Forging Careers in Human Rights Information Security Today

A network survey of sustainability challenges and opportunities for information security practitioners in the human rights sector

Aspiration, 2973 16th Street, Suite 300, San Francisco, CA 94103
Phone: (415) 839-6456 • info@aspirationtech.org • aspirationtech.org

Table of Contents

Introduction

Aspiration has worked with and in support of information security trainers and capacity builders in the human rights sector for over a decade.

We have witnessed the growth of these communities of practice from local to international levels, appreciating the opportunity to observe how the outcomes of the work of hundreds of practitioners worldwide have had a critical impact on the security, sustainability and efficiency of human rights organizations and individual activists.

With the goal of more deeply understanding the context in which they currently operate, we spent the past 6 months conducting a small-scale survey of a selected information security practitioners. All participants are credited in the following section of this document.

Our investigation aimed to engage individuals whose work represents different facets of the information security services provided to human rights organizations.

Our hope was to achieve a clearer understanding of what resources exist in support of their work, and what challenges and gaps hinder their practice and impact the contributions they are able to provide to the field.

This report summarizes our exploration and our corresponding findings, structured in the following sections:

- A survey overview, including information about the observations that inspired our survey, and the goals and reach of our exploration;
- A summary of findings, outlining the key challenges and needs highlighted by practitioners during our dialogs;
- A selection of learnings organized by thematic area, articulating in further detail the existing and missing resources in support of different aspects of practitioners' daily work, from raising funds, to managing their business operations, to keeping their knowledge up to date;
- Conclusions and thoughts on potential follow up initiatives;
- An appendix, sharing the questions used as a baseline for our discussions with the interviewed practitioners.

Participants and credits

The following is the complete list of interviewees, in alphabetical order. Their name and affiliation are published with their permission.

- Abir Ghattas, Information Security Technologist, Human Rights Watch
- Amanda Hickman, Factful/ Security Training in the Newsroom editor
- Azeenarh Mohammed, Information Security Trainer
- Cheekay Cinco, Freelance Trainer and Facilitator
- Mario Felaco, Digital Security Trainer/ Director of Con-nexo
- Maya Richman, Engine Room/ Astraea Lesbian Foundation for Justice
- Martin Shelton, User Researcher
- Natasha Msonza, Co-founder of Digital Society of Zimbabwe
- Norman Shamas, Information Security and Privacy Specialist
- Sarah Aoun, Information Security Trainer
- Szeming, Open Technology Fund Digital Integrity Fellow

A particular thank you goes to Ali Ravi, Confabium, for contributing his feedback on this report and the potential efforts that could strengthen the sustainability of the practitioner community and those who they support.

Survey overview

Our survey aimed to get a clearer picture of the systemic infrastructure within which information security trainers and capacity builders work today.

Research was structured around consultations with practitioners supporting human rights organizations, in different professional roles, circumstances and contexts.

The investigation focused on identifying existing resources and frameworks designed to sustain their operations, as well as the systemic challenges and gaps that they experience and deem critical to address.

Context and goals

Information security trainers and technology capacity builders who support human rights organizations constitute a broad and multifaceted stakeholder group within the human rights technology ecosystem.

Their profession requires uniquely interdisciplinary abilities, from technical literacy, to educational training, pedagogical knowledge, facilitation practice, well developed interpersonal skills, and a deep understanding of social, political and economic contexts.

They help human rights workers to build security culture in their organizations, and acquire the knowledge and confidence to take control of the technology they decide to use. They aim to provide them with tools to operate sustainably, and with practices that will fortify their stakeholders' rights and safety.

What we can observe today is the striking growth of this community and its impact on the sector over the past decade.

Thanks to the increasing numbers of capacity building endeavors and available trainings, information security culture and technical literacy have become part of the daily work of human rights organizations worldwide as never before.

Several networks of practitioners coordinate collective efforts to improve educational and training methodologies and resources.

The creation and cultivation of in-person and online spaces for security practitioners to meet and interact has helped them to build and strengthen trust relationships, and has provided channels through which to share knowledge and skills, and most importantly support one another.

Collaboration between security practitioners and technology developers and designers has helped bring to the forefront the criticality of technology usability, localization and accessibility.

Funders and resource providers are increasingly paying attention to their work, and exploring different forms of support to address their needs, such as project-based grants, fellowship programs, and travel stipends.

However, security practitioners still encounter numerous challenges in their work, and a number of gaps can be identified in the professional infrastructure which, if addressed, could better contribute to their sustainability and the growth of their communities of practice.

With the global rise of security threats to human rights organizations and those who support them, the need for more robust infrastructure designed to protect and sustain security practitioners has only become more critical.

All of these factors motivated us to learn more about their work, to acquire a clearer understanding of the infrastructure and resources that exist in support of their practice, and to take stock of the struggles and gaps holding them back in terms of both scale and sustainability.

