NETHOPE

2023 State of Humanitarian and Development Cybersecurity Report

Making progress, but more investment needed

As nonprofits, we hold personal information about some of the most marginalized and vulnerable people on the planet, and so robust cybersecurity is not 'nice to have'. It is paramount.

No organization is safe from becoming a target, no matter their size, their reputation, or level of preparedness.

In fact, **NGOs and Think Tanks are the second most targeted sector globally for cyber-attacks by nation-state actors,** according to Microsoft, with high-profile attacks on USAID, ICRC, and human rights activists in recent years showing just how sophisticated and targeted cyber-attacks have become.

The information in this report, findings from NetHope's State of Cybersecurity survey, is the only data source of its kind, tracking the progress of the nonprofit sector in this area. For the last two years, we've polled our nonprofit Members on their cybersecurity maturity, tracking the health and preparedness of some of the world's largest and most impactful INGOs.

We believe that the findings shared in this report reflect the state of cybersecurity not only amongst our Members, but among international nonprofits at large. Progress is being made – but it is not nearly fast enough, nor is it thorough enough.

If we are committed to doing no harm to those we work with, nonprofit leaders in concert with their donors and stakeholders need to prioritize investing in cybersecurity, and the ecosystem of contributors, technology partners, and government funders will have to support and enable them to do it. NetHope's nonprofit Members share growing concerns about having the appropriate staff, required levels of accountability, sufficient budget and necessary tools to respond to the scale of the threat. NetHope is making the case to ensure that the nonprofit sector has the skills, people and systems in place to protect and respect the data of those we are all seeking to support and uplift.

NetHope is already working with our over 60 international nonprofit Members in this area – and the insights from this latest survey are informing our response through our Digital Protection Program, as we seek to build capacity, grow funding, broker the right tools and partnerships, and work on enabling mechanisms to allow organizations to collaborate, share and act as part of a unified ecosystem. NetHope is establishing a Global Humanitarian Information Sharing and Analysis Center (ISAC), committed to supporting the increase of cybersecurity intelligence, shared services and tools for the humanitarian sector, in partnership with USAID, Okta and the CyberPeace Institute.

Lance Pierce,
CEO, NetHope

As nonprofits are increasingly threatened in the digital domain, they are increasingly more compromised in their ability to guarantee protection and safety of the data and people they work with. For those seeking a better understanding of what INGOs are wrestling with on the front lines of cyber attack, this report can help you build those insights. The more we all understand the effectiveness and state of play of our current cybersecurity systems, the more likely we will be able to develop shared defenses that will better protect organizations into the future, protect the data they collect on the world's most vulnerable, and help them save more lives in the process.

Contributors

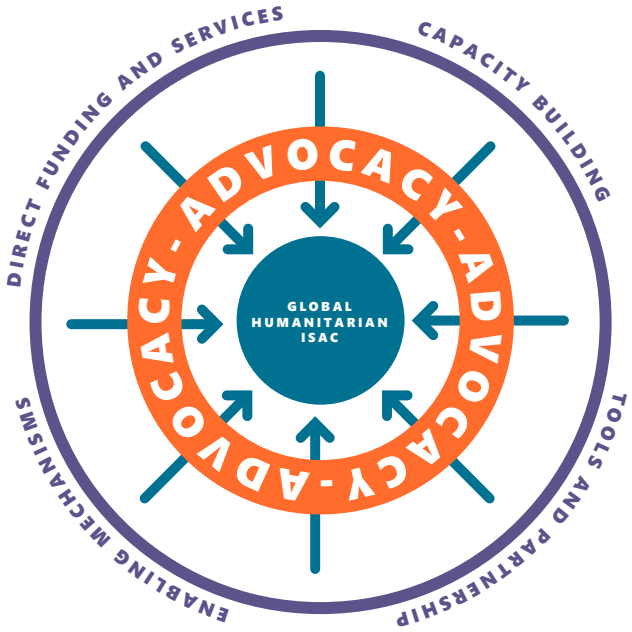
James Eaton-Lee
Chief Information Security Officer

Dianna Langley
Chief Operations Officer

Zarc Okere
Cyber Security Coordinator

NetHope Members

EXECUTIVE SUMMARY
Background



NetHope's Digital Protection Program has four mutually reinforcing components, underpinned by an advocacy program.

2023 State of Humanitarian and Development Cybersecurity Report
NETHOPE

As nonprofits find themselves increasingly at risk of cyber-attacks, NetHope is gathering data to track the health of our nonprofit Members when it comes to cybersecurity. This information can be used identify common shortfalls and catalyze collective action.

The data is gathered through NetHope's 'State of Cybersecurity in Members' survey: an annual survey polling NetHope Members on various aspects of their cybersecurity risk management, ability to consume support, and maturity. In 2022, 36 of NetHope's Members responded to this exercise – representing a little over half of our 60+ Members[1], who collectively make up around 60% of all non-governmental aid spend and serve about 1.7 billion people in 215 countries globally.

This is the second year NetHope has run this exercise. The data is intended to inform Member decision-making, sectoral advocacy, and NetHope's own program work – most notably our Digital Protection Program, a flagship initiative aiming to fill key capacity gaps and execute broader system change to make NGOs safer and more digitally resilient.

[1] https://nethope.org/who-we-are/our-members/

High-Level Conclusions

As global digital transformation of nonprofits forges ahead, so too do the risks associated with our ever-more interconnected and digitized world. Demonstrating this starkly, **in 2022, nearly half of the nonprofit respondents reported they had experienced a security breach in the past 12 months (45%)**. In our concurrent annual survey of Member need, a majority of NetHope Members indicate that cybersecurity and data protection remain priority areas for them in 2023.

This correlates with external data such as Microsoft's 2022 Digital Defense Report, which suggests NGOs are the second most targeted sector by state attackers after government itself. It's also emphasized by real-world examples of disruptive attacks made against nonprofits, such as that targeting ICRC, one of the largest International Humanitarian Actors, which disrupted its programming.

Yet, despite the priority Members claim to give to cybersecurity, data from the State of Cybersecurity 2022 survey suggests that **just 64% of Members have a structured Cybersecurity Program**, with 22% saying that the quality of their program has remained static as compared to the previous year. And while 75% of respondents believe the quality of their cybersecurity has increased either significantly or slightly in the last year, they still lack confidence in their programs.

