# 2024
# CYBER THREATS TO NGOS

## POWERED BY THE CTA

The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners who work together in good faith to share threat information and improve global defenses against cyber adversaries. CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

1.  Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real-time.

2.  Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3.  Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow globally, enriching both the quantity and quality of the information shared among its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operation collaboration to enable a more secure future for all.

For more information about the Cyber Threat Alliance, please visit:
https://cyberthreatalliance.org.

*Cover Image produced by Lars Conard*

## CYBER THREATS TO NGOS WORKING COMMITTEE MEMBERS

**Cisco Talos**
Nick Biasini

**CyberPeace Institute**
Adrien Ogee
Alexandru Lazar
Stéphane Duguin

**Defending Digital Campaigns**

**Fortinet**
Val Saengphaibul

**Granitt**
Runa Sandvik

**NetHope**
James Eaton-Lee
Dianna Langley

**NGO-ISAC**
Ben Johnson
Frank McGothigan

**Rapid7**
Martin McKeay

**RoundTable**
Karim Beldjilali

**Symantec by Broadcom**
Scott Swett
Brian Ewell

**Unit 42 Palo Alto Networks**
Amer Elsad

**UC Berkeley Center for Long-Term Cybersecurity (CLTC)**
Sarah Powazek

**Cyber Threat Alliance**
Chelsea Conard
Michael Daniel
Jeannette Jarvis
Linda Beverly
Kate Holseberg

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

*"Good cybersecurity is a team sport. Nonprofits need the strong support of the public and private sectors so they can safely and consistently continue to serve the parts of the planet and people who need it most."*

*— Dianna Langley, NetHope*

Cyber threats affect everyone, but the nature of those threats and the resources to address them vary widely between organizations. Non-governmental organizations (NGOs) occupy a challenging place along this continuum because they face an array of significant threats, and have limited resources to counter this activity.

Given these challenges, the Cyber Threat Alliance (CTA) organized a coalition of industry leaders to focus on cybersecurity for NGOs. This Joint Analytic Report (JAR) outlines prevalent threats, suggests remediation strategies, and provides guidance for the executive leadership to enhance their nonprofit's cybersecurity posture. Aimed at empowering NGOs, this report is designed to equip organizations with an understanding of prevalent cyber dangers and to arm them with effective countermeasures.

Recommendations for NGOs:

1.  **Emphasize Preparedness and Security Fundamentals:** NGOs must prioritize cybersecurity readiness; apply two-factor authentication (2FA), update software, and make regular backups as basic standards of security.

2.  **Adopt a Comprehensive Cybersecurity Strategy:** A robust framework includes adopting and maintaining general cybersecurity policies and response plans, as well as contracting a Managed Security Service Provider (MSSP).

3.  **Executive Responsibilities:** Leadership plays a pivotal role to navigate the cybersecurity landscape. A concerted effort from the boardroom to the frontline employees is essential to ensure the NGO's mission and operational integrity are safeguarded against cyber threats.

4.  **Leverage Free and Accessible Resources:** Numerous free resources are highlighted in the CTA website Recommended Resources to aid NGOs to enhance their cybersecurity posture, including tools for phishing training, tabletop exercises (TTXs), and comprehensive guides from entities like NetHope, CyberPeace Builders, and NGO-ISAC.

This JAR serves as a call to action, urging NGOs and the cybersecurity industry to address cybersecurity challenges head-on. By fostering a culture of proactive cybersecurity management, NGOs can significantly enhance their resilience against cyber threats. This collaborative approach not only secures critical data and resources, but also ensures the continuity of vital missions in the face of evolving digital risks.

# INTRODUCTION

Non-governmental organizations (NGOs) undertake a wide range of activities, working to address various social, environmental, and humanitarian concerns. They play a crucial role in complementing the efforts of governments and other stakeholders to address various challenges around the world. Every day, NGOs battle cyber actors seeking to perform reconnaissance, harvest stolen credentials and data, steal money, jeopardize the NGO's mission, and damage their reputation, to name a few. NGOs' cybersecurity capabilities to defend against their adversaries can vary due to the size, maturity, and resources to their organizations.

NGOs face many of the same cyber threats plaguing other industries, but they struggle to adequately fund or resource their cybersecurity needs. Numerous organizations have minimal budgets but large, distributed networks serving vulnerable populations. This mismatch contributes to them being attractive targets to threat actors including nation-states and hacktivists.

The resource limitations are a significant concern not just at the individual organization level, but across the entire NGO sector. Despite these challenges, NGOs have the opportunity to prioritize cybersecurity investments to protect their missions' successes. By shifting their perspective, NGOs can move away from viewing cybersecurity as a "technical luxury beyond our means" to recognizing it as "a critical enabler for achieving our goals."