To these ends, we engaged a limited group of practitioners, and documented the key findings from our discussions.

Scope of engagement

The interviewed practitioners have lived and worked as security trainers and capacity builders in Europe, the Middle East, Southeast Asia, Southern Africa, West Africa, Latin America and North America.

The interviews were conducted in English.

Due to the limited resources and time available to conduct this investigation, we were not able to include a broader demographic representation.

This survey does not aim to provide a comprehensive overview. However, we believe our findings may constitute a helpful contribution to deeper analyses of the human rights ecosystem and its sustainability.

Summary of findings

The accounts shared during practitioner interviews allowed us to snapshot some of the key strengths and shortcomings of the sectoral and operational infrastructure within which security trainers and capacity builders operate today.

Collaboration and cooperation are the backbone of these communities of practice, and fuel the co-creation and cultivation of peer learning spaces, training curricula, trainer resources, and mentorship paths.

Funders and resource providers are focused like never before on supporting this growing network of practitioners, and are in an ongoing dialog with them to best tailor their offer to the demand.

At the same time, we also recognize the fragility and transitoriness of several factors affecting the professional context of information security professionals.

Our interviews outline several gaps in what should ideally be provided via infrastructure designed to strengthen their sustainability and impact. The following is a brief summary of the needs that most resonated from the interviews.

- New and varied professional development efforts, focusing on a wider use of Training of Trainers (ToT) methodologies and resources, spaces to engage in peer-to-peer knowledge and skill sharing, long-term inter-generational mentoring relationships.

  Fellowship and mentorship programs are deemed extremely helpful by practitioners eager to strengthen their capacity, but their availability is currently very limited and their formats not always fine-tuned to the community's needs.

  Broader and sustainable infrastructure designed to enable knowledge and skill sharing opportunities would provide the sector with more skilled practitioners, paths for newcomers to learn a new practice, and opportunities for experienced practitioners who want transition from a user-training to a peer-mentoring role.

  It is also essential that those funding security trainings and capacity building activities understand that these professional development activities be included in costing models.

- Support of operational development and sustainability for security practitioners working independently or in small nonprofits.

  These specific types of professionals, who do not benefit from working for a larger well-resourced organization, face several challenges with sustaining their small enterprises.

  They need support from advisors who would help them design business sustainability strategies and costing models, along with resourcing to leverage their services accordingly.

  They also highlight the need for funds to cover for essential items such as bank accounts, web hosting services, Internet connection which, depending on the offering in the region where they operate, can reach prohibitive prices. Most current funding and costing models do not allow for adequate “overhead” or acknowledgement of these indirect costs.

  In absence of this support, independent practitioners find themselves in the position of needing to leave their human rights security practices in favor of more sustainable careers in the for-profit sector.

- Operational “back office” business skills and corresponding consultancy services supporting business management tasks like accounting, fundraising and grant writing.

  Most practitioners are concerned about these tasks, which they often have to learn from scratch and by themselves, and are also very time consuming.

Several interviewees outlined the demand for support with accounting and fundraising, ideally provided by consultants who know the sector and are able to strategically understand the nature of their job.

- Well-resourced paths concerning practitioner health and safety, including insurance models for different kinds of threats, depending on the nature of the service provided and the context in which an individual operates, and health care resources to recover from mental or physical trauma incurred on the job.

  Cases of aggression, detention and incarceration of information security practitioners due to the nature of their work are increasing worldwide. Financial, legal, operational and mental health infrastructure that could help to handle these cases is not yet developed as needed.

  Among the key resources that are most urgently needed:

  - Insurance programs covering practitioners who are required to travel in regions where they could be exposed to danger;
  - A rapid response system designed to intervene in cases of emergency with financial, legal and medical support;
  - After-care funds to cover means of sustenance and recovery costs.

- Financial support over extended periods of time for long-term capacity building initiatives in support of human rights organizations.

  All the interviewed practitioners agree on the critical importance for capacity builders to work with organizations over extended periods of time, in order to ensure the actual shift of culture and and retention of habits required by new security-enhancing processes and workflows.

  On one hand, most existing funding opportunities underwrite at most single years of organizational security support. On the other hand, practitioners state that a minimum of three months is required just to agree with their trainees on their engagement plan, and that one year is never long enough for an organization to be ready to take care of their information security independently.

  Funding and initiatives designed for practitioners to accompany organizations over extended periods of time would allow both trainers and trainees to engage in much more impactful and sustainable paths, while also ideally helping to mitigate the de facto “hard-to-mouth” cycles of project-based funding.

- Trustworthy aggregators of information about emerging technology and security threats.

  Security practitioners supporting human rights organizations operate in contexts which are affected by developments of social, political and economical nature. Furthermore, the rapidity with which emerging technologies and security threats constantly change is a key concern.