Asked whether cybersecurity is – overall – a well-managed risk area, 65% of respondents are not (or not at all) confident, while just 11% of Members are 'very confident'.

As other data in the survey suggests, NGOs are low risk and high reward for cyber attackers – an easy target due to limited defensive budgets and low maturity, but relatively high reward because of the funds cybercriminals may be able to access through ransom demands, fraudulent transfers and other threats. Geopolitical motives also make NGOs tempting targets for reasons that go beyond financial motives.

While the impact of a cybersecurity breach can be crippling, it is still an underfunded area in many of our Member organizations. The effectiveness of these initiatives requires a combination of the right tools, processes, and human talent, all of which have financial implications. **Two thirds of respondents reported that their cybersecurity program was underfunded (66%).**

As in 2021, staffing emerges as a key challenge, with NGOs still struggling to recruit, train, equip, and retain the right staff, many of whom also hold other IT-related roles within the organization. 26% of respondents reported that cybersecurity is led by the CIO, and worringly only 10% said it was led by a CISO. The rest responded that leadership fell to less senior roles.

It should be noted that effective cybersecurity (and digital protection) staffing, requires specialism in both the technology but also the specific contexts in which these global nonprofits work. This of course amplifies the shortage of suitable candidates for these senior roles, who must balance risks with the mission delivery imperative of their organizations. For example, hardening the security on your digital infrastructure has well-understood practices for high bandwidth, high digital literacy, high budget resource environments like the private sector. However, few proven practices are similarly found for hardening the digital infrastructure of a food program in Yemen, with high connectivity disruption, many interlinkages between nonprofits necessitating more porous digital boundaries, and vulnerable clients for whom continuity and ease of use of the service is a genuine lifeline.

Thus, having dedicated personnel to oversee cybersecurity is the crucial first step but only half the battle when this risk-balancing must take into account the organization's core mission too. It is vital, therefore, to have these risks and approaches overseen by the Board or Trustees of an organization. **However, a full third or 34% of respondents never (or only reactively) engage their board on cybersecurity.** The majority of the 66% respondents who do report to their boards regularly do so every quarter or more frequently, with 10% reporting only annually on the risks.

Key Takeaways and Recommendations

The body of this report explores key themes emerging from the survey, including *Staffing, Policy and Frameworks, Budgeting, Accountability and Responsibility, Cybersecurity Programs and Risk Management.* The key take homes include:

○ Focus on the basics

Many NGOs still lack basics like Multi-Factor Authentication across all applications, processes for patching, and User Awareness/Phishing Awareness training. NGOs without these basics in place are unlikely to resist even commodity or opportunistic attacks by commercial attackers.

○ Budget for cybersecurity

Senior Leaders, Board Members and Trustees must ensure they right-size budgets based on risk and the experience of their peers and/or comparable sectors. They also need to budget for their own time to engage on the topic and manage the risks well. Cybersecurity budgets should be expected to evolve with the shifting needs of the organization, keeping pace with the internal core operational needs, as well as the changing and contextual risk profile of digitally enabled programing by the nonprofit.

○ Get the governance right

Sound governance with strong leadership is essential to ensure risk management is understood and right-sized. Organizations who are not already regularly reporting to their boards should consider doing this at least biannually and leveraging reporting and mitigation structures from Cybersecurity Frameworks or risk assessments to ensure holistic approaches.

○ Use a framework

Cybersecurity Frameworks provide an off-the-shelf on-ramp to organizations building or iterating a program of works for cybersecurity. If you don't already use one, consider adopting a framework like the CIS Controls Framework, whose Implementation Groups may act as a stop-gap phased approach for organizations who have yet to build a holistic sense of overarching cyber risk. The CIS Framework is the agreed common default by the NetHope Digital Protection and Information Security Working Group as a good entry point. However, it should be noted that it is increasingly common for major institutional donors to request specific frameworks be applied and passed by their grantees, so framework choice may be influenced by those stakeholders, and/or may result in multiple frameworks needing to be reported to.

○ Invest in detection and response

As your program matures and your defenses grow, you will need to embed a continual capability to detect and remediate breaches in systems before they grow. Ensure you are developing the right skills and tools to do this. If your cybersecurity strategy does not include licensing or budgeting for tools such as EDR (Endpoint Detection and Response software), security operations staff, and/or partnerships with Managed Security Service Providers who can help you with this, consider adding this into your roadmap.

○ Share intelligence-led approaches

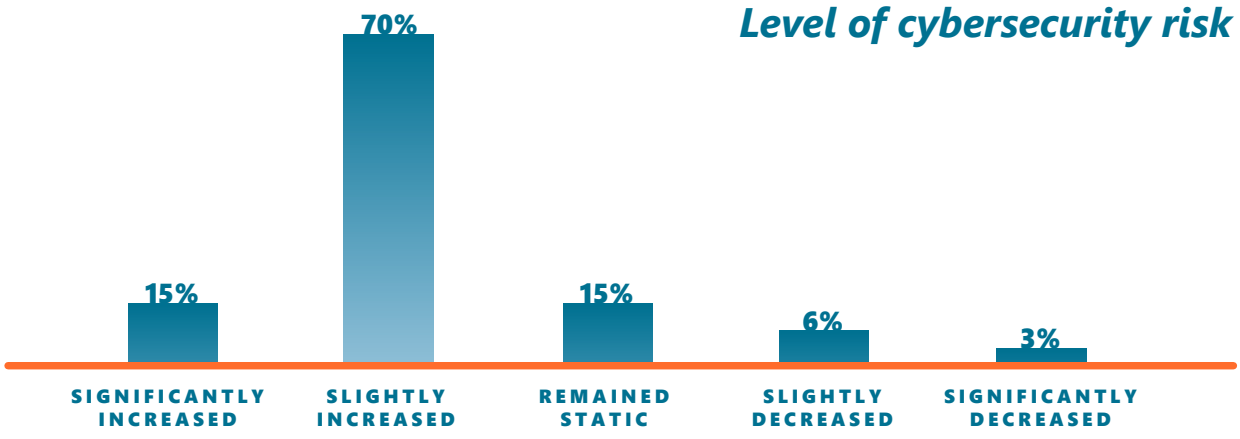
As organizations mature their ability to detect and respond, we become stronger together by sharing what we know and who is targeting us. Community-driven approaches – such as the existing NetHope Digital Protection and Information Security Working Group and NetHope Global Humanitarian ISAC – are key pillars of our approach to tackle this collectively. Make engaging with these a priority for your team if you haven't already.