Fortunately, enhancing security does not always come with a hefty price tag. Many measures focus on establishing effective processes and policies rather than high-tech solutions. As a result, NGOs can notably boost their cybersecurity without incurring substantial costs.

This report is an educational tool for NGOs, designed to elevate NGOs' awareness of cyber threats, offer remediation strategies, and assist in advocating leadership to invest in cybersecurity. It serves as a catalyst for cultural transformation within organizations, showcasing how NGOs can effectively evolve their cybersecurity posture. This comprehensive resource is a testament to the unique collaboration among industry leaders, notably CTA members working with entities like NetHope, the CyberPeace Institute, and the NGO-ISAC to build data-informed guidance and best practices that reflect the current landscape and the specific needs of NGOs. Through this collective effort, CTA aims to equip NGOs with tools to strengthen their cybersecurity practices, ensuring their crucial missions proceed with enhanced security and resilience.

Addressing these challenges requires collaboration from cybersecurity practitioners and NGOs. By enhancing the support framework dedicated to cybersecurity for NGOs, we can more effectively empower organizations to navigate the intricate landscape of cyber threats. In turn, strengthening their capacity to protect their essential work and a more robust defense of their missions.

# CYBER THREATS TO NGOS

## THE CHALLENGE

NGOs are exposed to a wider and more complex range of cyber threats than many organizations due to their involvement in political, governmental, and humanitarian areas. Alongside common cybercriminal activities similar to those encountered by commercial and governmental entities, NGOs are also targeted by nation-states and hacktivists. This combination of threats makes their cybersecurity landscape particularly challenging, requiring heightened vigilance and robust defense strategies.

The challenging cybersecurity landscape for NGOs not only encompasses digital threats but, in some instances, extends beyond the digital realm and

affects NGO personnel or clients in multifaceted ways. The complexity of these threats necessitates a broader discussion on how NGOs can better protect their infrastructure, staff, and constituency. Understanding the complex nature of these threats is essential, particularly in light of NGOs' constrained budgets and finite resources.

NGOs also operate within a context of markedly tighter resource limitations than other sectors, leading to fiscal constraints that hamper organizations' ability to thoroughly monitor and protect their digital environments. These disparities in resource allocation hinder their implementation of vital security best practices and critical protocols.

## THREAT ACTORS

Threat actors do not always target NGOs because they are NGOs. Many actors are purely opportunistic, looking for any vulnerable target rather than focusing on a specific industry. While these actors may not possess the same patience and skill as a nation-state, criminals nevertheless pose a significant risk to NGOs. Criminal actors operate much like any corporate entity, with structures and strategies in place to exploit vulnerabilities. They can disrupt operations and steal the money an NGO needs to achieve its goals.

Meanwhile, by operating in conflict zones or working on issues that some see as provocative, especially when advocating for social or political change, NGOs are also prime targets for nation-state threat actors and hacktivists. Many nation-states see NGOs as a threat, and they utilize open source and private tools as an effective means to spy on or harass NGO personnel, as well as hinder NGO activity. Hacktivists can also target NGOs because they perceive them as "enemies." Therefore, the sensitivity and specific nature of NGO operations render them susceptible to harassment or disruption through malicious cyber activity in a way that many other organizations do not experience.

Additionally, insider threats can pose a concern, involving individuals within an organization who have privileged access to critical systems and can inadvertently or maliciously compromise security.

## INTRUSION METHODS

How do malicious actors gain access to an NGO's digital environment? They use the same tools and techniques as for any organization. The two primary methods of intrusion are (1) social engineering, which involves persuading a human to take an action to open a hole in an organization's security, and (2) exploitation of known vulnerabilities, which are holes or weaknesses in the hardware or software used by the organization. Despite the impression media stories might give, incidents involving exploitation of previously unknown vulnerabilities (often called "zero-days") represent only a small fraction of security breaches (CISA).

# PAIN POINTS FROM THREAT TYPES

Cyber actors targeting NGOs use a wide range of tactics and techniques within the two broad methods cited above, each with its own unique implications and consequences. In the following section, we will explore the top cyber threats in detail, delineating the primary objective behind each category and highlight the vulnerability they exploit in NGO operations.

## PAIN POINT: STEALING MONEY

By virtue of being connected to the internet, NGOs are vulnerable to one of the most common kinds of cyber threats – criminals trying to steal money. The most common techniques for stealing money involve variations of social engineering, including phishing, spear phishing, vishing, smishing, and business email compromise. Additional approaches include fake websites and the gift card scam.