  Keeping up with emerging threats and harm reduction measures requires more time than practitioners have at their disposal to stay current. The emergence of one or more curated aggregators of reliable information security news would be deemed as an extremely helpful resource by several interviewees.

- Intermediary initiatives or organizations with the mandate to drive long-term efforts dedicated to strengthening the sustainability and strategic development of the information security ecosystem.

  The interviewed practitioners wish there could be one or more organizations or initiatives dedicated to supporting their community through a range of offerings. Among the services proposed:

  - Cross-sector analysis designed to assess their needs and envision improvement opportunities;
  - Co-creation and management of knowledge sharing spaces;
  - Facilitation of collaborative development of resources;
  - Development and oversight of professional development frameworks, offerings and infrastructure.

We consider these findings a work in progress, and welcome dialog and feedback on any and all of these topics.

Selected learnings by thematic area

This section of the report provides an overview of key learnings that emerged from our interviews, organized by thematic area.

Prioritizing professional development

Different forms of fellowship and mentorship models provide the international communities of security trainers and capacity builders with opportunities to develop new skills and knowledge.

The interviewed practitioners see these programs as extremely helpful in strengthening the career paths of mentees, the profile of the experienced practitioners who get a chance to serve in mentoring roles, and the community as a whole.

But these opportunities are not numerous, thus making the application processes extremely competitive, and the positive effect of these mentorship initiatives not easy to scale.

Furthermore, the interviewees call for new and different professional development efforts, focusing on a wider use of Training of Trainers (ToT) methodologies and resources, and long-term inter-generational mentorship relationships.

Mentioned professional development initiatives

The following is a summary of initiatives related to professional development for information security trainers and capacity builders which were mentioned during the interviews.

These programs all have different formats, targets and goals, but were all generally deemed as relevant to our exploration. Note that some of these, although known by interviewees through past experiences, may not be currently active.

- Digital Integrity Fellowship, Hivos

  https://www.digitaldefenders.org/sections/about-us/fellowship-2/
- Digital Integrity Fellowship, Open Technology Fund (OTF)

  https://www.opentech.fund/fellowships/difp
- Open Web Fellows Program, Ford Foundation and Mozilla

  https://advocacy.mozilla.org/en-US/open-web-fellows/overview
- Training of Trainers (ToT) camps, Front Line Defenders

  https://www.frontlinedefenders.org/
- The Information Safety & Capacity (ISC) Project

  https://iscproject.org/request-on-site-training-test/
- OpenNews Fellowship, Knight Foundation and Mozilla

  https://opennews.org/what/fellowships/

Overall, all these initiatives are considered to be positive efforts, and have in principle the potential to strengthen a practitioner's career path.

However, some of the formats they follow do not seem to be yet in tune with the needs of the information security practitioner community and could be further improved.

For example, initiatives designed for fellows to be embedded in an organization as staff for a set number of months can on occasion lack “smooth landing” opportunities to receive mentorship and/or help with post-fellowship job searches.

Programs which support an independent practitioner to help different organizations with improving their security culture are often set to last for lengths of time that are considered too short. The duration of the funded engagement is frequently insufficient to allow for the accompaniment of an organization through to an effective shift in their security culture.

Professional development opportunities envisioned by practitioners

All interviewees expressed the need for more accessible, structured, replicable forms of professional development support. The following are the two key proposals emerging from our discussions.

- The creation of a professional development pathways supporting:
    - Individuals who want to become information security trainers and capacity builders for human rights organizations, and who are taking their first steps into the new profession;
    - Practitioners already working as trainers and capacity builders who want to build a network of trusted peers to share knowledge and skills;
    - Experienced security practitioners who want to transition from trainer positions to a mentoring role.

  The key components that interviewees deemed necessary to support these types of objectives were the following:

    - Creation of mentoring programs which enable practitioners who are new to the profession or to a specific service offering to:
        - Shadow a more experienced peer;
        - Lead their first sessions under their mentor's supervision, ideally in a testing environment;
        - Gradually start to work independently while still being able to communicate and collaborate with their mentor for further guidance.
    - Creation and facilitation of regular Training of Trainers (ToT) in person events. Different events would be held for practitioners of different levels of experience.
    - Production of Training of Trainers (ToT) resources.
- The provisioning of initiatives and grants to support practitioners who seek ad hoc trainings and courses, to improve their technical knowledge and proficiency.

Fostering business development and strategy

Security trainers and capacity builders operating in the human rights field, especially when working independently or in small nonprofits, are weighed down by the lack of infrastructure to help them build and manage their businesses.

They express the need for support both at a strategic and tactical level.

At a strategic level, practitioners wish to receive guidance on how to best navigate the nonprofit sector, and find a balance between service innovation and business sustainability.