RESULTS AND DISCUSSIONS
Intro

Cybersecurity remains an important issue within organizations. 75% of the organizations polled expressed concerns that there was an increase in risk compared to the previous year, and 15% indicated that the level of risk remained static. The rest of the organizations polled report a decrease in the level of cyber risk faced, with the decrease mostly attributed to investments made by the Members, such as improving processes, augmenting staff to address cybersecurity threats, conducting regular assessments, improving budget allocations, and employee training amongst others.

> ***"Our risks increased significantly in specific contexts like the ongoing crisis between Ukraine and Russia."***
>
> - NetHope Member

Just under half of the nonprofits surveyed experienced a security breach which impacted their operations in the preceding 12 months, albeit many of the breaches had negligible known effects. Others did not experience any security breaches in the last 12 months, and a much smaller number (6%) were not aware if they experienced any breaches. Some respondents opted not to respond to this question for legal or other reasons.



Over the past 12 months, please indicate the change in cybersecurity risk your organization has faced - i.e the potential for loss, damage, misuse, or destruction of digital assets or data faced by your organization.

1. Staffing

As society relies more heavily on technology to help manage all aspects of our lives, the threat of cybercrime continues to escalate. Research shows that private sector organizations are continuing to increase spending on tools, approaches, and staff to meet this rising tide. As defensive approaches increase in complexity, having qualified personnel to manage complex tools and programs within NGOs has never been more crucial.

A majority of respondents (83%) indicated that they had a senior member of staff responsible for cybersecurity risk management. However, 17% of respondents indicated that they did not have "a sufficiently competent and experienced senior member of staff with designated overall responsibility for cybersecurity", suggesting that a significant proportion of INGOs may have a large leadership or skills gap. This is, however, an improvement on 2021 where 48% of Members responded that they did not have a "sufficiently competent and experienced senior member of staff with designated overall responsibility for cybersecurity".

When asked if they felt they had a sufficiently senior member of staff responsible for cybersecurity, 83% answered yes. However, it should be noted that cybersecurity is a specialist discipline and this is not reflected in these senior roles. In the next question we asked about the role who lead the effort and 52% of the respondents reported that cybersecurity is led by a technology generalist, while 19% reported a cybersecurity specialist holds responsibility for this practice and risk management but these people where not senior role holders. Worryingly, only 10% of survey respondents report a senior post holder (CISO or Senior Director) with cybersecurity expertise and responsibility.

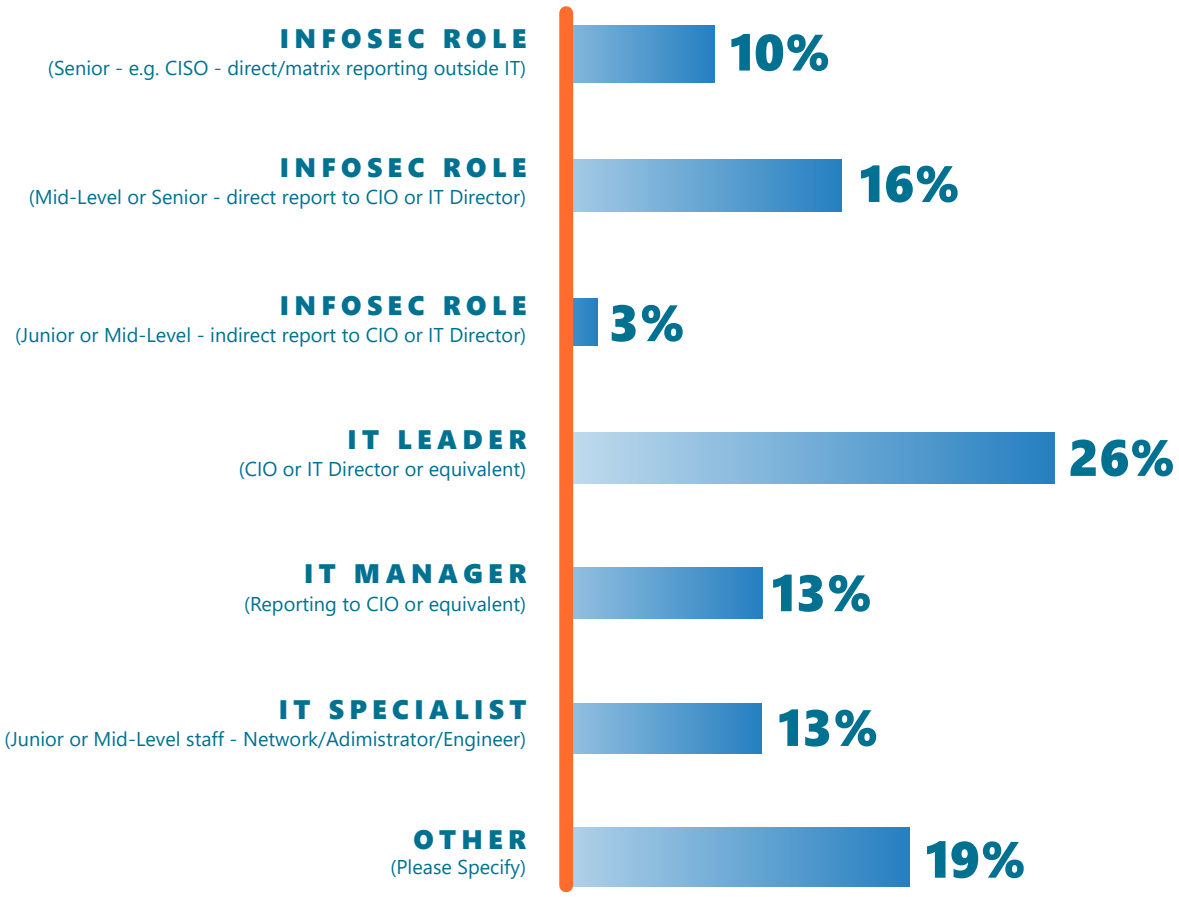
Where Members do not have dedicated staffing, some respondents provided additional reflections – outlining that a lack of budget allocation, support from the board, or a lack of training opportunities hampered their ability to 'hold' responsibility. Where respondents opted to provide more detail, all agreed that there is a need for dedicated cybersecurity resourcing and personnel, with some revealing plans for recruitment, including budget.