## Social Engineering

Social engineering threats exploit human psychology rather than technological vulnerabilities to gain unauthorized access to information or systems. Among the most common forms are phishing, spear phishing, smishing, and vishing. Phishing involves sending emails with malicious links or attachments under the guise of legitimate sources, targeting a broad audience without much personalization. In NetHope's soon to be published '2024 State of Humanitarian and Development Cybersecurity Report,'nearly 80% of survey respondents experienced phishing in the prior 12 months, making phishing the most common of any threat type to NGOs (NetHope). Spear phishing, a more targeted version of phishing, focuses on individual recipients or specific entities within an organization, deploying well-researched and highly credible threats that often lead to the deployment of malware. In the same '2024 State of Humanitarian and Development Cybersecurity Report,' NetHope's initial findings show that over 60% of survey respondents experienced spear phishing in the prior 12 months, making spear phishing the second most common of any threat type (NetHope). Smishing utilizes SMS text messages to trick recipients into revealing personal information by posing as reputable entities, exploiting the immediacy and personal nature of text messages. Vishing, or voice phishing, involves phone calls where the attacker impersonates a credible authority to solicit personal and financial information, leveraging direct conversation to create a unique pressure that encourages victims to comply without verification.

## Business Email Compromise

Business Email Compromise (BEC) represents a significant threat to the financial stability of NGOs. The goal is to trick employees into making unauthorized money transfers or revealing sensitive information that can be used for financial gain. As the name implies, the threat comes through an email to an employee or staff member. BEC activity is usually highly tailored to the victim organization, with the attacker having done some degree of reconnaissance to deceive the recipient. For example, malicious actors will find out the names of leaders in the organization and their roles, so that they can pretend to be the CEO asking for money to be transferred.

## Fake Websites

Criminals can also target an organization's customers or donors to steal money through fake websites. In this technique, criminals mimic legitimate platforms with a high degree of accuracy. They then use a technique called "search engine optimization" (SEO) to get the fake website to show up higher than the legitimate site in search results. Unsuspecting customers or donors can then be tricked into providing sensitive information or making unauthorized payments. In these cases, the money is diverted before it ever arrives at the donor's intended destination.

*NGOs are often targets of specific BEC scams where cybercriminals exploit the trust and authority of key personnel within the organization. In the Gift Card Scam, perpetrators impersonate a high-ranking individual, like the CEO, and send urgent requests via email or text messages to key employees. The visuals associated with this scam might feature company logos, signature blocks, and language that closely resembles that of the purported official. Thus, the attacker may pose as the CEO, claiming to be in a meeting and urgently request $200 worth of gift cards for a client or employee reward. The sense of urgency and perceived authority of the sender may pressure recipients into complying with the request without questioning its legitimacy, resulting in financial loss for the organization.*

Each method leverages a blend of technological tools and psychological tricks to exploit the innate trust and habitual responses of individuals, often culminating in the theft of money from unsuspecting victims.

## PAIN POINT: ESPIONAGE

Due to the nature of their work, NGOs are subject to nation-states wanting to spy on their activities. Governments may use the collected information for a variety of goals, including arresting NGO personnel, learning about an NGO's sources, clients, or recipients, tarnishing the NGO's reputation, and/or supporting disinformation campaigns or social engineering. While the aforementioned techniques to steal money can also be used for espionage, the most common way that nation-states spy on NGOs is through spyware.

A mobile phone or laptop is the most common device for spyware; however, malicious actors can use other devices as well. Such devices include the vast array of "things" that can now be connected to the Internet, from cameras to appliances to vehicles. Often referred to as the Internet of Things (IoT) devices, these items often contain vulnerabilities that are not commonly addressed, and/or they contain default settings that allow for unauthorized access and surveillance. Further, most organizations are unfamiliar with how many IoT devices are connected to their network and how they are accessible from anywhere on the Internet.

*"The level of sophistication in spyware dwarfs the sophistication of other cybersecurity activities that we see."*

*— Nick Biasini, Cisco Talos*

Spyware ranges from relatively straightforward surveillance tools that can capture keystrokes and browsing history, to highly advanced systems like Pegasus, which can covertly infiltrate smartphones to access messages, calls, and even activate cameras and microphones without the user's knowledge. This technological sophistication highlights the dual nature of spyware: it exists both as a commerical product available for legitimate security purposes and as a mercenary tool used for more clandestine activities.

### Commercial Spyware

Commercial spyware often masquerades as legitimate software, available through common channels such as app stores. It is a type of malicious software designed to access and collect private information from users' devices without their knowledge. Spyware can be particularly dangerous for NGOs, as it can gather sensitive information that could compromise the security and privacy of the organization.

### Mercenary Spyware

Mercenary spyware represents a more targeted and dangerous threat. While commercial spyware is usually disseminated through widespread channels, mercenary spyware is developed and deployed by entities with substantial resources, often for specific espionage purposes against high-value targets, including influential figures within NGOs.