Practitioners who start working on their own for the first time, seek advice on how to best design and present their offering. Others may decide to turn long-time collaborations with peers into new endeavors, and look for advice on how to build a sustainable organization.

At a tactical level, interviewees would welcome help with “back office” and operational management tasks which are time consuming to the point of interfering with the delivery of their services.

Tasks which are considered particularly challenging include submitting grant applications which require exceptionally thorough documentation, writing project reports, and accounting.

In regards to grant and report writing, practitioners wish funders would consider improving the requirements and formats which constitute their submission processes. Preferably, grant proposals and reports would be more straightforward to produce, and qualitative data and approaches would be given relevance at least equal to quantitative ones.

In regards to accounting, when a practitioner works independently or runs a small organization which cannot afford to hire an operations manager, the amount of time required to take care of accounts and tax declarations is often deemed disproportionate. Issues of cash flow management and revenue projecting are also extant.

This issue is particularly burdensome, especially considering that those who become responsible for these tasks are often totally new to them, and struggle to teach themselves new professional skills while simultaneously holding a full time job.

Interviewees wish they could receive the support of consultants or advisors to help them establish and practice administrative tasks.

The following is a summary of more specific findings emerged from the interviews.

Sustainability

- It is not uncommon for individuals who work as independent security trainers and technology capacity builders to struggle to sustain themselves with what they earn from this profession.

  In this case, they often have an additional for-profit job, for example conducting security assessments or working as IT security professionals for corporations or banks.

  Those who have an additional corporate job on the side, and who would rather work exclusively in the human rights sector, seek advice and guidance on how to build a sustainable independent business in this field.

- A growing number of practitioners express interest in establishing their own organization and seek advice on how to build a sustainable nonprofit or small- or medium-sized business. Among the most common needs raised in this regard:

  - Learning project management methodologies, to handle both individual and team efforts;
  - Understanding how to seek funding opportunities;

  - Knowing best practices to be followed when applying for a grant with a proposal involving multiple organizations;
  - Managing a distributed team;
  - For nonprofits, building and managing a supportive Board of Directors as well as best practices for incorporation and compliance.

We observe that many of these resources do exist, but are not packaged or aggregated in ready-to-consume formats for these types of pracitioners

Operations management

Practitioners who work independently, or who have acquired these responsibilities within their organization due to limited human resources, would very much welcome support with operations management.

The following are tasks with which it would be most beneficial to receive help:

- Managing contracts with staffers, consultants, vendors, especially for distributed teams of remote workers responding to different countries' legislations;
- Managing web hosting services;
- Accounting;
- Tax filing.

Fundraising and proposal writing

Fundraising is a very time consuming and arduous task, and is also an absolute necessity.

Interviewees assert that the funding opportunities in support of organizational security and capacity building are still few and far between.

Also, funders and resource providers seem to support mostly short-term projects, thus requiring a practitioner who wants this to be their only job to be constantly occupied by project proposals and grant writing tasks.

The requirements for submitting proposals are deemed cumbersome, sometimes overly demanding, and often disproportioned to the time that practitioners can dedicate to what is ultimately an unpaid task with limited hope of success.

Report writing

Most interviewees find the task of project report writing particularly time consuming, and often ruled by requirements that do not seem to be the most relevant for documenting the work done.

They wish there could be different ways to report on their work which do not require them to spend several hours writing a description of the work done. They also wonder if different types of media could be used instead of text, such as audio or video.

Furthermore, they would like to have more room to decide how different types of projects could be documented with different forms of reports.

Trainers and capacity builders are frequently asked to produce quantitative reports, and identify measurable short-term success criteria. This can constitute relevant information for some projects, but not for all. This is especially true when real impact can not be measured within constrained project time frames.

Practitioners would like qualitative reports to be valued as equally relevant, and stress how specific projects should be documented reporting their long-term outcomes instead of their short-term ones.

Articulating critical funding deficits

When asked about what initiatives or services are the most difficult to get funded, the interviewed practitioners mentioned a variety of items which can be summarized under the following categories: sustainability and safety, professional development, service impact and operational costs.

The vocations of security trainers and capacity builders are widely recognized as steep and not-well-defined career paths.

Working in highly stressful and sometimes dangerous contexts has hard consequences on their physical and mental health and safety, and resources in support of their wellbeing and healing are close to non-existent.

Independent practitioners often find themselves needing to hold second jobs in order to sustain their human rights-focused work.

Funding for professional development initiatives is scarce. This negatively affects practitioners needing to improve their skills and grow in their careers, as well as the practitioner community at large, which does not scale due to the lack of training and on-boarding avenues that would bring in more practitioners-to-be.

The interviewees expressed concern that the lack of financial support for long-term capacity building projects will hinder the impact of their work, and drastically limit the quality of the support provided to human rights organizations.