"Cybersecurity is a visible but not a well-managed risk for [our organization]. Managing it effectively requires financial investment and more resources and these are two major showstoppers that make it not a well-managed risk for [us]."

– NetHope Member

2. Responsibility and Governance

Responsible for cybersecurity in the organization

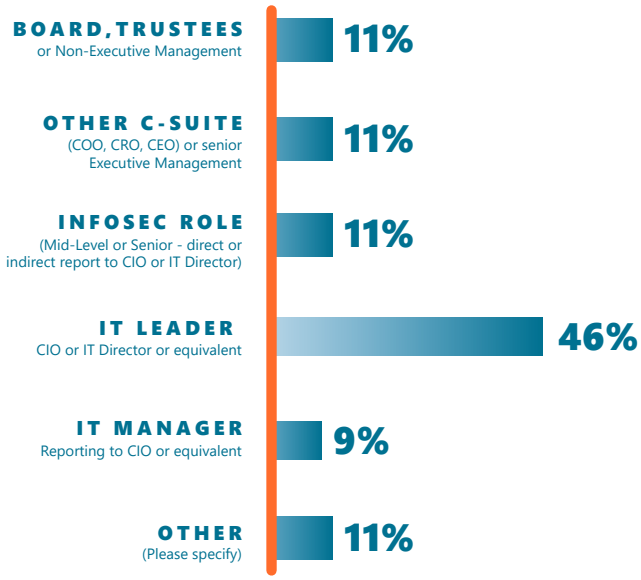


2023 State of Humanitarian and Development Cybersecurity Report NETHOPE

Many organizations try to get by with an IT staff member who also wears a cybersecurity hat – in some instances the CIO. However, some organizations still delegate cybersecurity to junior personnel. Even where a specialist is employed, a lack of senior leadership may result in difficulty executing complex change activity, reporting holistically into senior management, or other failure modes which lead to a low-quality overall program.

Organizations who 'double up' on roles may risk struggling to attract the kind of talent they need to keep up with external threats, and overburdening staff. The range of sub-specialisms within cybersecurity and the broader technology space will inevitably undermine the quality of NGOs' cybersecurity programs if they do not invest in dedicated roles in their teams for cybersecurity responsibility.

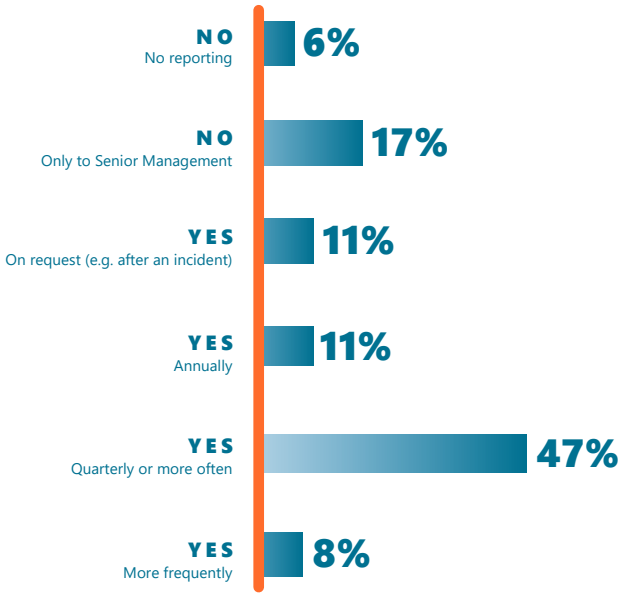
Who is Accountable for Cybersecurity?



2023 State of Humanitarian and Development Cybersecurity Report

NETHOPE

Do you report to the Board?



2023 State of Humanitarian and Development Cybersecurity Report

NETHOPE

2022 saw a significant increase in board reporting and interest on cybersecurity – with many respondents indicating that boards were now being briefed, in some instances monthly.

Nearly all Members polled (77% report on cybersecurity risk to their board – but 11% of these do so only on-demand, for example after an incident. However, around 16% report only to senior or executive management, and 6% don't do any reporting. We did not assess or investigate the qualitative structure of board reporting or comprehension in 2022.

In spite of the fairly high level of reporting, in relatively few instances (11%) the accountability for an organization's cybersecurity approach was regarded as sitting with the board, trustees, or non-executive management.

Within the NetHope network, 26% of the organizations polled indicated that the generalist CIO or IT Director equivalent role was accountable, with a further 26% indicating the accountability fell to a generalist IT role reporting directly or indirectly to the CIO or IT Director. 19% reported that this accountability was held by a specialist infosec role that reported to the CIO or IT Director equivalent, whilst 10% reported a CISO or equivalent role held the accountability and had a reporting line outside of the IT Department. The remaining 19% had more complex reporting lines for the role with this accountability, with less than half of those having a cybersecurity specialism.

3. Budgeting

Budgeting for cybersecurity is challenging, in part because implementing security measures is not a finite task, but rather an ongoing and evolving programmatic workstream which must be linked to organizational business lines, risk appetite, and the behavior of attackers to be effective.

By identifying security costs and assigning budget, organizations minimize the risk of wasted effort and maximize the chances of programmatic success for their cybersecurity initiatives.

In practice, without dedicated budgeting, structured improvements to safeguards such as phishing-resistant MFA, the reduction of attack surface, and the sunsetting of vulnerable legacy technology will be challenging for teams to achieve.

In 2022, 28% of respondents indicate that their organization's cybersecurity budget is fully known and that the budget allocated is adequate for their operations. A further 3% have no idea of their cybersecurity budget allocation, yet they claim that the allocation is adequate – suggesting that only around one third of NetHope Members feel that their cybersecurity spend is adequate even if the budget isn't fully visible to them.
However, 67% of the respondents stated that their cybersecurity budget allocation is not adequate. 56% of respondents know their cybersecurity budget and the other 11% have no idea of the allocation, yet assess it as inadequate, presumably because they feel the lack of staffing, tools and other resources dedicated to cybersecurity.