*It is important to note that spyware often occurs in the form of a threat to mobile devices due to the personal nature of the data stored on phones. The threat is more significant for organizations that use personal devices for work-related tasks. Threats targeting mobile platforms present a growing concern for NGOs as these devices become increasingly integral to daily operations and communication. Mobile devices are often perceived as a smaller surface to manipulate compared to traditional computers because they may receive less device management, making them attractive targets to cybercriminals.*

*Signs of infiltration or mobile device compromise include the device overheating, rapid battery drain, and unusual app behavior. A spyware intrusion may start from seemingly innocuous sources, such as accessing an intentionally shortened link, which might be sent by contacts you recognize, whether genuine or spoofed.*

## PAIN POINT: DISINFORMATION

*"An organization's reputation is one of the top assets leaders will try to protect."*

*— Karim Beldjilali, RoundTable*

An organization's reputation is directly linked to stakeholder trust. Without stakeholder trust, NGOs cannot achieve their mission. This relationship explains why an organization's reputation is one of the key assets leaders are tasked with protecting. It also explains why nation-states and hacktivists seeking to hinder an NGO's work try to attack its reputation. From a cybersecurity perspective, these malicious actors can employ disinformation campaigns to spread false information, tarnish reputations, and generate opposition to the NGO and its work. Social engineering techniques are often integrated into disinformation campaigns. The rise of artificial intelligence (AI) and "deepfakes" make this threat even more potent.

### Disinformation Campaigns Coupled with Social Engineering

Disinformation campaigns coupled with social engineering tactics present a multifaceted threat to NGOs, leveraging psychological manipulation and deceptive techniques to exploit human vulnerabilities. These campaigns aim to spread false or misleading information, often with the goal of damaging an organization's reputation, sowing discord among stakeholders, or influencing public opinion. Malicious actors will masquerade as trusted sources and/or leveral emotional appeals to deceive individuals into divulging sensitive information or taking actions detrimental to an organization's interests.

### AI and Deepfake Technology Influencing Disinformation

Although not yet widespread, emerging technologies such as artificial intelligence (AI) are poisted to heighten NGOs' financial vulnerabilities. These advanced tools enable fraudsters to craft highly convincing impersonations and manipulate digital content, posing a significant detection challenge. For instance, "deepfakes" - synthetic media in which a person in an existing image or video is replaced with someone else's likeness using AI - can be particularly damaging. Smaller NGOs might be targeted by localized fraud activity aimed at exploiting specific donor bases, while larger organizations face the risk of broader disinformation campaigns that could jeopardize major funding streams.

## PAIN POINT: DISRUPTING OPERATIONS

### Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money is paid. Ransomware typically encrypts the victim's files or locks the entire system down, rendering it unusable. The attackers then demand a ransom, usually in cryptocurrency, in exchange for providing the decryption key or restoring access to the system. Ransomware attacks can cause significant disruption to individuals, businesses, and organizations, often resulting in financial losses and data breaches.

While this type of attack may sound like it requires significant technical skills to execute, "ransomware-as-a-service" models have emerged over the past few years that enable unskilled actors to carry out such attacks. In this model, different groups work together to carry out ransomware, each specializing in a specific aspect; writing malicious code, gaining access to organizations, or encrypting data. Thereafter, each group receives a share of the eventual payments. The group collaboration enables criminal actors to increase the volume of ransomware, creating greater levels of disruption to organizations.

Notably for NGOs, they face ransomware that is politically motivated, where the threat is not always intended to obtain money, but rather to disrupt critical operations by sabotaging essential voting processes or compromising sensitive data associated

with high-profile events. To inhibit an organization, threat actors have a tactic to not always activate the ransomware immediately. The ransomware can be deployed months after the infiltration, where a threat actor will reside in the network after performing lateral movement, exacerbating the challenge of detection and mitigation.

*"We see about one ransomware attack a month among our Members."*

*— James Eaton-Lee, NetHope*

Ransomware has greater impact when malicious actors apply  "double extortion" tactics. With this extension, actors not only encrypt the victim's data, but also steal and threaten to release the data publicly unless the ransom is paid. This dual-pronged approach amplifies the pressure on organizations to comply with the demands, adding complications of reputtional damage and regulatory scrutiny alongside the disrupted operations. For NGOs, such tactics pose significant threats, as the potential exposure of sensitive information can jeopardize their credibility and the safety of their staff and beneficiaries.