Small capacity building organizations and independent practitioners struggle with the costs and time required to take care of administrative tasks. Furthermore, those who are based in countries with low bandwidth, high telecommunications rates and/or poor transport infrastructure, face unsustainable costs to run their business, and cannot find any sort of financial support to alleviate the burden.

Sustainability and safety

The safety of security trainers who work with human rights organizations is constantly endangered. Cases of aggression, detention and incarceration of these practitioners due to the nature of their work are increasing worldwide. Infrastructure that could help to handle these cases is not yet developed as needed.

- The vast majority of the contracts under which practitioners are hired seem to lack the inclusion of an insurance plan modeled on the potential risks and emergencies that could be encountered.

  The insurance should arguably be handled and covered by the organization or entity hiring the trainers, or alternately costing for such insurance should be considered a non-negotiable component of project budgets. Such insurance would model for different kinds of threats, depending on the nature of the service provided, and the context in which the practitioner operates.

- Interviewees are concerned with the lack of funding and well-resourced paths for rapid response to emergencies and safety issues on the job. They highlight the need for:
  - A strengthened rapid response infrastructure aimed at helping in cases of aggression, detention or incarceration;
  - Funding models to address the costs occurring during such emergencies;
  - Legal support programs with the necessary expertise to support these cases;
  - Initiatives advocating for the human and legal rights of security practitioners;
  - After-care funds to cover means of sustenance and recovery costs, for practitioners who experience aggression, detention or incarceration due to the nature of their work.

- The interviewed practitioners emphasized the need for health care support programs, in order to enable information security practitioners who are diagnosed with medically reported work-related issues to take paid time off and recover.

Professional development

- The majority of the interviewed practitioners underscores the lack of funding for a Training of Trainers (ToT) infrastructure, designed for both individuals who want to become information security practitioners, and individuals who are already working professionally in this field. More specifically, they highlighted the need for:
    - Training of Trainers (ToT) in-person events;
    - Training of Trainers (ToT) online resources;
    - Mentoring programs;
    - Channels to engage remotely in peer-to-peer knowledge and skill sharing.
- It is very hard for practitioners to obtain funds to undertake individual professional development endeavors. Many would like to attend courses to achieve higher technical proficiency, deeper knowledge of pedagogical methods or stronger knowledge of project management techniques. As it currently stands, funding and contracting models presume practitioners track the field at their own expense, which is particularly challenging when doing information security work, given both rates of change in the field as well as the high nature of the stakes in the human rights context.
- Several practitioners also highlight the need for paid research time.

  This would not only benefit their knowledge of relevant subject matter, but would also constitute an opportunity for them to create open resources, produce analysis of applications, and develop other tools that could support the work of other practitioners working in the sector.
- Security practitioners who are not permanently employed by organizations or institutions with dedicated travel budgets struggle to find financial support to attend professional meetings outside of their region or country.

  This has considerable negative consequences on their ability to operate in the field, because in-person opportunities to build and cultivate trust relationships is essential to the sustainability and quality of their work.

  The practitioners who are most affected by this challenge are those who are based in countries where international events usually do not take place, and where travel infrastructure is limited and accessible only at very high costs.
- Several interviewees highlight the importance of also acquiring professional experience outside of the region where they are based. Working abroad, either through a fellowship program, or through a traditional project-based hiring process, is considered a key opportunity to broaden and strengthen the knowledge and understanding of different contexts and user needs.

Service impact

The interviewed practitioners stress both the importance of and lack of funding for long-term capacity building projects. Most of the grants designed to foster organizational security initiatives are built on time frames which are deemed too tight, and not suitable to allow for substantial and long-lasting outcomes.

The ability to engage with an organization over time, and not on a short-term one-off basis, is considered necessary to provide them with meaningful and impactful benefits.

The following are some key observations shared on this matter.

- All interviewees who have been funded to offer short-term support to organizations have experienced the troublesome circumstance of being called back by their former trainees, in need of further assistance. Not being funded to work with them anymore, security practitioners find themselves in the distressing position of having to decide between refusing to help an organization in need, or working free of charge to their own disadvantage.
- Years of practice in the human rights field allow the interviewed practitioners to weigh in on the differences between working with organizations with at least one staffer dedicated to the information security of network, data, and personnel, versus those which cannot afford this resource.

  The advantage of having at least one IT staffer in house is invaluable. These individuals can follow up on an organization's security assessment, participate in the staff training, and be available to answer internal questions after a practitioner has completed their work.

  Security practitioners wish there was more funding available for human rights organizations to have such skilled professionals on their teams.