"The cybersecurity items are mixed in with the IT budget. Generally, it is fine, but we don't break out our budget into projects or much detail. So, it is hard to answer the above since we don't have detailed budgets"

– NetHope Member

While encouraging to note that 84% of the respondents are aware of their budgets, two thirds of NetHope's respondents believe their budget is inadequate.

In addition to the numbers above, a small number of respondents provided further reflections along with their answers. Several indicated that benchmarking spend amongst peers or identifying true cost was hard – with one reflecting that "there are a lot of areas that directly support infosec programs that come from other budgets," suggesting that the NGO "[doesn't] understand its true cost".

It is evident from the feedback that the majority of the Members need more resources – and support in accessing them and assessing what 'adequate' looks like – to ensure that their cybersecurity needs are well addressed.

The general effect of lack of adequate budgets will be felt in other areas like staffing, training and acquisition of tools. Members indicate that they have failed to recruit competent personnel in cybersecurity positions, relying instead on IT Specialists who work as cybersecurity personnel but, in many instances, without additional time or specialist training.

With drive but lack of funding and experience, these staff members may struggle to support their organizations strategically, to benefit their career development, or fund improvement activity. On the other side, organizations that have recruited experts may struggle to retain them due to competitive remuneration from other organizations, or burnout.

To successfully understand and budget for cybersecurity needs, all stakeholders within the organization, especially the Senior Leadership, need to understand the DNA of cybersecurity risk management, build an understanding of the cybersecurity risks their organizations face, and ensure that the activities and resources set aside allow the two to be well-matched.

Outside the risk management programs of individual organizations, the ubiquity of budgetary challenges suggests too that structured work is needed at ecosystem level to establish norms in terms of roles and responsibilities, funding pathways, and to align and benchmark practice.

"We are beginning to map cybersecurity risk at the level of our country programs to force them to take action. But holding them accountable is hard – they have many competing priorities, and it is just my team of non-specialists in IT doing it. Our executive sponsor is great, but our leadership don't understand the problem, and there is no more money to squeeze out of the system. Our donors don't want to pay for it. We do the best we can, but it isn't enough."

– NetHope Member

4. Policy Frameworks and Controls

Cybersecurity Frameworks

Cybersecurity frameworks break good cybersecurity practice into standard terminology and structures to allow consistency in establishing, aligning, measuring, and communicating approaches.

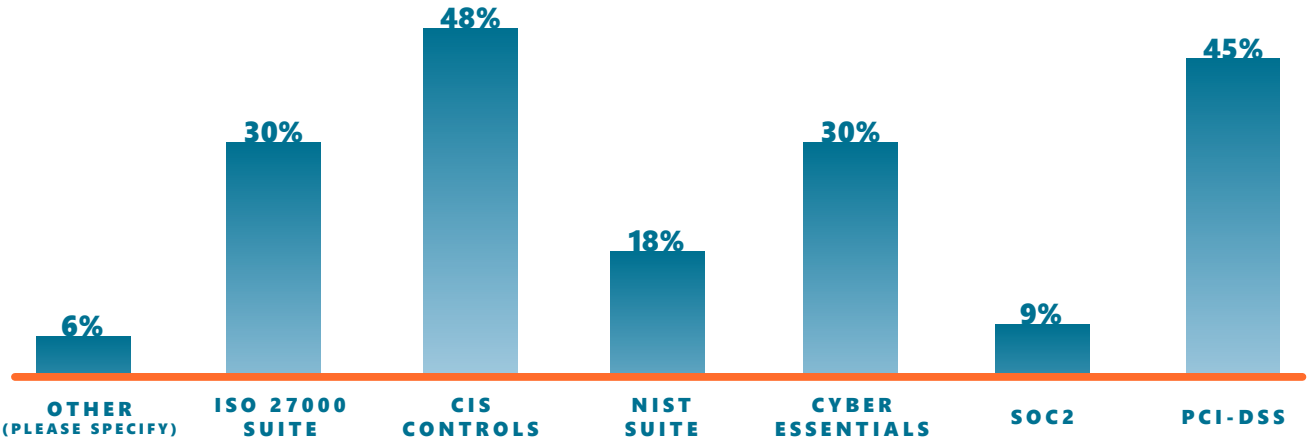
In some sectors, cybersecurity frameworks are mandatory, or at least strongly recommended. There are many national frameworks in existence, and some which are industry-specific.

Among NetHope Members, the CIS Controls Framework – chosen in 2019 by the NetHope Digital Protection and Information Security Working Group as a 'lingua franca' – remains popular, with 48% of the organizations polled using it, followed by the PCI-DSS Framework (linked to card payment acceptance).

Other frameworks mentioned include the ISO 27000 Suite, NIST Suite, SOC2, BSIMM, OWASP Tools, and Cyber Essentials, with some Members in the category using the IRAM2 and Salesforce frameworks. Several Members use frameworks mandated by donors, indicating that while they would to use a framework that is common amongst peers, donor constraints make this difficult for them.

Relatively few Members have not adopted a framework, or indicate a lack of familiarity with cybersecurity frameworks.

