial and government organisations and has characteristics associated with APT 41 activity and the Manuscript malware used by the Lazarus group ³³.

³¹ Fortiguard, “Riskware/Mewishid”, [Online]. Available: <https://www.fortiguard.com/encyclopedia/virus/7294236>

³² Malpedia, “win.pseudomanuscrpyt”, [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.pseudo_manuscript

³³ ThreatPost, “‘PseudoManuscript’ Mass Spyware Campaign Targets 35K Systems”. December 16th, 2021. [Online]. Available: <https://threatpost.com/pseudomanuscript-mass-spyware-campaign/177097/>

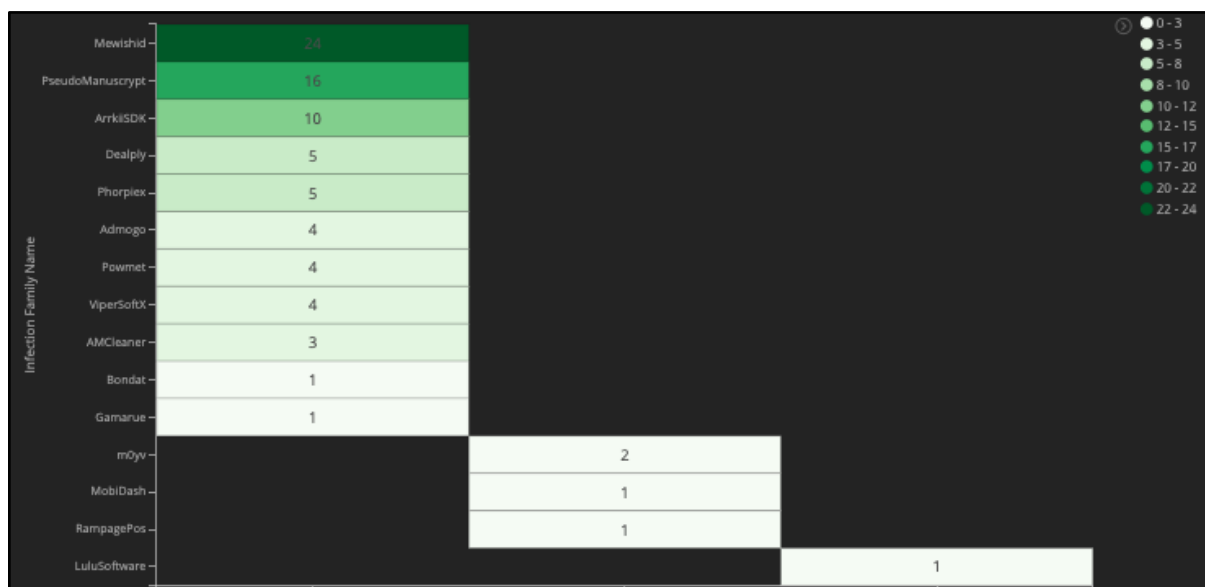


Figure 8: Heat map: malicious traffic detection count within 3 victims

The biggest amount of traffic, as shown in figure 9, was generated by the PseudoManuscript spyware. This may be due to recurrent infections or repetitive call-home attempts from infected devices. Other notable malware strains included:

- Gamarue: Usually delivered via removable devices, this worm has been used by at least one APT group in the past for information theft and installation of additional malware³⁴.
- M0yv: Although only two call-home attempts were detected, the presence of this installer is noteworthy due to its known use by the Maze ransomware developer³⁵.

³⁴ Red Canary, “Gamarue”, [Online]. Available: <https://redcanary.com/threat-detection-report/threats/gamarue/>

³⁵ Malpedia, “win.m0yv”, [Online]. Available: <https://malpedia.caad.fkie.fraunhofer.de/details/win.m0yv>

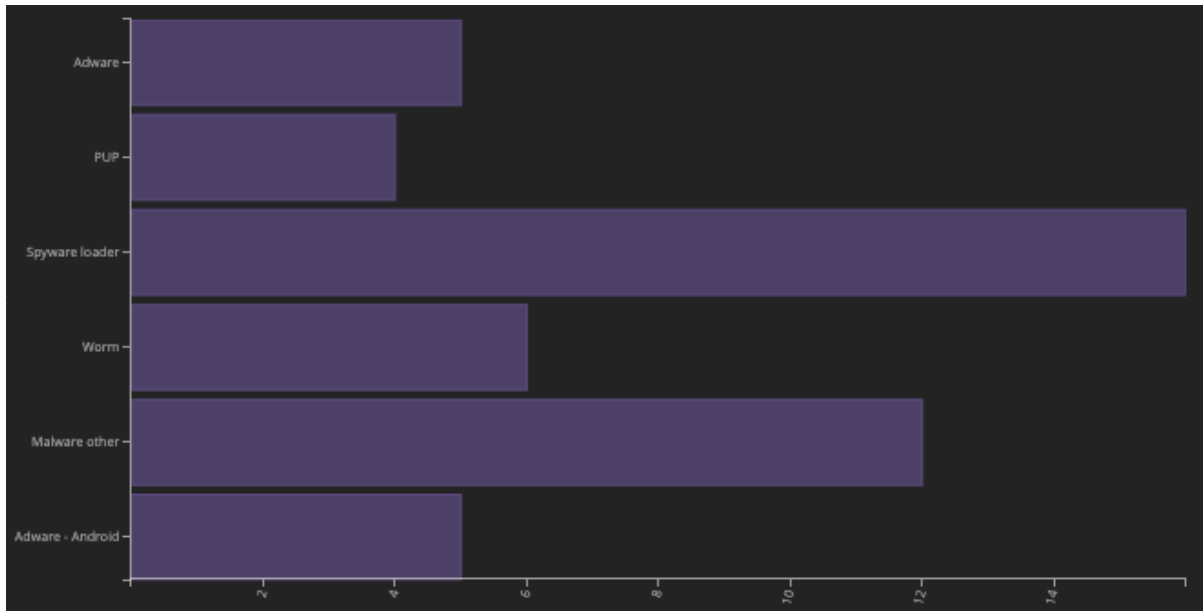


Figure 9: EU Count of infection traffic by category

Through geolocation data on IP addresses it was possible to map where traffic originated from. In the EU group, as shown in figure 10, traffic indicative of infected devices originated primarily from Ecuador (19.8%), followed by Croatia(13.3%), Kazakhstan(13.3%), Norway(13.3%), Romania (13.3%), United States (13.3%), India (6.7%), Bolivia (6.7%): the fact that malicious traffic associated with EU NGOs originated from countries outside the EU is due to the global operations of some NGOs.

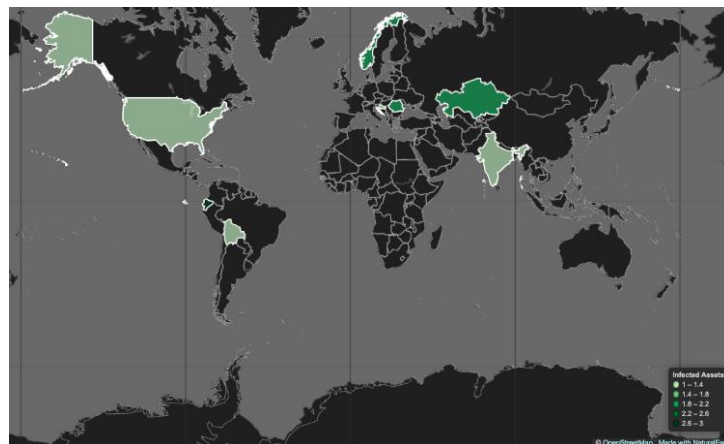


Figure 10: EU infection origin locations

Over the last year, most infections called home for less than 4 days, however repeated connection attempts indicating persistent infection continued for up to 36 days, as shown in Figure 11. The majority of infections occurred in the last half of 2023, peaking between August and November 2023, attributed largely to traffic generated by spyware infection activity breaking out from one external IP at a NGO in the EU group.

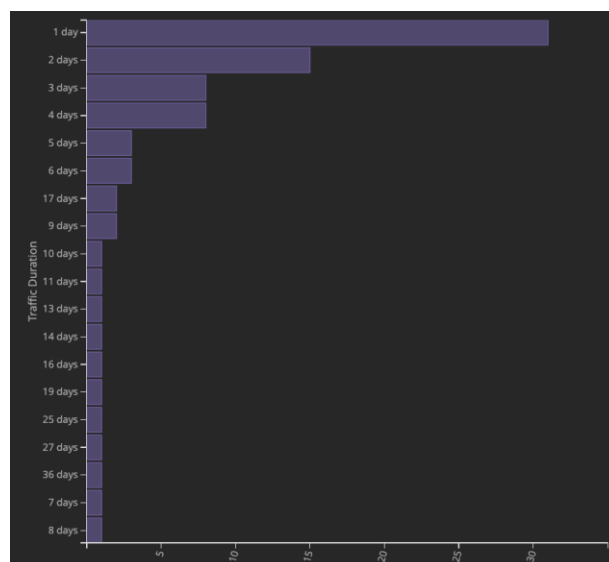


Figure 11: Call-home duration counts

4.3 Leaked credentials

According to Verizon research, stolen credentials played a role in 49% of breaches led by external actors, making credential theft one of the assets most sought-after by cybercriminals³⁶. These employ various tactics, including targeted phishing attacks, credential-stealing malware, and obtaining credentials from freely available combolists or databases purchased through initial access brokers. The leakage of these credentials presents a critical concern that demands urgent attention. Not only can it lead to unauthorised access, especially in the absence of multi-factor authentication, but it can also provide cybercriminals with valuable insights into their targets. This information may be exploited to bypass security measures, including MFA, and gain access to other services, given that passwords are frequently reused across different platforms.

The CyberPeace Institute conducted an analysis using data from deep and darknet sources to identify any instances of NGO user accounts being exposed on cybercrime and high-risk platforms, either for sharing or sale. Results showed that between January 2023 and January 2024, 70% of EU NGOs and 82% of Swiss NGOs had at least 1 user account obtained and leaked by unauthorised actors. 389 login credentials published in 31 leaked lists associated with stealer logs were found associated with over half of the NGOs in the EU group.