Operational costs

The administrative and operational costs of maintaining a business can be prohibitive for security practitioners working independently or in small nonprofits. Among the items deemed by interviewees as some of the most essential and difficult to fund are:

- Professional/organizational website and email accounts;
- A reliable Internet connection, particularly expensive to maintain in countries with poor broadband infrastructure;
- A dedicated organizational bank account, as opposed to regular personal bank accounts, required by foundations as mandatory requirement for nonprofits to receive financial support.

Tackling training management challenges

Our interviews identified a number of common challenges experienced by security trainers and capacity builders in regards to the management of the training and capacity building services they provide.

These can be summarized under two key categories: Organizational security culture, and human resources-related issues.

Organizational security culture

- Expectation management is a key challenge which often creates tension between practitioners and decision makers and staffers.

  Organizations tend to ask for very short trainings and, in the trainers' opinion, have unreasonable expectations for the impact that such brief engagements can provide.
- Security practitioners struggle to build understanding on the pressing importance of long-term process-focused capacity building, over short-term tool-based trainings.
- The presence of an in-house IT specialist is not always valued as it could and should be by their organization.

  It is not uncommon for IT team members to be considered exclusively responsible for network integrity and server security, and not for the security of the organization's assets and staffers.

  Therefore, they are not brought on board when the organization receives a digital security training. As a consequence of this role compartmentalization, the organization misses an important opportunity to strengthen the security of its staffers and its own sustainability.

Human resources issues

- The ratio between the number of trainees and the number of hired trainers is often an issue. When a trainer has to engage more than a few trainees at the same time, they end up having to sacrifice the quality of the service delivered.
- Working with organizations which cannot afford to have at least one IT specialist in-house is a challenge for security practitioners, who cannot count on their technical support.

  An IT specialist can support the work of a practitioner during the organization's security assessment and the staffers' training, and can serve as a reference person for follow up questions once the trainer has concluded their project.
- Depending on the social, political, economical context in which they operate, human rights organizations can have high staff turnover. This is a concern, as it can affect the ability of an organization to retain security-knowledgeable staff, and consequently increase potential vulnerabilities.

Drawing on training and capacity building resources

Over the past few years, a growing number of security practitioners and organizations have collaborated on the creation of new resources aimed at supporting information security trainers and capacity builders working with human rights organizations.

The types of resources vary widely, from curricula to be used during trainings, to security assessment frameworks, to training practice manuals.

There is of course still room for improvement. The interviewed practitioners shared their wish lists of educational aids which, in their opinion, would greatly help to strengthen the services and support they can provide.

Most-referred-to resources

The following is a list of the training resources which were most often referred to by interviewees.

- LevelUp: Very much appreciated for its resources on how to prepare for a training, and the suggested topic-based session formats. Its users would welcome the addition of more resources, as well as a regular revision of the existing modules to ensure they are current.

  https://level-up.cc/

- Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG): Resource most referred to by practitioners who want to learn how to conduct organizational security audits.

  https://safetag.org/

- Holistic Security: Key manual for all the practitioners who seek to integrate self-care, well-being, digital security, and information security into traditional security management practices.

  https://holistic-security.tacticaltech.org/

- Security Education Companion (SEC): SEC is designed for those who would like to help their communities learn about digital security but are new to the art of security training. As such, it is recommended by more experienced trainers to folks who are new to the profession and would like to start helping their peers with some essential learnings.

  https://sec.eff.org/

- Surveillance Self-Defense (SSD): Practitioners suggest this resource to folks asking for a starter checklist to secure their information, especially if their needs align with the profiles laid out in the SSD Security Scenarios section (LGBTQ youth, academic researcher, journalist on the move, activist or protester, etc). SSD is deemed most suitable to help users based in the US and Europe.

  https://ssd.eff.org/en

- Security Planner: Recommended by practitioners when they are asked for a quick starting-point-tool to identify general steps that users can take to make their accounts and devices safer.

  https://securityplanner.org/

- Digital Security Readiness Assessment Tool: Used by practitioners to make an initial assessment of what baseline systems an organization can improve before taking on new security initiatives.

  https://0xacab.org/iecology/security-checklists/blob/master/2_readiness_assessment_tool.md

Wishlisted resources

The following is a summary of the resources that interviewees wish existed in support of their practice:

- Guidelines to help a security practitioner with setting their client's expectations at the start of their professional collaboration.
- Best practices to design and build information security curricula for human rights organizations.
- A checklist enumerating key considerations to make, and steps to take, when designing an organizational security project.
- A checklist for trainers to assess the digital and physical security of a space under consideration to host a technology capacity building event. This could build on existing resources, such as the LevelUp module on *Creating Safe Spaces* https://level-up.cc/before-an-event/creating-safe-spaces.
- A template to help practitioners build workshop agendas, of different durations and for participants of different knowledge levels. The template would not include details about the activities to be facilitated, as choosing them would be the practitioner's responsibility. Still, this would help a trainer organize the time at their disposal, design the narrative arc of the workshop, and set its pace.
- A web-based platform aggregating different types of activities and exercises, including those listed in existing guides such as LevelUp, Security Companion, SAFETAG and more, for practitioners to pick and choose the ones most suited to a training they are designing.
- A web-based archive of stories that show the importance of information security, to help trainees with understanding different circumstances of vulnerability and their consequences. For example: "What could happen if someone had access to a staffer's mobile phone or email account?"
- A “hot line” service or helpline to support trainers with answers to specific technical questions which might emerge during trainings, and to provide them with easy-to-understand explanations of technical matters that they can include in their curricula.
- Guidelines for trainers and capacity builders to assess the physical security of a human rights organization's staffers and workspace(s).
- Best practices on how to follow up, both remotely and in person, with organizations after a training or assessment has taken place.
- A collection of best practices to provide information security support and education when it is not possible for the capacity builder and a human rights organization to meet and work together in person.

Keeping track of the field

Staying current is a significant aspect of the work of security trainers and practitioners working in a sector which is affected by developments of social, political and economical nature, the emergence of new technologies and often hard-to-predict information security threats.

The number of spaces and channels for practitioners to meet, build trust relationships, and explore room for collaboration is growing.

Peer-to-peer mailing lists focusing on a wide range of topics hold space for remote and asynchronous discussions between folks living in very different geographies. Interviewees indicate these lists as their preferred and most trusted sources of information and peer learning online.

A few international meetings, such as the Internet Freedom Festival (IFF), provide international travel support to participants, thus helping to bridge geographical distances and enabling the growth of international networks of security practitioners.

However, the opportunities to gather in small strategic meetings are still few and far between. This is a key issue, since such meetings are deemed to be a critical means for practitioners to improve and keep their training and facilitation skills up to date.

Furthermore, the rapidity with which emerging technologies and security threats constantly change is a key concern. Many interviewees struggle with finding their way through both more and less reliable information security news outlets, and assessing the risks caused by reported malicious attacks and their consequences for their trainees.

Emerging technology and security threats

Practitioners experience different issues with keeping up with emerging technologies and information security threats. Among them:

- Finding reliable aggregators of trustworthy information and news is a challenge. Identifying who or what to trust is a key concern.
- Keeping up to date on information security news requires more time than practitioners can afford to dedicate to it, thus also hindering their confidence in responding to the trainees' queries on the latest security threats.

Training methodologies and practices

The ability of practitioners to stay current on educational methodologies depends on several factors.

- Most of the manuals and guides available online are not up to date, as they are often tied to project-based funding which in many cases provides support for content creation, *but not for its maintenance*.
- Manuals and guides are one source of knowledge for security practitioners, but not the only one. Discussions with peers on training best practices and pitfalls are a necessary complement to the individual study of the subject matter.

General challenges

On the whole, in regards to staying current in their work on any topic or practice, all interviewees seek increasing opportunities to participate in in-person spaces, designed for fellow trainers and capacity builders to share skills and knowledge, at both international and regional levels.

Cultivating trust relationships with security researchers, analysts, and trainers is deemed to be of extreme importance in order to gain access to reliable information. At the same time, being part of a trustworthy network is something that is not accessible to many, for example due to lack of funding to travel and meet peers, or due to a lack of fluency in specific languages.

Large events are appreciated, because often they provide travel support that enables folks from a wide range of countries to meet together. This gives participants a chance to learn about experiences and contexts with which otherwise it would be much more difficult, if not impossible, to connect.

Smaller events, designed for participants to focus on one specific topic or project, are preferred however, as they allow for more specific, detailed, and confidential discussions to take place, and provide invaluable opportunities to build trust relationships and strengthen communities of practice.

Envisioning new forms of infrastructural support

Reflecting on the sectoral and organizational infrastructure within which they operate, the interviewed practitioners acknowledge the absence of intermediary initiatives or organizations with the mandate to support their professional category.

They recognize that there have been projects aimed at investigating their professional needs. One valuable example of such efforts is the Engine Room's and Ford Foundation's report *Ties That Bind: Organizational Security for Civil Society*[1].

However, they wish it would also be possible to move forward, and start envisioning and building more permanent infrastructure designed with their community's sustainability in mind.

Interviewees expressed the desire to receive the support of trusted professionals who understand their strengths and challenges, and can help them to imagine long-term strategic paths for their work.

The following are services that they imagine such intermediaries could provide.

- Contributing to the design of professional development programs and initiatives;
- Provisioning of resources for business planning and cost modeling, back office support, financial and cash flow management, and corresponding business soft skills development.
- Designing and facilitating peer-to-peer knowledge sharing spaces;
- Catalyzing and managing collaborative efforts, such as the co-creation of shared resources;
- Documenting and advocating for these challenges and needs with other stakeholders working in the human rights field, such as funders, technologists, and tool designers.