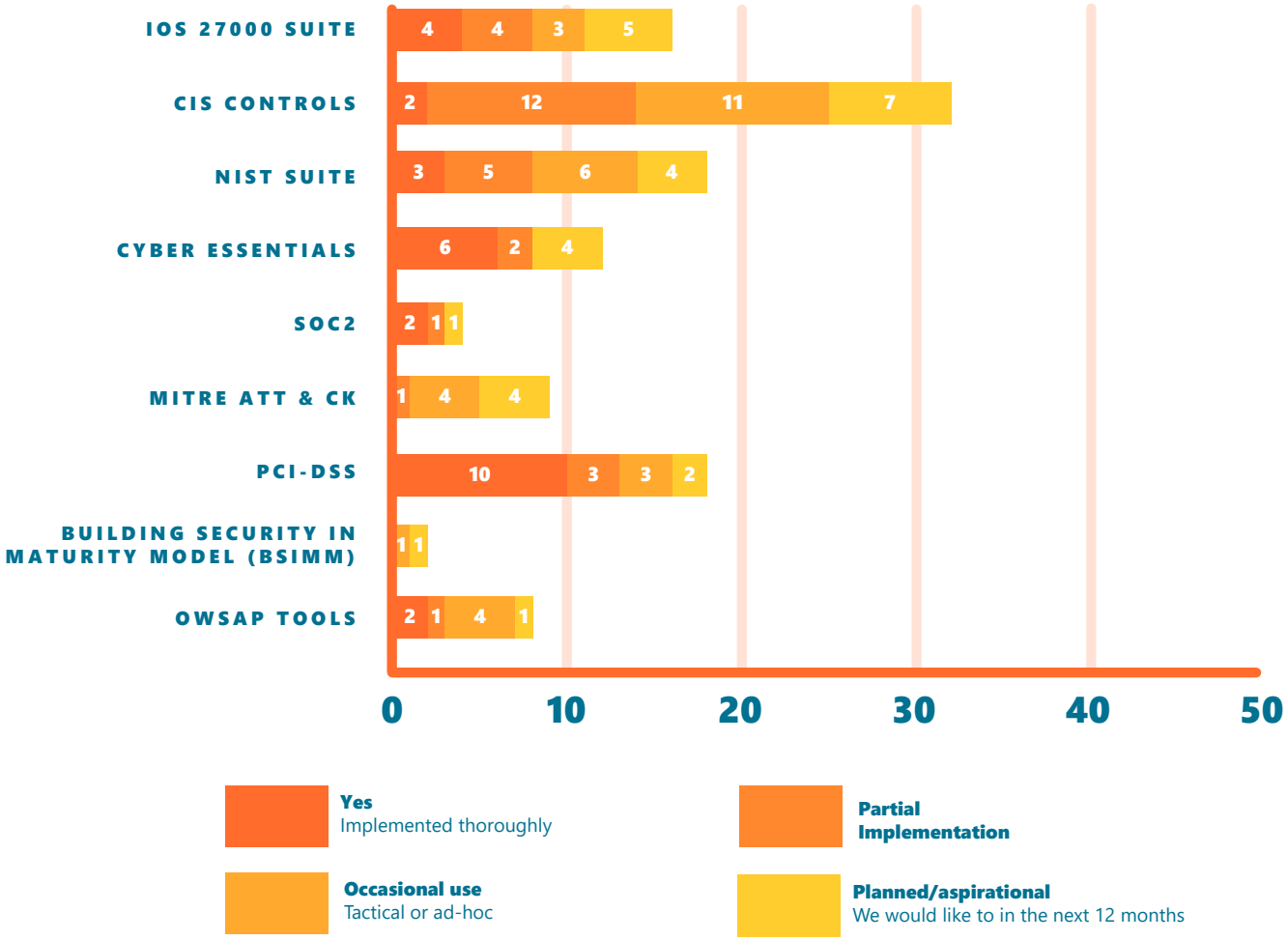
Which of the following frameworks are required or have been introduced within your organization as the result of external requirements (e.g. Donor, Insurer, other Compliance driver)



2023 State of Humanitarian and Development Cybersecurity Report

NETHOPE

Which of the following frameworks have you implemented/are you using?



2023 State of Humanitarian and Development Cybersecurity Report

NETHOPE

After CIS and PCI-DSS (contractually enforced amongst Members who take card payments in fundraising practice), the Cyber Essentials and ISO 27000 Suite appear to be the most common choices amongst NGOs.

While Cyber Essentials has been required by FCDO, the UK Government Funder, for its grantees for several years, the ISO 27000 Suite – an international standard – has been adopted in particular by more mature NGOs with better-developed cybersecurity teams, typically with at least a handful of specialist staff.

Reflection from these Members suggests that few NGOs are completely 'compliant' with the Suite, and formal certification is highly unusual. In practice, many Members using ISO are also using components of other frameworks, for instance leveraging the NIST CSF for board reporting, and potentially achieving Cyber Essentials compliance for programmatic areas which require it.

There does not appear to be alignment between framework adoption and size/revenue. Qualitative data from other areas of the NetHope Digital Protection Program suggests that many smaller NGOs with highly engaged technology teams have adopted frameworks successfully, whilst some larger NGOs have yet to adopt or implement a framework consistently or at all.

In the last year, Members have reflected that a rise in donor pressure to adopt or make use of frameworks through compliance requirements, contractual language or grant agreements can be both helpful and a hindrance. While some Members have successfully used these requirements to lobby for better funding and sponsorship internally, many have reflected anecdotally that a rise in compliance requirements, as well as competing requirements, is increasing overheads and complicating their risk management programs.

Adopting a framework generally requires backing and sponsorship from senior leadership, and dedicated resourcing to project manage implementation, undertake any necessary remediation, and pay for external costs where certifying.

Threat Detection and Response Tools

Amongst the most important tools in targeted organizations are tools for identifying compromised systems and assets, and quickly moving to remediate.

Modern tools leverage cloud data analytics to analyze millions of data points, using data obtained from commercial providers and peers to manage threats, and most mature organizations will use a mixture of Next Generation Anti-Virus (NGAV) or Endpoint Detection and Response (EDR) software installed on workstation as well as other tools that consume network traffic or monitor cloud assets.

Amongst NetHope Members, a majority of respondents (72%) have tools that help to detect and respond to threats, including tools such as the Cisco Meraki stack, Microsoft Defender and Azure Sentinel. However, most of them are still not confident that the tools they use for device management give them the required 100% visibility.

In particular, a little under half (44%) of organizations indicate that they do not have sufficient manpower to use these tools effectively.

> ***"I don't think anyone should ever answer this with a confident yes. So, I put a tentative yes. We have tools in place, but I would not be confident we could detect an intelligent, planned, targeted, and resourced attack."***
>
> **– NetHope Member**

Organizations in the survey that do not have tools to detect and respond to attacks agree that it is really important to have these tools in place, with 92% responding they were very concerned that they didn't.