³⁶ Verizon. “Data Breach Investigations Report”. 2023. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>

In Switzerland, the situation was worse, with 557 accounts published in 34 leaked datasets associated with stealer logs, concerning almost two thirds of the NGOs in the Swiss group. Whilst this does not mean that the credentials leaked have been exploited by cybercriminals, or even that they could be exploited, it is a source of concern for two reasons. First, we know that only about half of the NGOs in the research use multi-factor authentication. Second, the large majority of them do not monitor leaked credentials; not only are they mostly unaware of the threat, half of them don't actively protect themselves against unauthorised access. This suggests that cybercriminals could gain access without many of the NGOs even knowing about it.

4.4 Case studies

In the context of the CyberPeace Builders program, which connects cybersecurity volunteers to NGOs, several NGOs in the EU, and in Switzerland, have shared information about past or ongoing cybersecurity incidents. Two of them have been documented publicly. An additional one has been anonymised, and is presented hereafter. Each case study will contain information about the case, the intelligence that was readily available at the time and could have been shared had an incident reporting platform existed then, along with an analysis of this information presented using the diamond model.

The Diamond Model of Intrusion Analysis is a conceptual framework used in cybersecurity to analyse and understand cyberattacks. This model was developed to provide a more structured and comprehensive way of looking at cyber intrusions, beyond the simpler approaches that were commonly used before. The Diamond Model focuses on the relationships between four core features of an intrusion:

- **Adversary:** This represents the entity that is responsible for the cyberattack. Understanding who the adversary is, their capabilities, intentions, and resources can provide insights into the attack's motives and potential next steps.
- **Capability:** This refers to the tools, techniques, and methods the adversary uses to carry out the attack. Analysing the capability can help in identifying the nature of the threat and in developing defensive measures.
- **Infrastructure:** This includes the physical and virtual resources utilised by the adversary to conduct the attack, such as malware command and control servers, and the networks used for communication. Understanding the infrastructure can aid in detecting and mitigating attacks.
- **Victim:** This represents the target of the attack, which could be an individual, organisation, or system. Knowing the victim and understanding why they were targeted can help in identifying potential future targets and in strengthening defences.

The Diamond Model emphasises the interconnectivity of these four elements, suggesting that an understanding of one can enhance understanding of the others. It's particularly useful for threat

intelligence and security analysis, as it helps analysts to piece together the how and why of an attack, predict future threats, and develop effective countermeasures.

4.4.1 Case 1: Spear-phishing attack against Belgian NGO

Case information

The EU Disinfo Lab, which had already been targeted by a DDoS attack in 2020, was targeted in 2022 by a spear-phishing campaign that leveraged a breach at USAID, a trusted government donor in the US. 149 NGOs around the world were targeted by this attack. As we had reported back in 2022: *The email, shown below, invited recipients to click on a link. Upon doing so, victims' devices downloaded a piece of malicious code that gave the attacker persistent access to their machine and allowed "action-on objectives, such as lateral movement, data exfiltration, and delivery of additional malware"*³⁷. This attack was attributed by Microsoft to Nobelium, the group behind the SolarWinds attack in 2020³⁸.

Intelligence available

Please refer to Appendix II for details on the various types of intelligence presented hereafter.

Contextual Intelligence

- **Strategic threat intelligence:** derived from exchanges with the CEO of one of the targets of the spear-phishing campaign - advanced practices regarding email communications, high awareness of phishing risks and advanced persistent threats targeted at NGOs, advanced security procedures including strong data backup policies, high-level of cybersecurity maturity, although mostly undocumented at the time of the incident.
- **Tactical Threat Intelligence:** knowledge of a previous, targeted DDoS attack and suspicions of government espionage.

Incident-Specific Intelligence

- **Technical threat intelligence:** raw data only - sender's email address, content of the email, and characteristics of the malicious link. Email and application logs available.
- **Operational Threat Intelligence:** none available at the time of the incident, but soon after a detailed Microsoft report included attribution and TTPs.

³⁷ CyberPeace Institute, "Non-Profit Organization Targeted by Cyberattack: Valuable Lessons for You". July 23rd, 2021. [Online]. Available: <https://cyberpeaceinstitute.org/news/non-profit-organization-targeted-by-cyberattack-valuable-lessons-for-you/>

³⁸ Microsoft Security, "New sophisticated email-based attack from Nobelium". April 27th, 2021. [Online]. Available: <https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/>

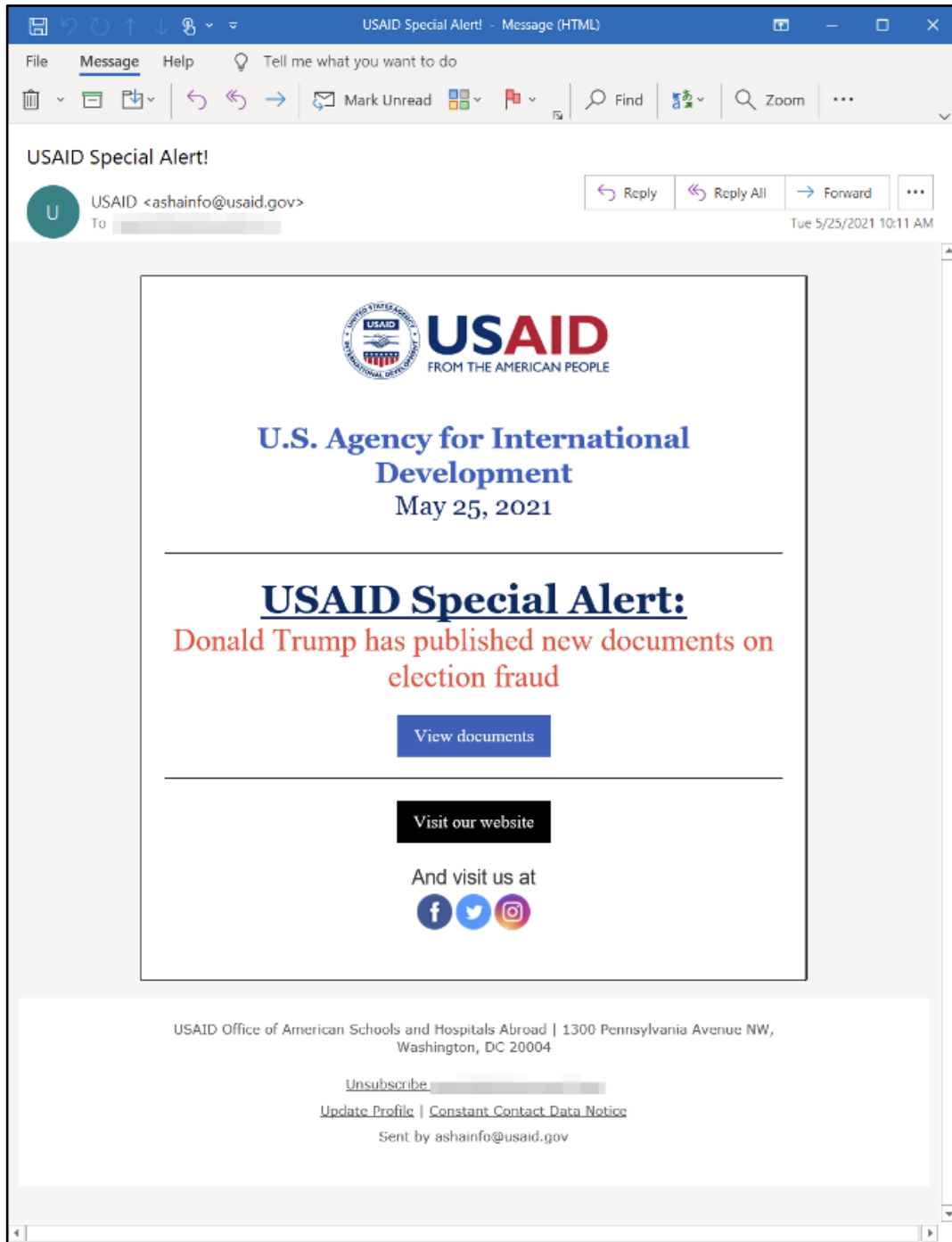
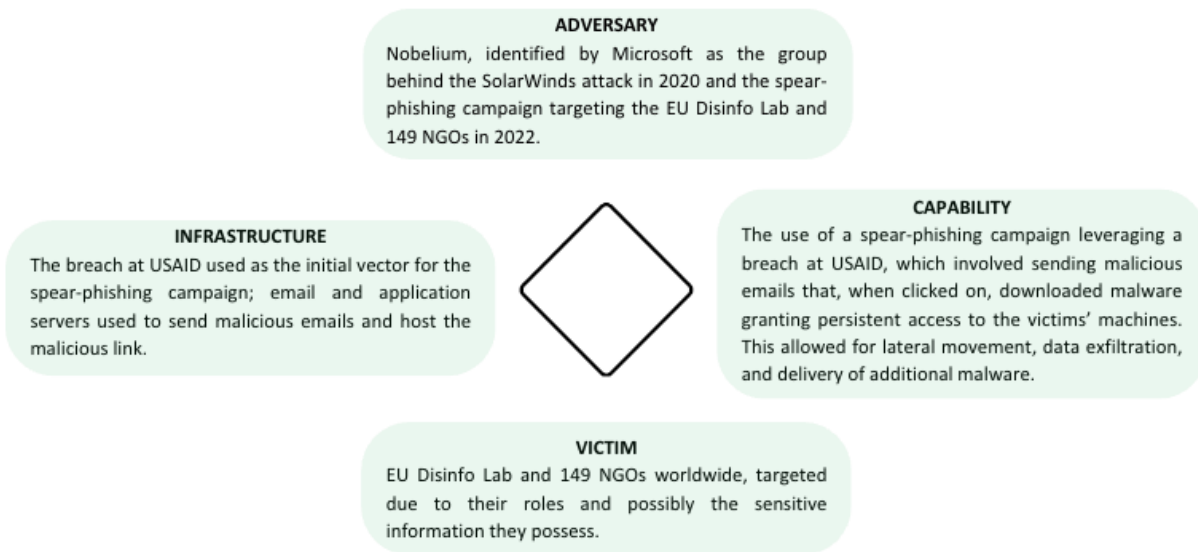


Figure 12: Spear phishing email received by EU Disinfo Lab in 2022

Case-specific diamond model



4.4.2 Case 2: Active directory compromise in a Swiss NGO

Case information

A second incident was brought to our attention impacting a Swiss NGO in 2021. As we reported back then: *On the 4th of November, the CyberPeace Institute started to see unusual e-mail messages circulating, originating from real persons, and validated as genuine by the servers. The typical content of these e-mails is constructed as a reply to an existing discussion thread and is normally written in the same language. It will typically start with a short greeting and point to two URLs. The e-mail ends with content from the original thread.*