In certain cases, ransomware may escalate into "triple extortion" wherein attackers extend their targets beyond the organization to encompass its network of supporters and end-users. In the context of NGOs, however, this strategy may prove futile, as these entities and their beneficiaries often lack the financial means to meet ransom demands. Consequently, attackers may shift their focus to target those who finance NGOs, such as grant providers, by exploiting their ability to pay, escalating the ripple effect of the ransomware across the ecosystem.

NGOs who have been affected by ransomware are not shielded from future attacks. The same or other ransomware actors could target the NGO in the future. It is possible that during recovery effects, the original threat actor, or other actors, could have undetected access to a network, leading to a subsequent breach. This stark reality calls for a paradigm shift in how NGO leaders perceive post-attack security. It is imperative to abandon any false sense of safety and acknowledge that the first attack could be a precursor to a sustained campaign.

### Denial of Service

Denial of Service (DoS) is a threat that can disrupt essential services and impede operations. DoS involves overwhelming a targeted system with a flood of network traffic, rendering it inaccessible to legitimate users. For NGOs, which often rely on digital platforms to deliver vital services and communicate with stakeholders, the threat of DoS can have significant consequences, with the potential to completely halt operations.

NGOs can also be an unwitting participant in a DoS. Threat actors could gain access to an NGO's IoT device and then make that device part of a "botnet." A botnet is a network of internet-connected devices, each of which has been infected with malware, allowing them to be controlled remotely by a malicious actor without the owner's knowledge. These botnets utilize the combined computing power of many devices to work together and generate the network traffic used in a DoS. When malicious actors use an organization's IoT devices for a DoS, the NGO's technology will reduce performance.

## IMPROVING CYBERSECURITY: A PRACTICAL GUIDE

In the face of these threats, what should an NGO do? The good news is that, while no organization can reduce its cyber risk to zero, NGOs can substantially reduce their risk and enhance their ability to recover if they suffer a cyber incident. Further, these steps do not necessarily involve spending huge amounts of money, deploying lots of complex technology, or impeding workflow. Instead, to better safeguard their essential work, NGOs should start with what we call the cybersecurity fundamentals. These practices are

applicable to almost any organization and reduce your cyber risk, regardless of the threat actors your organization faces. Further, these steps are not all or nothing; even partial implementation will improve an organization's cybersecurity. Once an organization has the fundamentals in place, it can adopt a more comprehensive cybersecurity management framework and begin to implement more complex controls that protect against more sophisticated threats.

> *Between early 2022 and 2024, the CyberPeace Builders with the CyberPeace Institute conducted 148 General Cybersecurity Assessments, involving 108 distinct NGOs, to help nonprofits evaluate their own maturity level and compare to industry standards and peers.*
>
> *The CyberPeace Builders is dedicated to strengthening the cybersecurity posture of NGOs by providing comprehensive assessments, guidance, and support to implement effective security measures. These evaluations revealed that certain controls significantly improved assessment scores.*
>
> *Those controls are marked with a 📍 .*

## THE CYBERSECURITY FUNDAMENTALS

For entities just starting out on their cybersecurity journey, the following four actions will lay the foundation for more advanced work. These actions include:

1. Change the mindset

2. Manage cybersecurity proactively

3. Contract with a managed security service provider

4. Implement five key cybersecurity controls

### Change the Mindset

The first fundamental is to stop treating cybersecurity as a technical luxury. Instead, NGOs should treat cybersecurity as a critical mission enabler to ensure that clients, customers, and recipients receive the appropriate services, that donors have confidence resources will reach intended recipients, and that staff are digitally protected. Adopting a different mindset for cybersecurity changes the way the entire organization engages with the topic for the better.

### Manage Proactively

Once an organization thinks about cybersecurity as a mission enabler, then it needs to start managing it proactively. While this step will become more complex over time, at the beginning it consists of three parts:

1. Adopt general cybersecurity policies: 📍 Security policies are the backbone of an organization's cybersecurity framework, providing clear guidelines and procedures to protect sensitive information and technological assets. Fortunately, organizations do not have to create policies from scratch. Many generic versions are available that can be adapted to an organization's specific circumstances. Such resources are located on the [CTA website](#).

2. Adopt response plans: 📍 At some point, every organization will have a cybersecurity incident, experience a natural disaster, or suffer some disruption in its operations. When such events happen, the organization needs to have plans in place for how to respond. These plans should include an Incident Response Plan, which outlines steps to take in response to a security breach; a Disaster Recovery Plan, detailing procedures for recovering lost data and restoring system functionality after a breach; and a Business Continuity Plan, ensuring that critical business functions can continue during and after a significant disruption. Even though no incident response or disaster recovery effort will

unfold exactly as planned, having a plan enables an organization to respond effectively. As with general cybersecurity policies, sample response plans exist for an NGO to adapt it to its particular circumstances.