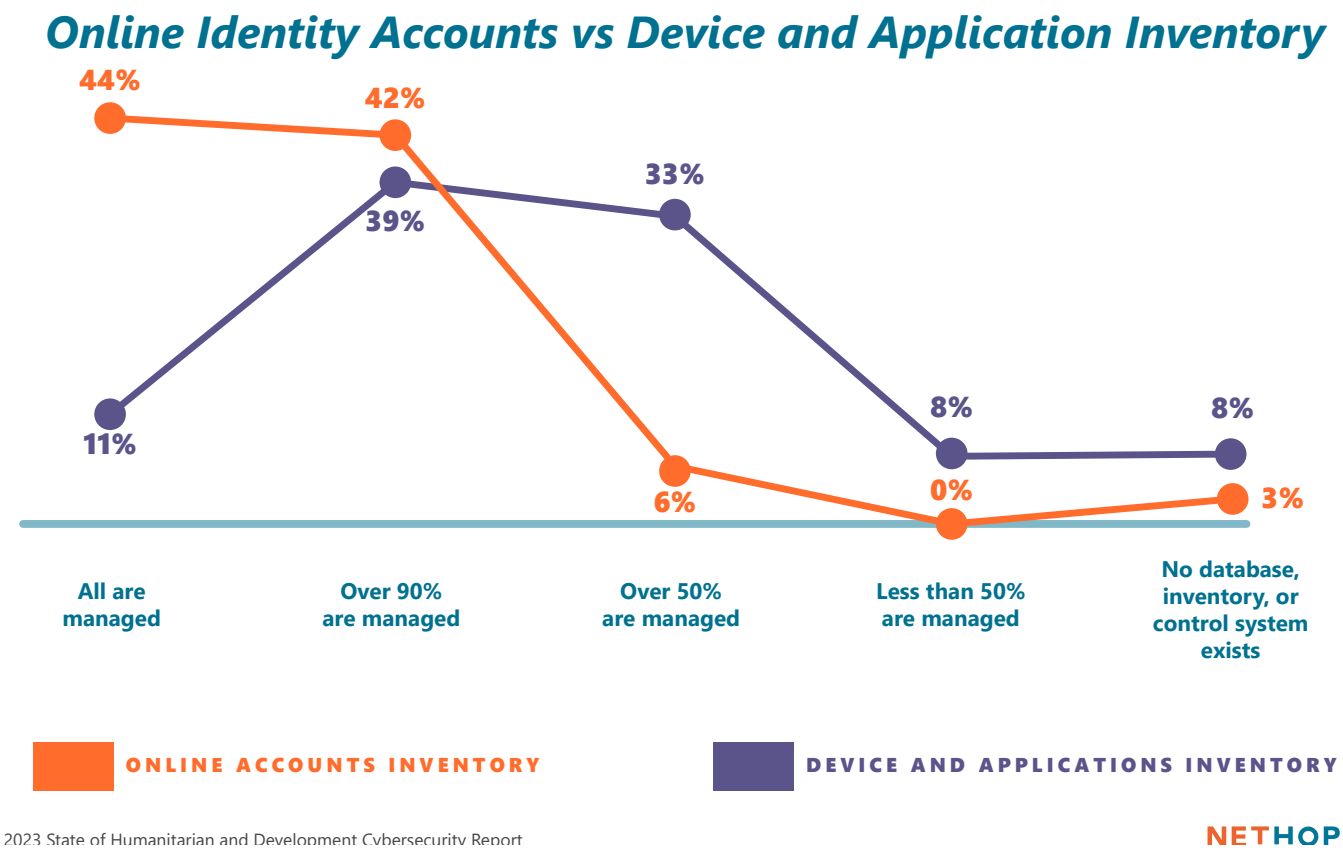
In an age in which humanitarian organizations are routinely targeted by well-resourced state actors at regional and national level, these are concerning capability gaps which can only be resolved with the core funding necessary to invest at scale across the ecosystem.

Asset and Account Management

Inventory management is one of the most crucial aspects of cybersecurity. It provides a solid foundation for risk assessment, incidence response, compliance, and overall asset management. Through user management, organizations can monitor what data and software users can see, how much of it they can see, and whether they have full rights within the software to edit any data. This helps to increase the overall security as it focuses on the 'need to know' basis, which can help simplify deployment processes for new software or technologies.

Within the NetHope network, 44% of Members are confident that they have visibility of all online identities (which is up from 26% in 2021), with a further 42% confident they had over 90% of their identities managed (was 48% in 2021). However, only 11% of the respondents have visibility of all the all devices and applications, with a further 39% responding they have over 90% of their organizations devices and applications managed. In 2021 4% had full visibility, with 41% reporting they had over 90% visibility, a steady increase in the right direction.

While some Members don't have an automated system in place, they are trying to work with what they have, including the use of MS Excel and MS Word. Others are working towards perfecting their systems, but the geographic distribution of their offices pose a challenge. The Members who do not have a system are working to have one in the future and others are fine-tuning what they have to fit their needs.



2023 State of Humanitarian and Development Cybersecurity Report

NETHOPE

The majority of the organizations in the survey have quite low visibility, with only 11% of the organizations having 100% visibility of all their devices and applications. 8% have no inventory system at all.

Another key challenge that emerged in the survey is the management of BYODs. Most of the respondents reported that they did not have the ability to manage the personal devices of their staff and volunteers installed with their corporate applications.

Account Protection and Multi-Factor Authentication

Nearly half (48%) of NetHope Members have all logins covered by Multi-Factor Authentication, making accounts more resistant to common types of attack. Of the remainder, more than a third have 90% coverage, while 6% have only reached 50% coverage. Of Members who have not yet achieved 100% coverage, a majority have a plan in place to achieve full coverage.

These figures are hopeful, reflecting a significant improvement in the last two years. In 2021 only 30% of respondents had all their logins covered by MFA, with 22% responding that they had very little or zero coverage.

5. Cyber Insurance

Cyber insurance policies allow NGOs to externalize some risk, reducing the cost to their reserves to remediate larger incidents and offering assurance to boards and other stakeholders that in the event of a critical incident, business impact is minimized.

While most of them have never been called upon to utilize them, 61% of the survey respondents have bought cyber insurance. 33% of the respondents were uninsured, where 8% plan to acquire insurance while the other 25% of the total respondents do not.

Of these 33%, many cite budget as a key factor behind their decision, with some indicating that they have experienced challenges retaining coverage.

> ***"No plans for insurance, our board's view and our view is that the money is better spent on an incident retainer and that cyber insurance can add to the complexity in responding to a security breach, taking some control away from us to comply with insurance policy clauses"***
>
> **– NetHope Member**

While the insurance market has become markedly more conservative in the last few years, the prevalence of insurance amongst respondents suggests that it remains a preferred option – and attainable – for NGOs who budget and invest appropriately.