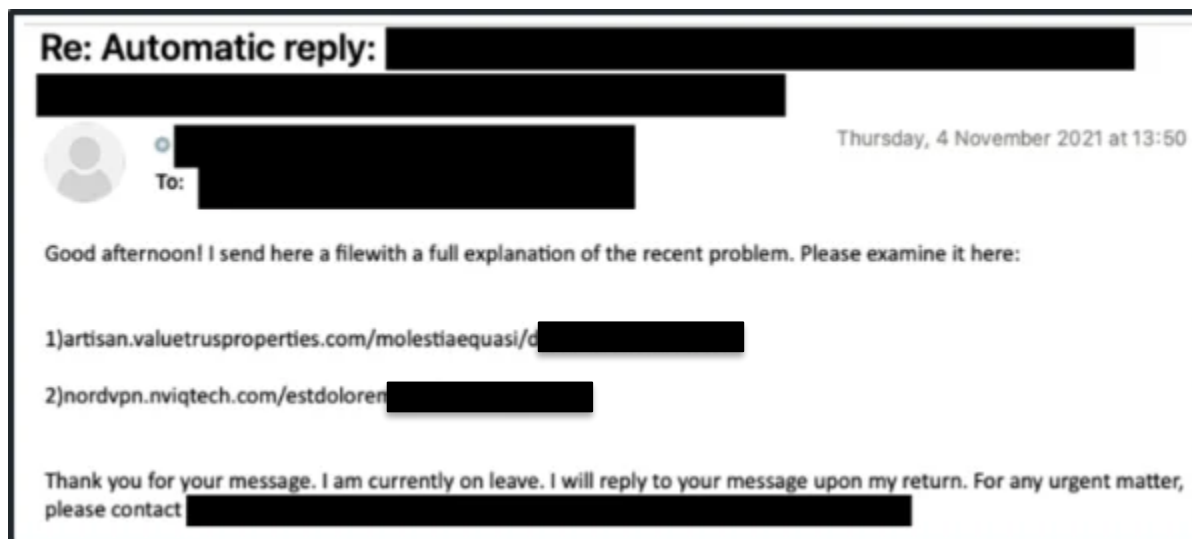


Figure 13: Sample email (sanitised)

By analysing the e-mail headers, it could be concluded that the e-mails had been sent by legitimate accounts and from the genuine servers of the entities they were supposed to come from.

The CyberPeace Institute immediately reached out to the compromised NGOs via an alternative communication channel, which confirmed that the e-mails were not legitimate, and the servers had been compromised. The Institute was able to analyse the first steps of distribution of the campaign in the hours that followed the initial detection, warn partners, and provide support to compromised entities for disaster recovery, information sharing and monitoring of the situation.

Global knowledge about the campaign among cybersecurity actors started to spread on the 8th of November and the first-stage payload was flagged as malicious by Microsoft Defender on the 9th. However, at least one victim was already hit at the very beginning of November.

The first-stage payload

Our team performed digital forensics and reverse-engineering on the attack. It was therefore possible to understand in detail how the infection occurs.

The links in the e-mail point to a zip file containing an Excel sheet (.xls). If scripts are not enabled in Excel, the user will be encouraged to enable them.



Figure 14: Message prompting the user to enable the execution of the malicious script

The script will then download more malicious content from third party compromised websites, drop the files in the C:\DATOP folder on the personal computer of the user who received the e-mail and modify a few registry keys to make it persistent with each opening of Microsoft Office. Consequently, the malicious content can operate only on Windows systems (registry keys are exclusive to Windows). The execution of the malicious script is transparent to the user. However, if the download fails, a pop-up may appear to warn that the script failed.

Intelligence from our partner Group-IB indicates that the first-stage payload was crafted using SilentBuilder (a.k.a. EtterSilent), a tool/service specifically designed for this purpose. Hence, crafting of malicious documents and further distribution can be delegated, which makes the identification of the attacker more difficult.

The sources for the second-stage payload that the CyberPeace Institute discovered in the scripts, correlate with Indicators of Compromise (IoC) reported by TrendMicro.

The second-stage payload

The malicious content, dropped in C:\DATOP on the user's computer, will download only if some specific conditions are met and the links quickly become inoperative. It is delivered in various forms, most of the time, DLLs or executables. It has elements seemingly linking to SquirrelWaffle and Qakbot/QBot, two

malware strains used in ransomware campaigns and other types of cyber extortions. They will typically become active at a later moment, when the time is right.

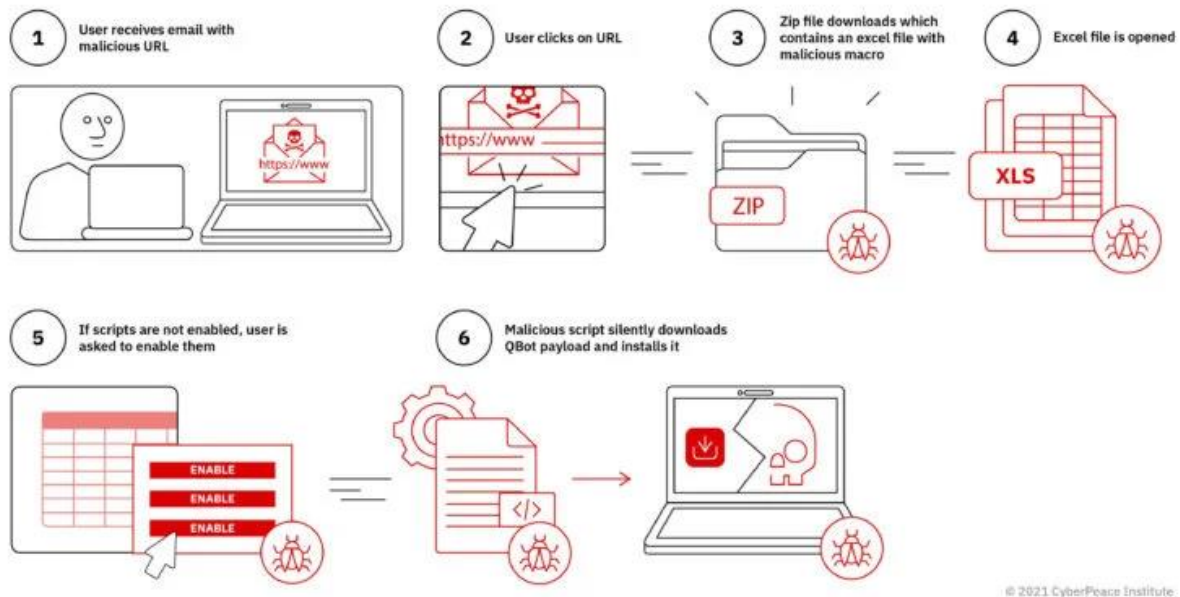


Figure 15: The QBot infection process

Based on our research to date, which classifies files as Qakbot (a banking trojan), the spreading of malicious files via malspam campaigns and findings from an ongoing investigation into the infrastructure behind the payloads, we assess this campaign to likely be of cybercrime / financially motivated nature. In some cases, it was also reported that Qakbot was used for uploading Cobalt Strike, a powerful tool for targeted attacks on infrastructures. [...]

Initial compromise

SCRT, with whom we have collaborated closely during our investigation, was able to determine that this malware campaign started with the compromise of on-premise Microsoft Exchange servers that were not up to date with security patches. More precisely, the attackers exploit the ProxyLogon (CVE-2021-26855) and ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) vulnerabilities to enter an Exchange server, deploy their tools and execute code remotely.

Microsoft Exchange 2013, 2016 and 2019 are all impacted. Multiple security updates were issued by Microsoft in 2021 to correct these vulnerabilities.

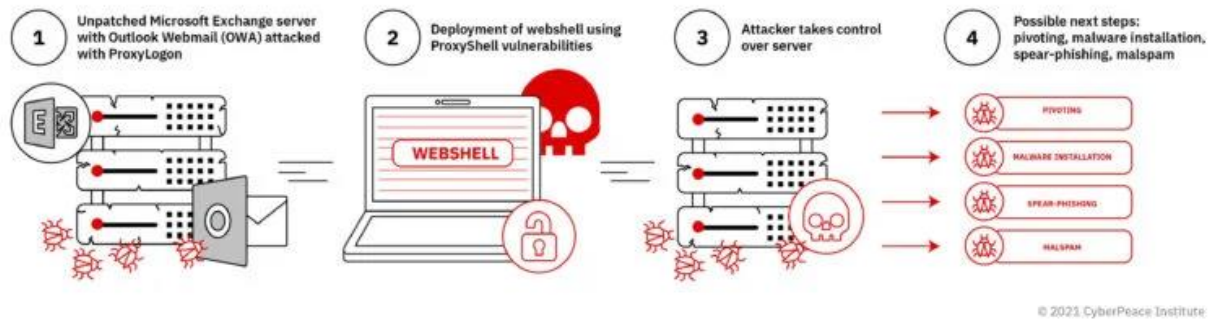


Figure 16: How the exchange server is compromised

The original article also includes defensive and recovery steps, which are not included here for brevity.