[1] *Ties That Bind: Organisational Security for Civil Society*, Engine Room. https://www.theengineroom.org/civil-society-digital-security-new-research/

Conclusions

What surfaces as the key learning from this survey is that professionals working in very different information security capacity building contexts and circumstances expressed a common set of pressing needs for shared permanent infrastructure designed to strengthen the sustainability and efficacy of their work.

This matches what we have observed over years of work in the human rights field: the sector does not have a comprehensive strategy for success and sustainability of security practitioners.

The scarcity of funds increases the fragmentation of a sector in which service providers are under-resourced and under tremendous safety, financial and circumstantial pressures.

Practitioners with different levels of expertise and offerings also describe a lack of professional development infrastructure, which would help them to optimize their competencies and relevance in delivering services.

In recent years, positive instances of incremental improvements and changes in the way the sector operates have occurred, such as the offering of fellowships dedicated to supporting practitioners in furthering their careers, and the funding of efforts which go beyond traditional security management practices and integrate well-being and self-care into their frameworks.

But neither the learnings, nor the evolutionary changes to our intervention models are systematically documented, shared, applied or scaled.

Recommendations

Following up on the findings from this limited survey, we believe that it is critical for the sector to acquire a clearer understanding of the infrastructure that exists in support of information security practitioners, and of the challenges and gaps that hinder their profession and the contributions they can make to the human rights field.

This body of knowledge could constitute an essential foundation to catalyze further discussion aimed at provisioning improved and more sustainable infrastructure.

For this purpose, we recommend undertaking a wider cross-sector survey, engaging workers at human rights organizations, practitioners from different domains supporting their efforts, and funders subsidizing the sector.

The following are some of the key topics that such investigations could explore.

- Maintenance and improvement of practitioner skills and knowledge, both within own domains and cross-domain.
- Contextualization of the services provided through interaction and dialog with human rights workers.
- Critical analysis of different security assessment and training methodologies, aiming to evaluate their efficacy and suitability in varying contexts.
- Review of existing professional development initiatives to improve their offering to better match the needs of practitioners.
- Opportunities to model new and varied professional development efforts, leveraging peer-to-peer knowledge and skill sharing, and long-term inter-generational mentorship relationships.
- Strategic support of business development and sustainability planning through ad-hoc consultancy services and back-office support.
- Increased education and awareness-raising targeted at human rights organizations, helping them to be better and more realistic consumers of information security services.

- Establishment of well-resourced paths concerning practitioner health and safety, including insurance models and care resources for different kinds of threats and traumas that can incur on the job.
- Identification of pilot initiatives that could be funded to test out new forms of support, for example in regards to emergency rapid response infrastructure, sustainability of long term organizational security efforts, and mentorship-based programs.

The findings emerging from this broader series of discussions could then be summarized and shared with the wider community, inviting feedback and possibly also further iterations.

Once a solid initial analysis is articulated, those outcomes will represent a compelling opportunity to invite one or more cross-domain groups of stakeholders to engage in strategic dialog on different key issues.

At that stage, the exploration could focus on envisioning how improved infrastructure in support of practitioners working in the human rights field might look. Participants in the discussions could aim to collaboratively draft and evaluate different scenarios for further development, implementation and long term funding.

Most importantly, we believe that for this effort to strive for long term sustainability, it should be community-designed, community-led, and community-owned.

Appendix: Interview questions

1. How well do you feel are you able to stay current in your work? "Current": In regards to new and emerging tech, and also capacity building methodologies and practices.
2. How do you do it? E.g. talking with people met at conferences, etc.
3. Are there specific resources you use? E.g. blogs, newsletters, mailing lists, etc. Please clarify if a resource is public or if you would like to mention it off the record.
4. Are there lists of resources, directories, or maps you make use of? E.g. lists of information security trainers, lists of trusted vendors, etc. Please clarify if it is public or if you would like to mention it off the record.
5. Are there other (not financial) resources that you wish existed to support your work?
6. Are there things you find hard to get funded?
7. What do you find yourself spending a lot of time on? Think in particular about tasks you might like to avoid. E.g. administrative work, operations management.
8. In your opinion, which challenges are faced by technology capacity builders, trainers, intermediaries in the human rights space?
9. Which are ongoing challenges that *you personally* keep encountering in your work?
10. To what degree do you think of the work your currently doing as a career path?
11. To the degree that this is a career path, what kind of professional development resources do you wish existed?
12. Thinking about the topics we discussed today, do you know organizations or initiatives focused on the needs of technology trainers and capacity builders in similar terms?
13. Where would you benefit from having roadmaps, templates or checklists to support processes or activities that are part of your work?
14. Is there any other question that you think we should ask to folks like you, as we have further interviews?
15. Is there someone you would recommend us to interview?