3. Conduct regular oversight: Just like with adhering to accounting practices and managing legal liability, cybersecurity is a leadership responsibility. Therefore, NGO leaders should regularly ask questions, receive reports, and make changes as necessary to keep cybersecurity a management focus. Recently, more emphasis has been put on a Board of Directors for oversight of cybersecurity. In light of this trend, we have included the next section to discuss the relationship between executive leadership and the Board and their respective responsibilities.

These policy decisions are not always easy to implement consistently considering the unique operational model of NGOs, especially those that rely heavily on volunteers. The inconsistency in training and commitment levels, alongside the competitive cybersecurity talent market, presents notable challenges to establish effective cybersecurity practices. Nevertheless, overcoming these obstacles is worthwhile. Robust cybersecurity policies can significantly enhance an NGO's credibility, attract more donors, and ultimately contribute to its financial health and sustainability, despite the initial hurdles in talent acquisition and training.

### Contract a Managed Security Service Provider (MSSP)

Few organizations have the ability to provide all of their cybersecurity in-house. With the exception of large enterprises, some portion of the cybersecurity work needs to be outsourced to an MSSP. An MSSP can provide key services, such as monitoring the "dark web" for leaked information about an organization and scanning the organization's website and applications for vulnerabilities . Further, an MSSP can provide firewall and filtering services and keep them up to date.

### Implement Five Key Cybersecurity Controls

*"NGOs need to set up basic standards of security to maintain their operations."*

*— Martin McKeay, Rapid7*

The final step for entities starting out on their cybersecurity journey is to implement five key cybersecurity controls. Different expert groups recommend slightly different cybersecurity measures. The United Kingdom has the cybersecurity essentials, Australia has the essential eight, the Institute for Security and Technology's Blueprint for Ransomware Defense identifies 14 foundational controls, and the Center for Internet Security has its top 20, just as examples. However, five security controls stand out as having a high return on investment and show up in all of the sets above:

- Use a **password** manager: people often struggle to generate their own passwords. They may follow a personal algorithm to create a unique, new password; however, that password can potentially be guessed if previous passwords are known. Yet, asking people to remember long, random, and unique passwords is impossible without help. Password managers solve this struggle. A password manager enables a user to only memorize one complex, unique password. The tool then creates and maintains the passwords for websites and applications, enabling long, random, and unique passwords for each.

- Use more than a password: Referred to as two-factor **authentication** (2FA), the core idea is that the organization needs to use more than just a username and password to verify that someone trying to log in or access an account is who one says one is. Although any form of 2FA is better than none, using a trusted authenticator application rather than SMS for 2FA provides a more secure verification process. For NGOs operating in areas without reliable internet access, a physical security token, like a YubiKey,

offers a viable alternative by providing a tangible second factor of authentication, making accounts significantly harder to compromise. This control should apply to personal devices used to access NGO Information Technology (IT) systems.

- **Update** software automatically: Keeping all software up to date ensures that an organization employs all the latest patches. Since a key threat outside of social engineering is exploiting known vulnerabilities, having the latest software dramatically reduces cyber risk. Cybersecurity is an ongoing effort, and updates are important to help address vulnerabilities that have been uncovered, as well as to provide ongoing maintenance. Therefore, instead of trying to remember to check for updates or ignoring update notifications, enable automatic update installations whenever possible.

- Filter **links**: Make sure that your MSSP employs a tool to filter out as many malicious links as possible. Since social engineering usually involves malicious links, having the ability to filter out known bad links reduces risk. Of course, these filters will not catch all the malicious links, so users must remain wary, but filtering will help.

- Make regular **backups**: Although adversaries may try to corrupt backups or use extortion techniques that do not rely on encrypting data, having robust data backups in place greatly increases organizational resilience to a wide variety of threats. Backups can be done using cloud services or storage devices like external hard drives that are not normally connected to the network or other devices; storing data in an alternative location that is safe and secure provides another layer of protection.

A useful mnemonic for remembering these five controls is to think of them as your friend PAUL B: passwords, authentication, updates, links, and backups.

## ADOPT A MANAGEMENT FRAMEWORK

Once an organization has the fundamentals in place, the challenge is maturing cybersecurity processes and establishing a culture that embraces security. How should an NGO prioritize tasks, assign responsibility, and allocate resources? In other words, it needs a management framework. Fortunately, resources exist to help with this challenge, such as the National Institutes of Standards and Technology's Cybersecurity Framework 2.0. The Framework is not a cookbook of technical controls; rather, it provides a way to think about cybersecurity at an executive level. Other frameworks can provide the necessary scaffolding to manage cybersecurity over the long-term. The one that works best for an organization will depend on its location, size, and resources. The key is to select a framework, implement it over time, and track progress against agreed upon goals. Within this broad range of activities, two are worth highlighting as advanced steps.