Intelligence available

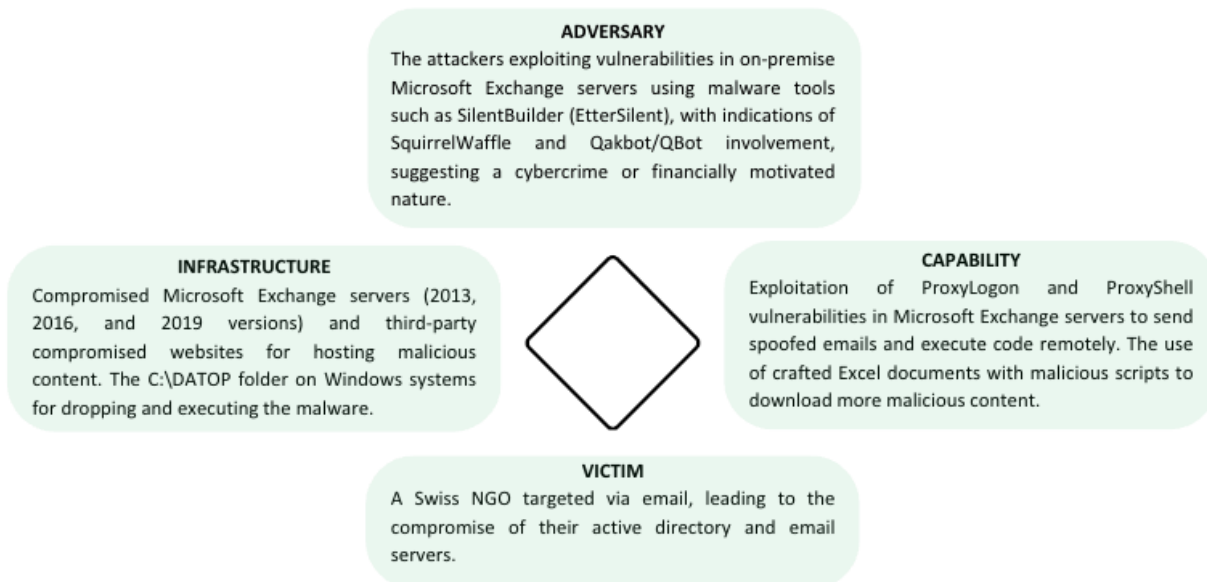
Contextual Intelligence

- **Strategic Threat Intelligence:** limited information available, the IT manager had been on extended leave and the person leading the incident response lacked cybersecurity or IT background. No documented policies were available, and although the NGO was operating in a sensitive area, there was limited awareness of the cyber threat.
- **Tactical Threat Intelligence:** none available.

Incident-Specific Intelligence

- **Technical Threat Intelligence:** spoofed emails, compromised email servers, malicious scripts and files, active directory event logs.
- **Operational Threat Intelligence:** a third-party investigation revealed that the campaign exploited vulnerabilities in on-premise Microsoft Exchange Servers (ProxyLogon and ProxyShell) to deploy malicious content. The use of specific malware strains such as SquirrelWaffle and Qakbot/QBot was also identified. Intelligence was in human-readable format only.

Case-specific diamond model



4.4.3 Case 3: EU-based NGO targeted by ransomware attack

Case information

An NGO based in the EU (country not mentioned to preserve anonymity) experienced a ransomware attack in 2023, which encrypted their web server data including 10+ years' worth of information. The threat actors demanded a €5000 ransom in exchange for a decryption key. The NGO, lacking backups and unable to identify the ransomware type, sought assistance from volunteers from the CyberPeace Institute and law enforcement.

Timeline:

- Day 0: Discovery of the ransomware attack; all files encrypted except for a ransom note.
- Day 2: Initial assessment by a volunteer; NGO's CTO had attempted communication with the attackers via Jabber.
- Day 10: Volunteer's plan of action included attempting decryption, engaging with the attackers, and contacting hosting providers and law enforcement.
- Day 11: No progress in unpacking encrypted files or contacting the attackers; potential for vandalism by amateur hackers suspected.
- Day 13: Negotiations initiated with threat actors; reduction in ransom demand to \$300.
- Day 14: Inquiry into the legitimacy of the crypto-exchange used for the ransom payment; identified as a Seychelles-registered entity.
- Day 16: NGO contemplating police involvement; concern over legal implications.
- Day 17: Decision to pay the ransom, subject to testing the decryption tool.

- Day 20: Attackers unwilling to prove decryption capability; doubts about the existence of a functional decryption tool.
- Day 21: Decision against paying the ransom due to lack of decryption proof.
- Day 22: Focus shifts to enhancing website security and preventing future attacks.

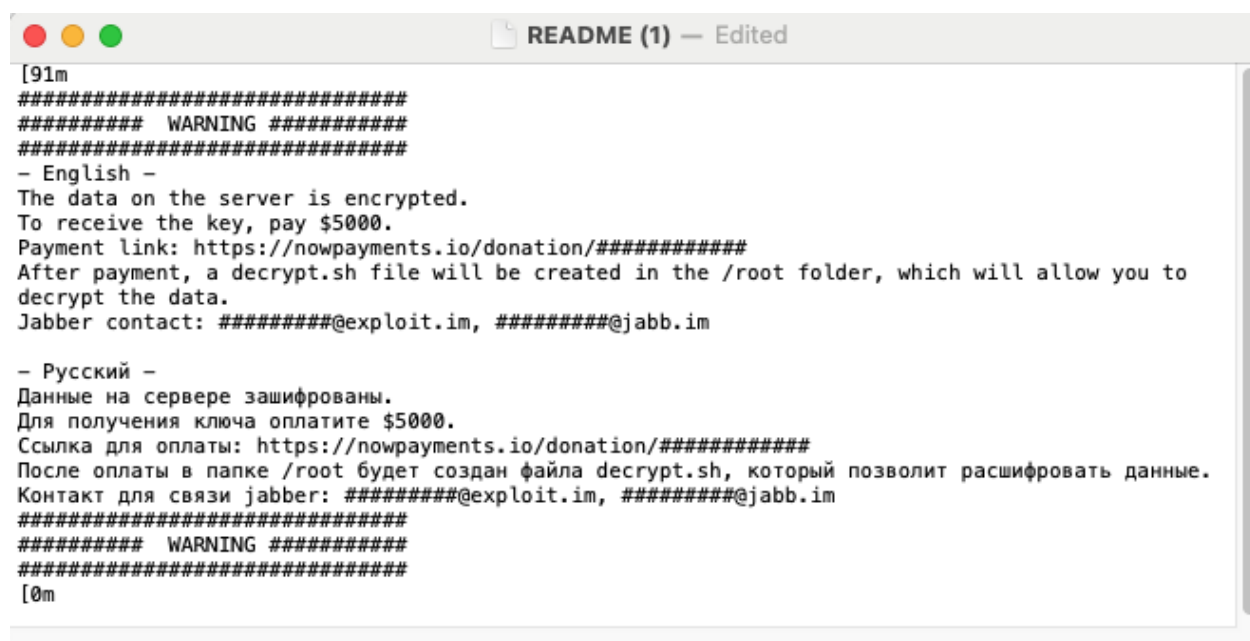
Intelligence available

Contextual Intelligence

- **Strategic threat intelligence available:** none available other than area of operation and possible motive of attackers in general.
- **Tactical intelligence:** none available.

Incident-specific intelligence

- **Technical threat intelligence:** web server location, technical details about server (e.g. Apache version) but no logs, ransomware-encrypted data on the web server, ransomware type obtained from an analysis of encrypted file on nomoreransom.org, indicating potential types like CrySIS, XORBAT, Nemucod, MegaLocker, or Hakbit.
- **Operational threat intelligence:** a ransom note demanding \$5000, Jabber handle, and nowpayment.io handle for ransom payment, victim/criminals communication logs, see figures 17 and 18, correspondence with Europol and French law enforcement regarding potential assistance and legal considerations, insights into the attackers' behaviour and capabilities based on their responses and actions.



```
[91m
#####
##### WARNING #####
#####
- English -
The data on the server is encrypted.
To receive the key, pay $5000.
Payment link: https://nowpayments.io/donation/#####
After payment, a decrypt.sh file will be created in the /root folder, which will allow you to
decrypt the data.
Jabber contact: #####@exploit.im, #####@jabbb.im

- Русский -
Данные на сервере зашифрованы.
Для получения ключа оплатите $5000.
Ссылка для оплаты: https://nowpayments.io/donation/#####
После оплаты в папке /root будет создан файла decrypt.sh, который позволит расшифровать данные.
Контакт для связи jabber: #####@exploit.im, #####@jabbb.im
#####
##### WARNING #####
#####
[0m
```

Figure 17: Ransom note received by NGO

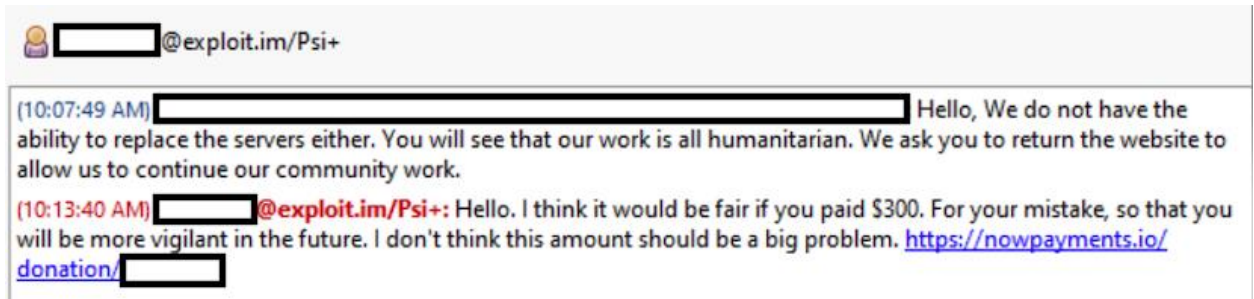
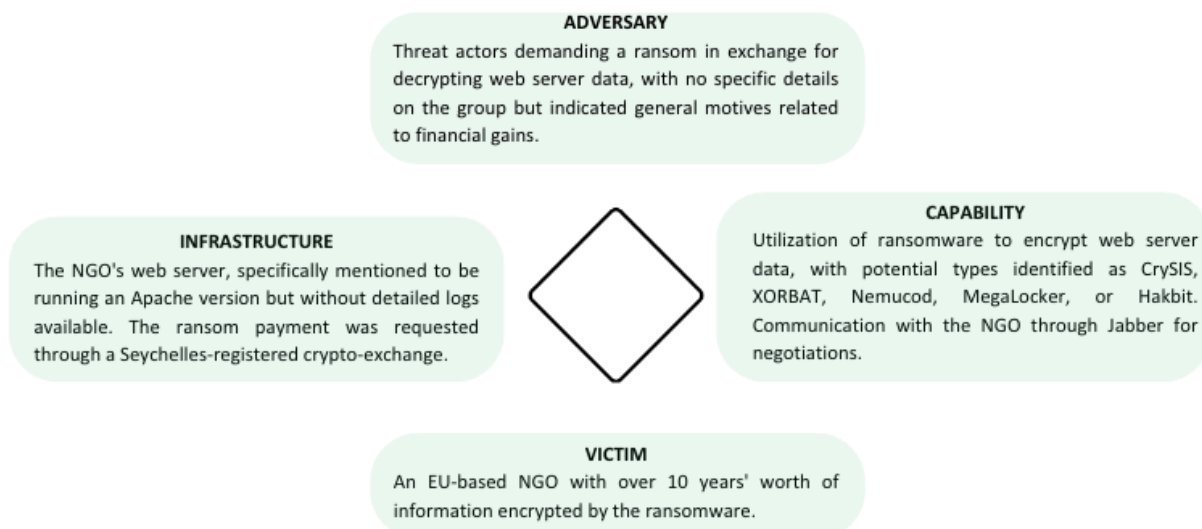


Figure 18: Negotiation communication logs

Case-specific diamond model



4.5 Key cyber incidents prioritised and managed by LEAs/CERTs

LEAs and CERTs handle a variety of cyber incidents impacting NGOs, with phishing, malware, and device compromises being the most common. In addition to responding to these threats, many agencies also take a preventive approach by assisting NGOs in strengthening their defences. Below are some key insights from their experiences.