Of those who answered yes to having cyber insurance, few were comfortable disclosing the use of those cyber insurance policies, with only about a quarter willing to indicate they made a claim within the last five years, and the remainder declining to respond or providing a negative response.

Methodology

A 30-question survey was created and sent out to the primary contacts of NetHope Member organizations and their broader teams.

Building on 2021's survey, the number of questions was increased based on feedback and informal/anecdotal data from Members.

2022's survey in particular added questions on Members' cyber insurance, assessment of their overall risk, assessment of the improvement in their cybersecurity program quality, cybersecurity leadership, frameworks in use, and various questions allowing evaluation of NetHope's Digital Protection strategy.

Results were analyzed in aggregated form and are presented without a link to specific organizations. Where possible, results have been augmented and contextualized based on learning and reflection from other components of NetHope's Digital Protection Program.

Conclusion

Many more NGOs now have governed, resourced programs which are beginning to consistently apply key controls, mapping their assets, protecting users and accounts or making them more resistant – making those NGOs likely to be more resilient to common forms of attack.

Yet most NGOs remain skeptical regarding their overall resilience. Few are comfortable that their programs are well-funded, and there remain significant gaps to be filled before the ecosystem as a whole is characterized by cybersecurity programs that match regulated or mature industries. This year, we present the following key reflections for INGOs:

Overall Program and Governance

NGOs should ensure they have a trained or experienced senior member of staff who holds overall responsibility for a cybersecurity program of work – both at a technical level, but also as an overall program with appropriate discussions into executive and non-executive management teams regarding risks.

The interface with those structures should be mutually understood, with a defined reporting cadence, and should ideally include key metrics. Many organizations find they benefit from a 'named' trustee or non-executive whose portfolio includes cybersecurity and has a specific brief to retain a weather eye on their organization's posture.

Management of cybersecurity must not just 'live on the risk register', but must be a managed program with specific objectives – for instance, addressing technical debt, executing a risk treatment plan, aligning with a framework, or implementing specific controls which the organization is missing. Senior technology leaders who do not know what their organization's cybersecurity strategy is must familiarize themselves with it, or – if nonexistent – are well-advised to explore objectives along these lines.

Cybersecurity Frameworks

For almost all NGOs, a cybersecurity framework will be the right way to bring structure to a cybersecurity program, and in many instances one will be required by external factors such as donor pressure or compliance obligations.

This year, many more NGOs are implementing the CIS Framework, but there also appears to be more diversification due to these donor requirments, with increasing numbers of NGOs anecdotally reporting adoption of NIST, Cyber Essentials, and other frameworks.

For NGOs, the data suggests that CIS, followed by Cyber Essentials and the ISO Suite, are likely the 'right' choice where a framework has not been adopted already. NGOs who are not already utilizing a framework to manage their

internal program and align with boards and donors should strongly consider adopting one in 2023.

For Donors, this data suggests that further alignment activity amongst donors is important to avoid fragmentation that hurts the NGOs. We are already seeing multiple compliance frameworks required for multi-donor grants or programs, and ultimately resource wastage as nonprofits institute multiple models for assessments of their cybersecurity. We urge caution particularly within Institutional Donors who may be tempted to introduce more national frameworks into their grant chains, particularly where the burden of compliance may 'freeze out' some NGOs, notably more local implementing partner NGOs.

Technical Controls

Below the level of NGOs' overall management, data this year points towards a significant increase in the number of NGOs embedding MFA and Identity Management, as well as the quality of asset management.

Yet a significant number of NGOs report gaps in both technology and people capacity for detection and response, lacking Endpoint Detection and Response (EDR) tools. These tools aggregate and analyze data which may enable detection and investigation of breaches such as Security Incident and Event Management (SIEM) tools, etc.

For NGOs who do not already have basics such as asset management and MFA in place, the data strongly suggests they should regard themselves as falling 'behind the curve', with at least one respondent pointing towards challenges retaining insurance as a result.

Yet the fact that MFA now appears to be a 'basic' – shifting rapidly from the 'top-up' rollouts many NGOs are still undertaking of a technology often still perceived by users and technology teams as 'new' – reflects the speed with which cybersecurity moves.

Against a backdrop of increasing digital hostility, both in conflict-affected humanitarian response environments and the explicit targeting of NGOs, this acceleration will continue.

This year, the lack of detection and response technology and the staff to manage them remains a stark gap. These are vital to set up a speedy lifecycle working across cloud, mobile, and personal computing assets which detects, closes down, and is capable of analyzing breaches and intrusions as attacks mount and keep increasing in technical sophistication.

Next Steps

While we hope these takeaways and conclusions are useful to INGOs negotiating the role of digital in our increasingly hostile virtual world, as implementing organizations they can only undertake work they are funded to do in ways that are compatible with the wishes of their public and private funders.

NetHope recognizes that the deficit in digital protection and cybersecurity capabilities of these nonprofits is caused by a complex and interwoven set of factors, and thus we have developed our multi-part approach to address these systemic issues to positively influence the pace, sequence, cost, and impact of future cyber investments across the nonprofit sector.

This rise in cyberthreats and their risks can not be tackled by any one organization alone, or even with bilateral agreements. Instead this problem requires private sector, public sector and nonprofits join together in concert, facilitated by a shared platform that fosters collaboration, and curates threat information, mitigations and training so we can find success together.
The NetHope Global Humanitarian Information Sharing and Analysis Center (GH ISAC) is that shared platform.

A Time for Transformational Change
We face an unprecedented moment. The GH ISAC is a historic and comprehensive initiative that needs transformational investment to dramatically scale up to impact and protect the nonprofit sector when it needs it most. We anticipate the overall cost of this program for the needed and sustainable transformative change will be USD$7 Million over five years.

We appreciate your interest in this initiative and recognition of the importance of cybersecurity for the nonprofit sector.

The GH ISAC ensures that nonprofits can continue their missions – helping people who are most vulnerable, supporting communities and countries as they seek peace, and protecting the planet for the good of all. With your support, together, we are confident we can uplift nonprofit cybersecurity resilience.