### *Security Awareness Training*

Educating users about the dangers of opening or clicking a suspicious email attachment or link will not eliminate a threat, but it will demonstrably reduce the frequency with which it occurs. If users receive suspicious or unexpected messages from someone whom they know, users should directly contact the individual through a different channel to confirm the message (Abrougui). An unsolicited WhatsApp message from a sender whom one does not know is an example of a red flag.

To further equip organizations, leaders with security responsibilities can play a pivotal role by leading workshops focused on ransomware, helping to clarify the signs of an attack and developing strategic responses, including decisions around ransom payment. Such education is vital to prepare the entire organization – from the boardroom to the frontline employees – to recognize and respond to cybersecurity incidents promptly and effectively.

CYBER
THREAT
ALLIANCE

*"Trust but verify by picking up the phone and calling the number after a lookup that it's a valid number to call. If you are suspicious of a message from an individual or organization whom you know, verify with them through a different channel. It is possible the legitimate phone number was spoofed."*

*— Ben Johnson, NGO-ISAC*

### Device Security

All users should maintain up-to-date devices to allow security updates to address potential vulnerabilities. Users should also reboot phones regularly as many spyware applications are designed to persist only until the device is restarted (Abrougui). To enhance device security further, running antivirus scans helps detect and remove any malware that could have slipped through. In extreme cases where a device is compromised, performing a factory reset stands as the most effective method to completely remove all traces of an infection, returning the device to a secure state.
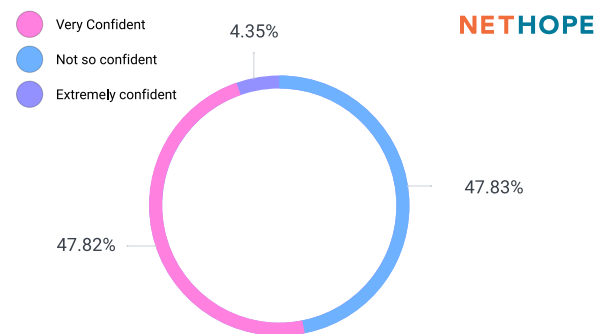
Organizations such as Access Now and Citizen Lab are valuable resources for navigating the complexities of spyware incidents. In the event of a mobile attack, immediate actions include consulting a threat researcher or contacting the State Department if the compromise occurs abroad. One may also place the phone in a secure bag and send it to experts like Citizen Lab for analysis. In this way, NGOs integrate physical security measures with digital safeguards to protect mobile devices and other physical assets.

# EXECUTIVE LEADERSHIP AND BOARD RESPONSBILITIES IN NGO CYBERSECURITY

As noted in the previous section, executive leaders and the Board both play pivotal roles in cybersecurity. However, NGOs with less experience in managing cybersecurity may not be clear on what those roles are and how they differ. Therefore, this section outlines each role's key elements and describes how they complement each other.

NetHope's soon to be published '2024 State of Humanitarian and Development Cybersecurity Report' supports the notion the role of cybersecurity is not clear for many NGOs (NetHope). The survey reveals a distinct division among these organizations, with respondents nearly evenly split between those who are confident in their organization's cybersecurity visibility and management and those who are not.
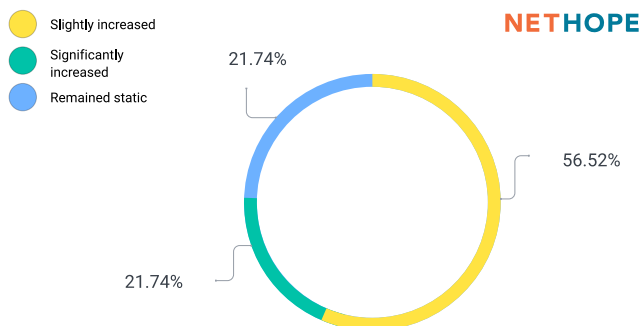
*Are you confident that cybersecurity is a viable and well-managed risk for you?*



On the other hand, this same survey indicates a positive trend in cybersecurity management. 78% of responding organizations reported an improvement in cybersecurity management over the last year, as shown in the next graphic (NetHope). Notably, there was no indication of a decline in cybersecurity quality among the surveyed organizations, implying

a sector-wide recognition of the critical nature of robust cybersecurity practices.