4.5.1 Types of cyber incidents managed

When it comes to the survey conducted for LEAs and CERTs, participants were asked about the types of cyber incidents they manage for NGOs. The feedback suggests that LEAs are involved in addressing a wide range of incidents, with a particular focus on common attack vectors such as phishing and malware. The most commonly managed incidents included:

- **Phishing and credential compromise:** Several respondents noted that phishing emails, leading to credential theft or compromise, were the most frequent type of incident handled.
- **Malware:** Incidents involving malware infections were also mentioned, particularly where NGOs faced significant operational disruption.
- **Device compromise and account breaches:** In some cases, respondents dealt with suspected or confirmed device compromise, as well as breached user accounts.

In addition to responding to incidents, some agencies also play a preventive role, helping NGOs set up defences before attacks occur. One respondent highlighted a focus on prevention as a key strategy in managing potential cyber incidents.

4.5.2 Prioritisation of cyber incidents reported by NGOs

Effective incident prioritisation is critical to ensuring that NGOs receive timely responses when facing cyber threats. The survey responses revealed varied approaches to how agencies assess and prioritise reported incidents:

- **Prioritising based on victim type:** Some respondents did mention treating incidents reported by NGOs as "Priority 1" (P1) events, warranting immediate attention, especially when they involve major breaches or threats to essential services.
- **Prioritising based on impact:** Several respondents indicated that incidents are prioritised based on the potential impact on the NGO's operations or reputation, without special consideration compared to other victims.

While impact-based prioritisation remains common, there is a growing recognition among some agencies of the need to treat NGO incidents with greater urgency, especially when they involve critical breaches or threats to essential services.

5. Platform requirements for NGO cyber incident reporting to LEAs

5.1 LEA/CERTs platform requirements

Among the questions included in the surveys, several were designed to identify the challenges faced by respondents. This information enables the team to better adapt the platform to meet their needs and minimise those challenges.

5.1.1 Challenges faced when managing incidents for NGOs

Respondents highlighted several recurring challenges:

- **Lack of Resources:** Some agencies pointed to limited resources, both in terms of personnel and technology, as a major barrier. This is particularly true when dealing with multiple incidents simultaneously, which strains existing capacity.
- **Communication Gaps:** Several respondents mentioned difficulties in establishing and maintaining consistent communication with NGOs, which can lead to delays in incident response.
- **Lack of Cybersecurity Awareness in NGOs:** Many NGOs are not fully equipped to identify or report cyber incidents, making it harder for LEAs to intervene effectively. Respondents pointed to the lack of cybersecurity training within NGOs as a key factor.

5.1.2 Types of data received from NGOs

For those respondents who receive data from NGOs, the types of data commonly provided include:

- **Incident Logs:** Many NGOs share logs that detail suspicious activity, including login attempts, IP addresses, and phishing attempts.
- **Indicators of Compromise (IOCs):** Some NGOs provide IOCs, such as malware signatures, URLs, or IP addresses involved in the attack.
- **Minimal Data:** In some cases, NGOs only provide basic data or reports, which can be insufficient for thorough investigation.

5.1.3 Success stories or positive outcomes from collaborations

Respondents were asked to share any success stories or positive outcomes from their collaborations with NGOs. A few notable examples included:

- **Prevented Major Breaches:** One respondent shared a case where early detection of phishing attempts led to the prevention of a significant data breach at a large NGO.
- **Improved Awareness:** Several respondents highlighted cases where NGOs, after receiving assistance from LEAs, implemented stronger security measures and improved their internal awareness of cybersecurity risks.

5.1.4 Cyber threat reporting platform

Data Gaps Identified by Respondents (limitations)

Respondents were asked to specify any critical data they are not receiving but would find useful. Several key data gaps were identified, which, if addressed, could significantly improve the ability of law enforcement agencies (LEAs) and NGOs to respond to and investigate cyber incidents more effectively:

- **Open Source Threat Intelligence:** One respondent mentioned that their organisation relies heavily on open-source threat intelligence but noted that the process is resource-intensive. Access to more streamlined and efficient threat intelligence sources would be useful, enabling faster decision-making without excessive manual effort.
- **Information on Security Controls Used by Other NGOs:** Several respondents highlighted the need for visibility into what security controls other NGOs have in place. This information could help with shared learning and potentially enable economies of scale when procuring cybersecurity tools or services across multiple NGOs. Shared insights into best practices and controls would also help NGOs benchmark their own security measures against industry standards.
- **Domain Associations:** One respondent pointed to the importance of domain associations—linking domains and IPs to known threats. This data would enhance the ability of LEAs to connect seemingly disparate incidents and trace cybercriminal activities across different NGOs or attack surfaces.
- **Incident Reports and IOCs:** Respondents noted the need for more comprehensive incident reports and Indicators of Compromise (IOCs). IOCs, such as methods of cyberattacks or specific pieces of evidence, are crucial for aiding investigations. LEAs stressed that any piece of evidence could be the key to identifying and catching the perpetrator, making it vital for NGOs to provide as much detail as possible in their reports.
- **Network Traffic Logs and DNS Data:** Several respondents pointed out the lack of detailed network traffic logs, particularly DNS traffic and high-level alerts that NGOs might be receiving. This data could help identify the origin and scale of attacks and detect any suspicious traffic leading up to an incident, providing valuable insights into the attack patterns.
- **Timeline of Events:** As previously mentioned, detailed timelines of incidents are often missing. Knowing exactly when an attack was first detected and how it unfolded is essential for reconstructing the events and understanding the attack's full scope. This timeline data would be invaluable for improving incident response and ensuring better preparedness for future incidents.

5.1.5 Use of data provided by NGOs

All respondents indicated that they do use the data provided by NGOs to respond to and mitigate cyber threats. However, they emphasised the importance of receiving comprehensive and timely data to facilitate faster and more effective responses.

5.1.6 Benefits of a dedicated threat reporting platform for NGOs

Respondents were asked how a dedicated cyber threat reporting platform tailored specifically for NGOs would benefit their agencies. Several potential advantages were identified:

- **Centralised Reporting and Sector Awareness:** A dedicated platform would provide a single, centralised location for NGOs to report cyber incidents, allowing law enforcement agencies to have better visibility into the types and frequency of attacks against the nonprofit sector. This would not only help identify specific threats relevant to NGOs, but also facilitate sector-wide awareness. Respondents noted that sharing best practices across the nonprofit sector would benefit all organisations, as it would provide a better understanding of the common challenges NGOs face.
- **Faster Incident Response and Threat Intelligence:** Respondents indicated that such a platform could improve incident response (IR) by making it easier to share threat intelligence in real time. With increased telemetry and Indicators of Compromise (IOCs) automatically collected and shared, the platform would enhance the speed and accuracy of law enforcement and NGO responses to cyberattacks. Keeping agencies up-to-date on what is happening in real-time would enable quicker, more informed decisions.
- **Knowledge Sharing of Latest Tactics, Techniques, and Procedures (TTPs):** Another key benefit highlighted by respondents was the ability to share the latest cybercriminal tactics, techniques, and procedures (TTPs). This would improve the knowledge-sharing process between NGOs and law enforcement, ensuring that both parties are aware of emerging threats and how to defend against them. This feature would also keep agencies informed about the latest cyberattack methods being used against NGOs, including the types of attacks, causes, and patterns that attackers may employ.
- **Threat Analysis and Pattern Detection:** The platform would allow users to analyse threats and detect patterns more effectively. By correlating incidents across the nonprofit sector, LEAs could identify trends and track the behaviours of cybercriminals, including common attack vectors and patterns that the criminals might use. This capability would support long-term investigations and help prevent future attacks by revealing recurring threats.
- **Enhanced Data Sharing and Collaboration:** A structured and consistent data-sharing mechanism would reduce the manual effort required to gather and process incident data. With features like automated data collection (e.g., IOCs, incident logs, timelines), the platform would improve collaboration between NGOs and LEAs, particularly in identifying cross-border threats or incidents that impact multiple organisations. Respondents noted that having this data available would help with incident response and threat intelligence efforts across regions.
- **Historical Data Analysis and Trend Identification:** The platform would also provide the ability to store and analyse historical data, helping LEAs and NGOs track recurring incidents and identify long-term trends. This feature would allow agencies to assess the effectiveness of their interventions over time, while also revealing deeper insights into the evolving tactics of cybercriminals targeting the nonprofit sector.

5.1.7 Specific data to be prioritised on a dedicated threat reporting platform

Respondents were asked what specific data should be prioritised on a dedicated threat reporting platform to make it actionable for their agencies. The feedback highlighted several critical types of data that would enhance the effectiveness of law enforcement responses:

- **Indicators of Compromise (IOCs):** Respondents consistently emphasised the need for real-time IOCs, such as malicious IP addresses, URLs, and file hashes. Additionally, the method of attack (e.g., was it a zero-day exploit or modified malware) would provide further context for law enforcement agencies to quickly assess and block ongoing threats or investigate their sources.
- **Detailed Incident Logs:** Many respondents noted that comprehensive incident logs, including timestamps, affected systems, DNS traffic, and actions taken, would be invaluable. These logs would allow for a more thorough analysis of the attack, providing insights into the nature of the attack and enabling LEAs to respond effectively.
- **Threat Actor Information:** Some respondents expressed the need for threat actor profiles or any intelligence related to the suspected perpetrators of the attacks. This could include any information that might link the threat to an organised crime group (OCG) or known cybercriminal group. Understanding how a cyberattack unfolded—whether the attacker changed their malware tactics or used a known vector—would be crucial for LEAs in investigating and prosecuting cybercriminals.
- **Affected Systems and Data:** It was suggested that a focus on the specific systems and data compromised during the attack should be prioritised. Knowing which systems were targeted or breached allows LEAs to better assess the severity of the attack and provide appropriate support.
- **Timeline of Events:** Several respondents indicated that a timeline of events showing when an attack was detected, how it progressed, and the response measures taken by the NGO would be critical. This would provide essential information for LEAs to reconstruct the attack and understand the effectiveness of the response.
- **Cross-Organisation Impact:** Another important piece of data identified was information on whether similar attacks are affecting multiple organisations. This would allow LEAs to identify coordinated or widespread campaigns and respond more proactively. Near misses and incidents that NGOs avoided could also be valuable for improving defences across the sector.
- **Proportionate Controls and Defences:** Respondents emphasised the importance of understanding the threats and attack vectors NGOs are facing, so law enforcement can assess what proportionate controls and defences are necessary to implement.
- **Effectiveness of Microsoft Security Toolsets:** One respondent noted the relevance of understanding the use, uptake, and effectiveness of security tools like Microsoft Defender, which many nonprofits rely on for consolidation of security controls. Case studies and walkthroughs of how these tools have helped mitigate specific attacks would be helpful in shaping defence strategies.
- **New Attack Walkthroughs:** Respondents also wanted walkthroughs of new attacks, detailing how they unfolded and what lessons could be learned from those incidents.

5.1.8 Useful features for a cyber threat reporting platform

The survey responses outlined several key features and capabilities that would make a cyber threat reporting platform more beneficial for law enforcement agencies (LEAs) and non-governmental organisations (NGOs). These features focus on improving cross-border visibility, facilitating intelligence sharing, and enhancing the ability to identify and respond to cyberattacks. Below are the major points highlighted by respondents:

- **Visibility Across Borders:** One respondent pointed out the importance of visibility across borders. Cyber threats often transcend geographical boundaries, especially in the case of global NGOs. A platform that offers cross-border visibility would enable LEAs and NGOs to track cyber threats internationally, allowing them to detect patterns and threats that might otherwise go unnoticed within local or regional contexts. This would enhance collaboration among law enforcement agencies across different countries and improve coordinated responses to global cyber threats.
- **Log and Malicious Email Sharing for Intelligence Gathering:** Another valuable feature mentioned is the ability for NGOs to easily share logs and examples of malicious emails. This would facilitate intelligence gathering across organisations, helping to identify trends and common attack vectors. One respondent suggested that Microsoft could integrate into this platform, using the shared data to help shape their protection controls. As NGOs are frequent targets of cyberattacks, having a large body of shared intelligence could help inform protection mechanisms, not just for NGOs but for the wider tech ecosystem.
- **Malicious IP Address Identification:** Several respondents emphasised the need for a feature that can flag malicious IP addresses. This real-time identification would allow NGOs and LEAs to quickly identify and block traffic from known malicious sources. By integrating this feature into the platform, organisations could proactively prevent attacks by recognising and neutralising threats before they cause damage.
- **Incident Querying via API:** One suggestion involved an API for querying incidents and indicators. This would allow NGOs and LEAs to programmatically access incident data and threat intelligence, making it easier to integrate the platform with existing security tools and systems. Such an API could enable faster response times by automating data retrieval and providing real-time updates on emerging threats.
- **Traffic Monitoring During Incidents:** A feature that provides an overview of network traffic preceding and during an incident was also highlighted as valuable. By monitoring traffic in real time, the platform could give NGOs and LEAs the ability to detect anomalies or suspicious patterns that may indicate a cyberattack in progress. This feature would significantly enhance situational awareness during incidents, allowing for faster containment and mitigation of the threat.
- **Cyber Attacker Identification:** Respondents indicated that the platform should include capabilities to help identify the cyber attacker or the threat actor behind an incident. Whether through IP address tracing, language patterns in phishing emails, or ransomware notes, having a feature that gathers data useful for attributing attacks would be critical. This would help law enforcement agencies in tracking down and prosecuting cybercriminals, while also helping NGOs understand the nature of the threats they are facing.

- **Threat Actor Information:** Related to the identification of attackers, another respondent stressed the need for any data that might help identify the threat actor, such as IP addresses or the specific language used in phishing emails or ransomware notes. Having this information would be invaluable in building threat actor profiles and linking multiple incidents that may be perpetrated by the same group or individual.

In summary, the features and capabilities identified by respondents revolve around enhancing cross-border visibility, improving intelligence sharing, and offering advanced tools for identifying and responding to cyber threats. These include the ability to share logs and malicious emails, identify malicious IP addresses, provide API-based querying, monitor network traffic during incidents, and offer tools for identifying the threat actor. Together, these features would make a cyber threat reporting platform a highly effective tool for both NGOs and LEAs in combating cyber threats.

5.1.9 Specific support and resources for NGOs

The final question in the survey focused on the types of support or resources that would be most beneficial for NGOs to improve their cybersecurity posture. The survey responses reveal a wide range of ideas for support and resources that would benefit NGOs in strengthening their cybersecurity posture. Across the responses, several common themes emerged, highlighting the areas where NGOs face the greatest challenges and the kinds of assistance that would have the most significant impact.

- **Access to Affordable or Free Resources:** One respondent pointed out the need for support in identifying good value or free resources to help mitigate or defend against cyber threats. Given that many NGOs operate with limited budgets, accessing cost-effective or no-cost solutions is crucial. This type of assistance would enable NGOs to implement the necessary cybersecurity measures without putting additional financial strain on their operations.
- **Expertise and Leadership in Cybersecurity:** A major challenge for NGOs is the lack of internal cybersecurity expertise. As one respondent noted, providing a Virtual Chief Security Officer (vCSO) as a Service could be an effective solution. This approach allows NGOs to gain security leadership and expertise on a fractional basis, without the burden of hiring a full-time CSO, which many NGOs cannot afford. This flexible, outsourced leadership would help guide NGOs in developing and maintaining a robust cybersecurity strategy.
- **Advanced Threat Detection and Response Capabilities:** Several respondents mentioned the need for endpoint detection, Security Operations Centre (SOC) capabilities, and threat hunting training. These advanced cybersecurity measures, typically used by larger organisations, would help NGOs detect and respond to cyber threats more effectively. Additionally, threat intelligence and Extended Detection and Response (XDR) were highlighted as critical tools to help NGOs proactively identify and mitigate potential attacks before they cause significant damage.
- **Training and Tooling:** Training was one of the most frequently mentioned needs, with respondents pointing out that many NGOs lack the fundamental knowledge to manage cybersecurity risks. Training programs on basic cybersecurity practices, threat detection, and the use of specific security tools would empower NGO staff to better protect their organisations. In

addition, access to the right tooling is essential, as it would enable NGOs to monitor their networks, detect vulnerabilities, and respond to incidents more effectively.

- **User-Friendly Platforms and Points of Contact:** One respondent emphasised the importance of providing NGOs with a user-friendly cybersecurity platform that simplifies threat detection and incident reporting. NGOs often lack the technical expertise to navigate complex security systems, so a simplified interface would make it easier for them to engage with cybersecurity tools and protocols. Additionally, establishing clear points of contact with relevant agencies would streamline communication in the event of a cyber incident, ensuring that NGOs can get the help they need quickly.
- **Improving IT Infrastructure:** Some respondents also suggested enhancing the overall IT infrastructure of NGOs to support better cybersecurity practices. Upgrading outdated systems and improving network security would lay a stronger foundation for managing cyber threats. This could be paired with advice on implementing an Information Security Management System (ISMS), a structured approach to managing sensitive information and ensuring cybersecurity standards are met.
- **Regular Updates and Information Sharing:** Finally, one respondent emphasised the need for updated information on tools, techniques, and best practices. Providing NGOs with ongoing updates about the latest cybersecurity trends, threats, and tools would keep them informed and help them make informed decisions about their security strategies.

In summary, the support and resources that NGOs need to improve their cybersecurity posture include access to affordable resources, expert guidance (through services like a virtual CSO), advanced threat detection and response capabilities, training, and user-friendly tools. Providing these resources would enable NGOs to better defend against cyber threats while operating within their limited budgets and technical expertise.

5.2 NGO platform requirements

The incidents, presented in Section 4.5 involving the EU Disinfo Lab, a Swiss NGO, and an unnamed EU-based NGO vividly illustrate the diversity of cyber threats and the complexities involved in responding to such incidents. These cases underscore the challenges NGOs face, from identifying the nature of the attack to recovering from its impacts, highlighting the critical need for a structured support system.

NGOs often operate with varied scopes of work, sizes, and technical environments, which can significantly influence their vulnerability and response strategies to cyber incidents. For example, the specificity of the attacks on these NGOs underscores the importance of having a detailed understanding of an organisation's profile and technical setup to tailor the response effectively. Hence, an Organisational Information Module and Technical Infrastructure Overview feature in the platform are essential to provide law enforcement and support entities with the necessary context for effective assistance.

The detailed documentation of the type of attack, its impact, and a timeline is crucial for understanding and mitigating the incident efficiently, as seen in these cases. Whether dealing with ransomware or spear-phishing, the ability to precisely categorise the incident and outline its evolution is vital for both NGOs and responding entities. This necessity justifies the inclusion of an Incident Notification Module in the platform, ensuring incidents are accurately reported and acted upon.

The challenge of securely sharing technical data and the results of passive scans was evident in these incidents, where access to and analysis of digital evidence could have significantly impacted the response and recovery processes. The need for a Technical Data Upload Module that allows for the secure transmission of logs, forensic dumps, and other critical digital evidence is thereby highlighted, providing law enforcement with the information needed for thorough investigations.

NGOs face legal uncertainties and complexities when navigating the aftermath of cyber incidents, particularly concerning the filing of complaints and the management of legal documentation. The EU-based NGOs deliberations over legal actions illustrate the need for a Legal Support Interface module in the platform, offering guidance, templates, and a streamlined process for legal complaint filing.

Immediate access to recovery resources, including decryption tools and forensic analysis aids, is crucial for NGOs lacking in cybersecurity resources, as demonstrated by the EU-based NGO's struggle with encrypted data. A Recovery Assistance Hub on the platform would directly address this need, facilitating quicker recovery and resilience building post-incident.

The value of expert volunteer support was highlighted across these cases, underscoring the importance of a coordinated response effort. The integration of a Volunteer Support Coordination feature, including a connection to volunteer networks and a directory of managed detection and response services, responds to the essential role that expert assistance plays in incident response and recovery.

Lastly, the broader challenges faced by NGOs in terms of shared intelligence, accessibility, and proactive cybersecurity measures point to the need for optional requirements like a Cyber Threat Intelligence platform, a Translation module, and features for Incident Analysis and Trends. These additions would enrich the platform's capability to foster a collaborative, informed, and multilingual environment for cybersecurity within the NGO sector.