*In the last 12 months, do you feel your organization's program in relation to your organization's needs has:*



- Slightly increased
- Significantly increased
- Remained static

21.74%

56.52%

21.74%

NETHOPE

*"The best way to avoid chaos is to have a culture of security and start early with conversations about how to best prepare for potential incidents."*

— *Runa Sandvik, Granitt*

## BOARD VERSUS EXECUTIVES: WHAT'S THE DIFFERENCE?

The key difference is straightforward to state, although sometimes difficult to implement in practice: Boards oversee cyber risk while executives manage cyber risk (Clinton). Thus, the Board's duty is to ask the right questions, approve the overall level of risk the organization is willing to take on, and hold executives accountable for implementing necessary cybersecurity measures. Boards should not choose cybersecurity solutions or direct specific actions (Clinton).

*"Speaking to the C-Suite is one of the best ways to impact cybersecurity."*

— *Karim Beldjilali, RoundTable*

In contrast, executives should provide the Board with a cyber risk assessment, explain how cybersecurity can support the organization's mission, identify and track appropriate cyber metrics, allocate adequate

resources, and implement the cybersecurity measures provided earlier in this report.

## BOARD-EXECUTIVE INTERACTION

In the for-profit world, and particularly for public companies, there is an ongoing debate about the "right" way for Boards and executives, particularly Chief Information Security Officers (CISOs), to interact. For most NGOs, the specific mode of interaction is less important than the fact that it occurs at all. For example, smaller NGOs might lack a dedicated CISO, and so cybersecurity responsibilities might fall to another executive. Some larger NGOs may choose to have the CISO report directly to the Board, while others might have the CISO report through the executive responsible for overall risk. The key is ensuring that the Board receives the necessary information to make risk-informed decisions and approve budget allocations.

## MAKING RISK DECISIONS

Regardless of size, the necessity for leadership to have candid discussions about risk acceptance is critical. The Board and executives must understand that choosing not to implement certain cybersecurity measures equates to accepting a certain level of risk. Integrating cybersecurity risk into the organization's overall risk calculus is essential. This integration helps it become an integral part of business continuity plans focused on security and vital business operations.

To enable these risk conversations, decisions must be framed in clear, jargon-free language, to ensure all organizational leaders and Board members are considering the same problem and potential actions. A human-centered dialogue around cybersecurity fosters engagement and facilitates comprehension of its fiduciary impacts. Simplification of the topic through clear policies and educational initiatives can demystify cybersecurity, transitioning NGOs from a state of reactive measures to a proactive stance.
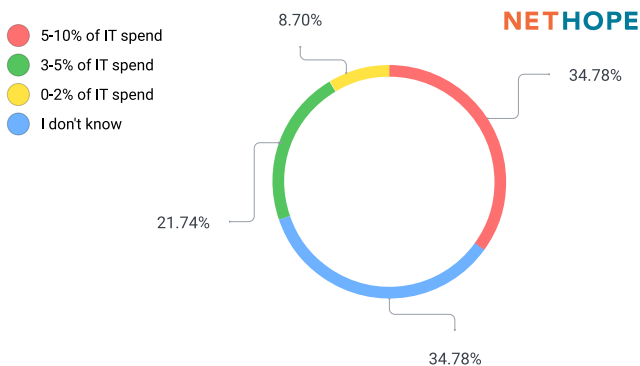
16

*"Running an entity that is cyber secure is more profitable than running organization that is not."*

*— Stéphane Duguin, CEO, CyberPeace Institute*

## APPROVING BUDGET ALLOCATIONS

Once a Board accepts a certain level of cyber risk, executives have to allocate adequate resources to achieve that targeted level. While the specific amount required will differ between organizations, the graph below from NetHope's soon to be published '2024 State of Humanitarian and Development Cybersecurity Report' illustrates the current cybersecurity budget allocations among various organizations. Currently, the majority of organizations invest between 3% to 10% of their IT budget on cybersecurity measures (NetHope). The "right" allocation is the one that allows the organization to accept its desired level of risk.

*What is your cybersecurity budget?*



Legend:
- 5-10% of IT spend
- 3-5% of IT spend
- 0-2% of IT spend
- I don't know

NETHOPE

8.70%
34.78%
21.74%
34.78%

# WORKS CITED

Abrougui, A. Global Trends in Digital Security. Internews, Nov. 2023, internews.org/wp-content/uploads/2023/11/Global-Trends-in-Digital-Security.pdf.

Clinton, Larry. *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue*. Kogan Page, 2022.

CISA, Cybersecurity Advisory AA23-215A: Cybersecurity and Infrastructure Security Agency. "AA23-215A: Cybersecurity Advisory." CISA, 3 Aug. 2023, www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.

NetHope. "NetHope." NetHope, 2024, www.nethope.org. (NetHope, 2024 State of Humanitarian and Development Cybersecurity Report)

# MORE INFORMATION AND RESOURCES

For more information and resources, visit the [CTA website](#).

# CYBER THREATS TO NGOS
# 2024

POWERED BY THE **CTA**