These cases collectively affirm the necessity for a comprehensive platform that addresses the entire spectrum of needs arising from cyber incidents in NGOs, from initial reporting and legal support to recovery and proactive defence strategies.

5.3 Platform modules proposals

5.3.1 Organisational information module

- **NGO Profile:** A section to input details about the NGO, such as proof of registration, location, scope of work, and size, to give law enforcement a comprehensive understanding of the entity.
- **Technical Infrastructure Overview:** Feature for NGOs to describe their technical environment, including network architecture, critical assets, and cybersecurity measures in place.
- **Digital Resilience Evaluation:** Option to include the NGO's cybersecurity maturity evaluations, offering context on the organisation's security posture. Connection with CyberPeace Institute's General Cybersecurity Assessment tool³⁹, or others.

5.3.2 Incident notification module

- **Type of attack:** Enables NGOs to specify the nature of the cyberattack (e.g., ransomware, phishing, DDoS) for precise incident categorisation.
- **Incident Impact:** Allows for the reporting of ransom demands, including amount, cryptocurrency wallet addresses, and communication logs with attackers, if relevant, but also operational impacts, etc.
- **Incident timeline:** Feature to document the sequence of events, facilitating a clearer understanding of the incident's evolution.
- **Ticketing system:** Proof for the NGO that an incident was reported.

5.3.3 Technical data upload module

- **Secure File Upload:** Secure upload capability for logs, forensic dumps, encrypted files, ransom notes, and other digital evidence that could aid in the investigation.
- **Passive Scan Results:** Ability to upload passive scan results to provide insights into potential vulnerabilities exploited in the attack.

5.3.4 Legal support interface

- **Legal Complaint Assistance:** Guidance and templates to help NGOs file a legal complaint regarding the cyber incident, directly through the platform, including information on different ways to do this in each country.
- **Existing Complaint Documentation:** Facility to upload documentation related to any complaints already filed with law enforcement or other authorities.

³⁹ "Measure to Improve: The GCSA's Role in Nonprofit Cyber Resilience", CyberPeace Institute, January 30, 2024, <https://cyberpeaceinstitute.org/news/measure-to-improve-the-gcsas-role-in-nonprofit-cyber-resilience/>

5.3.5 Recovery assistance hub

- **Decryption Tools Repository:** Direct access to a curated list of up-to-date decryption tools and guides for their use (e.g. www.nomoreransom.org).
- **Forensic Analysis Resources:** Links to forensic tools and resources to assist NGOs in conducting preliminary investigations and preserving evidence for law enforcement.

5.3.6 Volunteer support coordination

- **Volunteer Assistance Request:** Connection to the CyberPeace Builders, to allow NGOs to ask for help from volunteers.
- **MDR Directory:** Access to a directory of managed detection and response companies willing to assist NGOs.

5.3.7 Optional requirements

- **NGO-specific Cyber Threat Intelligence platform:** A platform dedicated to NGOs that would allow them to share / digest cyber threat intelligence with / from each other, potentially augmented by partner feeds.
- **Translation module:** The platform could be made available in all EU languages.
- **Incident Analysis and Trends:** Feature for NGOs to access anonymised data on recent cyber threats and trends affecting the sector, fostering a proactive approach to cybersecurity.
- **Feedback Mechanism:** A system for NGOs to provide feedback on their experience with the incident reporting process and the assistance received, allowing for continuous improvement of the platform.

These platform requirements are designed to streamline the incident reporting process for NGOs, enhance their access to recovery tools and expert support, and foster a collaborative environment between NGOs, law enforcement, and cybersecurity volunteers. This holistic approach not only aids in the immediate response to incidents but also contributes to building a more resilient cyber ecosystem for NGOs.

Conclusion

The comprehensive analysis presented in this study underscores the complex cybersecurity challenges and vulnerabilities NGOs within the EU must confront. Despite varying levels of cybersecurity maturity, the findings reveal a concerning landscape: commendable efforts in areas like backup procedures and digital perimeter security are offset by pronounced deficiencies in incident response capabilities and advanced endpoint protection. The widespread vulnerabilities identified in network, application, and data security domains, coupled with an array of cyber incidents ranging from ransomware attacks to credential leaks, highlight an urgent need for cybersecurity within the EU humanitarian NGO sector.

The survey revealed key challenges and opportunities in cybersecurity collaboration between LEAs and NGOs. Limited interaction and common threats like phishing highlight the need for structured communication and affordable cybersecurity tools. A unified cyber threat reporting platform would streamline reporting, improve incident response, and enhance collaboration across NGOs. By addressing current vulnerabilities and fostering proactive data sharing, the platform would significantly strengthen NGOs' resilience against growing cyber threats.

In response to these challenges, the development and implementation of a dedicated incident reporting platform, as envisaged by the UnderServed project, emerge as critical. This platform, tailored to address the unique needs and vulnerabilities of EU NGOs, would serve as a cornerstone for improving cyber incident management and recovery. By enabling efficient reporting, tracking, and analysis of cybersecurity incidents, the platform would facilitate swift response and mitigation efforts, significantly reducing the potential impact of cyberattacks on EU NGO operations.

Moreover, such a platform would foster a collaborative environment, collectively enhancing the sector's cybersecurity preparedness and resilience. The integration of features such as real-time communication channels, access to decryption tools, forensic resources, and volunteer support further underscores the platform's role in bridging critical gaps in EU NGO cybersecurity capabilities.

Ultimately, by advocating for systematic data collection, sharing, and analysis of cyber incidents, this report underscores the imperative for EU NGOs to adopt a proactive and collaborative approach to cybersecurity. In doing so, EU NGOs can not only defend against current cyber threats but also anticipate and prepare for future challenges, ensuring their ability to continue delivering vital humanitarian and developmental services without interruption.

The proposed incident reporting platform represents a significant step forward in achieving these objectives, symbolising a collective commitment to safeguarding the invaluable contributions of EU NGOs in a digitally dependent world.

References

- Al Achkar, Ziad. n.d. "Achieving Safe Operations Through Acceptance: Challenges and Opportunities for Security Risk Management." [Online]. Available: https://gisf.ngo/wp-content/uploads/2021/12/Digital_Risk_how_new_technologies_impact_acceptance_and_raise_new_challenges_for_NGOs.pdf
- B2B Cyber Security, "Ransomware Victim Caritas Refuses to Pay". September 25th, 2022. [Online]. Available: <https://b2b-cyber-security.de/en/ransomware-opfer-caritas-will-nicht-zahlen/>
- Cybersecurity and Infrastructure Security Agency CISA, "Known Exploited Vulnerabilities Catalog". <https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1>
- CNN, "Humanitarian aid to Ukraine disrupted by cyberattacks". April 23rd, 2022. [Online]. Available: <https://edition.cnn.com/2022/04/23/politics/humanitarian-aid-ukraine-war-cyberattacks/index.html>
- CVE-2019-11043 Detail, "NIST National Vulnerability Database. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2019-11043>
- CyberPeace Institute. "Cyber Incident Tracers | CyberPeace Institute," October 10, 2023. <https://cyberpeaceinstitute.org/cyber-incident-tracers>
- CyberPeace Institute. "CyberPeace Builders." CyberPeace Builders, n.d. <https://cpb.ngo/>
- CyberPeace Institute, "Measure to Improve: The GCSA's Role in Nonprofit Cyber Resilience". January 30th, 2024. [Online]. Available: <https://cyberpeaceinstitute.org/news/measure-to-improve-the-gcsas-role-in-nonprofit-cyber-resilience/>
- CyberPeace Institute, "Non-Profit Organization Targeted by Cyberattack: Valuable Lessons for You". July 23rd, 2021. [Online]. Available: <https://cyberpeaceinstitute.org/news/non-profit-organization-targeted-by-cyberattack-valuable-lessons-for-you>
- Data Protection Commission (DPC), "Annual Report 2023," [Online]. Available: https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf

- European Civil Protection and Humanitarian Aid Operations. "Humanitarian Partners". February 1st, 2024. [Online]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/partnerships/humanitarian-partners_en
- Forbes, "Hackers Sell Access to a \$2 Billion Nonprofit, a Californian Hospital, and Michigan Government" February 23rd, 2022. [Online]. Available: <https://www.forbes.com/sites/thomasbrewster/2022/02/23/hackers-sell-access-to-a-2-billion-nonprofit-a-californian-hospital-and-michigan-government/?sh=33a007dc5758>
- Fortiguard, "Riskware/Mewishid", [Online]. Available: <https://www.fortiguard.com/encyclopedia/virus/7294236>
- International Committee of the Red Cross (ICRC), "Cyber attack on the ICRC: What we know". June 22nd, 2022. [Online]. Available: <https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know>
- L'Informé, "Les dessous de la cyberattaque contre Akadem, le site du Fonds Social Juif Unifié" [Online]. October 4th, 2023. Available: https://www.linforme.com/tech-telecom/article/les-dessous-de-la-cyberattaque-contre-akadem-le-site-du-fonds-social-juif-unifie_1051.html
- Limerick Leader, "Limerick Domestic Abuse Charity Targeted in Cyber Attack". March 23rd, 2020. [Online]. Available: <https://www.limerickleader.ie/news/home/773188/limerick-domestic-abuse-charity-targeted-in-cyber-attack.html>
- Malpedia, "win.m0yv." [Online]. Available: <https://malpedia.caad.fkie.fraunhofer.de/details/win.m0yv>
- Malpedia, "win.pseudomanuscrpyt". [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.pseudo_manuscript
- Microsoft Security, "New sophisticated email-based attack from Nobelium". April 27th, 2021. [Online]. Available: <https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/>
- Misconfigurations and Weaknesses Known to be Used in Ransomware Campaigns | CISA" Cybersecurity and Infrastructure Security Agency CISA <https://www.cisa.gov/stopransomware/misconfigurations-and-weaknesses-known-be-used-ransomware-campaigns>
- NIST. "Cybersecurity Framework | NIST". [Online]. Available: <https://www.nist.gov/cyberframework>

- NIST - "CVE-2019-0211." [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2019-0211>
- NIST "CVE-2021-40438." [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2021-40438>
- Ralph, Pat. "Philabundance Falls Victim to Cyberattack, Loses Almost \$1 Million." PhillyVoice, December 1st, 2020. <https://www.phillyvoice.com/philabundance-cyberattack-theft-1-million-dollars/>
- Red Canary, "Gamarue", [Online]. Available: <https://redcanary.com/threat-detection-report/threats/gamarue/>
- S. C. Leadership, "What is CVSS - Common Vulnerability Scoring System". October 24th, 2023. [Online]. Available: <https://www.sans.org/blog/what-is-cvss/>
- Shaping Europe's Digital Future. "Cybersecurity Policies". March 20th, 2024. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>
- Solidarity Action Network, "Resisting Sustained Phishing Attacks". [Online]. Available: <https://solidarityaction.network/wp-content/uploads/resisting-sustained-phishing-attacks.pdf>
- SOS Children's Villages International, "Statement on Cyber Security Incident". October 6th, 2024. [Online]. Available: <https://www.sos-childrensvillages.org/news/statement-on-cyber-security-incident>
- Spelhaug, Justin. "Strengthening Cyber Defenses for Nonprofits." Microsoft on the Issues, December 13th, 2021. <https://blogs.microsoft.com/on-the-issues/2021/10/21/cyber-defenses-security-program-nonprofits/>
- Tech Monitor, "EU Disinfo Lab in DDoS Attack". July 20th, 2020. [Online]. Available: <https://techmonitor.ai/technology/cybersecurity/eu-disinfo-lab-in-ddos-attack>
- The Common Vulnerabilities and Exposures (CVE) Website. [Online]. Available: <https://www.cve.org/>
- The Irish Times, "Rehab Group Falls Victim to Cyber Attack". March 16th, 2022. [Online]. Available: <https://www.irishtimes.com/business/technology/rehab-group-falls-victim-to-cyber-attack-1.4828860>

- ThreatPost, “‘PseudoManuscript’ Mass Spyware Campaign Targets 35K Systems”. December 16th, 2021. [Online]. Available: <https://threatpost.com/pseudomanuscript-mass-spyware-campaign/177097/>
- United Nations University, Institute of Macau, “Civil society organizations' cyber resilience”. 2021. [Online].
https://collections.unu.edu/eserv/UNU:8262/Civil_Society_Organizations_Cyber_Resilience.pdf
- Verizon. “Data Breach Investigations Report”. 2023. [Online]. Available:
<https://www.verizon.com/business/resources/reports/dbir/>
- Ville De Genève - Site Officiel. “International Institutions, Permanent Missions and Non-governmental Organisations”. February 5th, 2024. [Online]. Available:
<https://www.geneve.ch/en/themes/international-geneva/international-institutions-permanent-missions-non-governmental-organisations>

Appendices

Appendix I - Survey questions

NGO survey questions

1. 1A. Does your NGO have an up-to-date assets inventory of all your digital and physical assets?
2. 2A. Does your NGO ensure adequate management of user accounts of people who join or leave the organisation (i.e., account creation, update, suppression)?
3. 3A. Does your NGO follow a process to provide access privileges based on user roles and responsibilities?
4. 4A. Does your NGO ensure that all physical and digital assets are up-to-date and adequately configured?
5. 5A. Does your NGO securely dispose of hardware and software assets that are no longer needed/supported?
6. 1B. Are your NGO's endpoints (computers, laptops, mobile devices) protected with up-to-date security software against malware and other cyber threats (e.g., antivirus)?
7. 2B. Are your NGO's physical assets (i.e., computers, laptops) equipped with a virtual firewall between your organisation's network and the internet?
8. 1C. Does your NGO use a Virtual Private Network (VPN) for staff to access work resources remotely?
9. 2C. Does your NGO have a list of all the cloud services it uses for monitoring and security purposes (e.g. email, HR, finance tool, etc.)?
10. 1D. Are your NGO's critical functions for delivery of essential services to vulnerable populations identified?
11. 2D. Is your NGO backing up its critical functional data?
12. 3D. Are your NGO's backups stored securely and verified for restoration?
13. 4D. Does your NGO have a disaster recovery plan in place in the event of a cybersecurity incident?
14. 1E. Did your NGO ever conduct a website vulnerability scan?
15. 2E. Did your NGO ever conduct a technical email security assessment?
16. 1F. Does your NGO use multi-factor authentication (MFA) for accessing sensitive data or systems (e.g. email, cloud, finance tool, social media, etc.)?
17. 2F. Does your NGO use a password manager to securely store and manage passwords?
18. 3F. Does your NGO educate users to have passwords that are unique and complex?
19. 1G. Does your NGO provide cybersecurity training to its employees and volunteers?
20. 2G. Did your NGO conduct phishing simulations for all staff?
21. 1H. Does your NGO have the capability to monitor the dark web to identify any potential data leaks?
22. 2H. Does your NGO have the capacity to monitor logs activity?

- 23. I1. Does your NGO have a cybersecurity policy?
- 24. I2. Does your organisation have an incident response plan?
- 25. I3. Does your organisation have cyber insurance coverage?
- 26. I4. Does your NGO have a data protection policy?
- 27. I5. Does your NGO have the capacity to encrypt sensitive data?
- 28. I6. Is your NGO using secure channels to share sensitive data?
- 29. I7. Does your NGO have a vulnerability disclosure policy?
- 30. I8. Does your NGO have an AI guidance policy?

LEA survey questions

- 1. Organisation
- 2. Full name
- 3. Email
- 4. Position
- 5. Does your agency have interactions with NGOs regarding cyberattacks? (Yes/No)
 - a. How often do these interactions occur?
 - i. Daily
 - ii. Weekly
 - iii. Monthly
 - iv. Other: [Please specify]
 - a. Through what channels do these interactions occur? (Email, Phone, In-person, Online Platform)
 - b. What types of cyber incidents are you managing for NGOs?
 - c. How do you prioritise incidents reported by NGOs?
 - d. What challenges do you face when managing incidents for NGOs?
 - e. Are you receiving data from NGOs about cyberattacks? (Yes/No)
 - f. If yes, what types of data are you receiving from NGOs about cyberattacks?
 - g. Can you share any success stories or positive outcomes from your collaborations with NGOs on cyberattack incidents?
 - h. How do you measure the impact of your agency's interventions in cyber incidents reported by NGOs?
- 6. If there is critical data you are not receiving but would find useful, please specify what it would be.
- 7. Do you use the data provided by NGOs to respond to and mitigate cyber threats? (Yes/No)
- 8. How would a dedicated threat reporting platform benefit your agency?
- 9. What specific data would you like to see prioritised on such a platform that would be actionable for your agency?

10. What features or benefits could a cyber threat reporting platform offer to make it more useful for law enforcement agencies?
11. Would support or resources be beneficial for NGOs to improve their cybersecurity posture? (Yes/No)
12. If yes, what kind of support or resources would be beneficial for NGOs to improve their cybersecurity posture?

Appendix II: NGO-led shareable cyber threat intelligence

When discussing the multifaceted landscape of cybersecurity, it is crucial to understand the different layers of threat intelligence: Strategic, Tactical, Technical, and Operational. Each plays a pivotal role in painting a comprehensive picture of cyber threats, enabling organisations to prepare, defend, and respond effectively to the evolving digital dangers. By dissecting these layers, we delve into the depths of cybersecurity strategies, from high-level policy planning to the technical specifics of thwarting cyberattacks.

1 Contextual intelligence

1.1 Strategic threat intelligence

- **Source:** Primarily obtained from NGO senior leadership, supplemented by insights from external cybersecurity advisories and sector-specific intelligence reports.
- **Description:** Contextual intelligence provides a non-technical overview of the NGO's cybersecurity posture, encompassing the availability of security governance documents (such as data protection policies), vulnerabilities, and historical incidents. It also includes insights derived from sector-wide comparisons and predictive analyses to anticipate evolving threats influenced by NGO activities.
- **Format:** Typically presented in text format, with the option to include presentations, reports and other types of human-readable documents.

1.2 Tactical threat intelligence

- **Source:** Chief Information Security Officer (CISO), supplemented by technical staff and incident response teams.
- **Description:** Tactical intelligence delves into the tactics, techniques, and procedures (TTPs) employed by threat actors in previous instances, targeting either the NGO directly or similar organisations. Consideration is given to known bad actor profiles or threat actor groups relevant to NGOs.
- **Format:** Presented in text and documents. Could be structured formats such as JSON or XML for enhanced interoperability.

2 Incident-specific intelligence

2.1 Technical threat intelligence

- **Source:** NGO's IT team or subcontractors, including cybersecurity product vendors for threat feeds.
- **Description:** Technical threat intelligence comprises raw technical data such as IP addresses, URLs, malware signatures, phishing email samples, forensic dumps, and other artefacts. It may

also include specific types of logs (e.g., firewall, network, application) and recommended formats for sharing.

- **Format:** Raw technical data, with common formats like CSV or PCAP for network traffic.

2.2 Operational threat intelligence

- **Source:** NGO's CISO, infosec experts, or specialised subcontractors, potentially augmented by partnerships with external cyber intelligence sharing communities.
- **Description:** Operational intelligence provides detailed insights into specific attacks, including their nature, motive, timing, and execution methods. Consideration is given to the effectiveness of response measures and mitigation strategies employed.
- **Format:** typically shared in the Structured Threat Information eXpression (STIX) format, facilitating standardised sharing and analysis through protocols like the Trusted Automated Exchange of Indicator Information (TAXII) and platforms like the Malware Information Sharing Platform (MISP) or OpenCTI.

Appendix III: Glossary

- **Attack and Cyberattack:** 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.
- **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.
- **Cyberpeace:** a state achieved when human security, dignity and equity are ensured in digital ecosystems.
- **Cybersecurity:** the practice of protecting computer systems and networks from unauthorised 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.
- **Data breach:** 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): 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 authorised parties can view it.
- Firewall: a part of a computer system or network that is designed to block unauthorised access while permitting outward communication.
- Hacktivists: persons or groups that gain unauthorised 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 organisation'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.
- Legacy systems: outdated computing software and/or hardware that are unable to resist contemporary forms of attack, and present a risk for other applications and data that may share the same infrastructure.

- Man-in-the-middle attack (MitM): 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).
- 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 organisation's domain.
- Risk: the likelihood of harm or loss due to vulnerabilities. Cyber risk encompasses threats such as cyberattacks, data breaches, and system failures, necessitating proactive management to safeguard against potential harm.
- 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: 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 unauthorised entry into a secure system.
- Secure Sockets Layer (SSL): an encryption-based Internet security protocol.
- The principle of least privilege (PoLP): 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, 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 anonymises 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.