Ties That Bind

Organisational Security for Civil Society

Prepared by The Engine Room for the Ford Foundation
March 2018

THE
ENGINE
ROOM

This research report, commissioned by the Ford Foundation, was conducted by The Engine Room from January-December 2017. The content of this report does not reflect the official opinion of the Ford Foundation, and responsibility for the information and views expressed in the report lies entirely with The Engine Room.

Commissioning Editors and Content Support: Michael Brennan, Jean Cook, Ryan Gerety, Jenny Toomey.

Lead Researcher: Zara Rahman (The Engine Room)
Research Assistant: Paola Verhaert (The Engine Room)
Research and Content: Nicole Anand, Alix Dunn, Laura Guzman, Anca Matioc, Maya Richman, (The Engine Room)
Illustrations: Jason Li, http://hongkonggong.com/
Report Design: Adjoa Opoku

The Engine Room requests due acknowledgement and quotes from this publication to be referenced as: The Engine Room: Strengthening The Digital Security Support Ecosystem, March 2018. This report is available at https://theengineroom.org.

Contents

Introduction

As the use of digital technologies has spread throughout civil society, they have brought with them new opportunities for groups to amplify their work at greater speed and scale than before. But they have also brought new realms of risks and vulnerabilities. For civil society, one response to those risks can be seen in the **digital security support ecosystem**, a sprawling ecosystem of organisations, individuals, collectives and multi-stakeholder groups who seek to provide security support for civil society.

This report adopts a broad understanding of digital security, encompassing not only security-focused interventions and those traditionally understood under the digital security label, but also areas of weakness or vulnerability for civil society in their use of digital technologies and technical infrastructure on an institutional level.

Traditionally, digital security support has been provided through trainings, often tools-focused. This has not worked – societal context changes fast, and with it, the appropriateness of certain tools. In this report, we look beyond tools-centred approaches to digital security to consider areas of vulnerability for civil society more broadly, and how they can be addressed. We take a broad approach of what is understood as **digital security support**, considering emotional support and social interventions as well as technical ones.

Taking into account Ford Foundation's focus on strengthening institutions, in this discussion and analysis we look at **building a healthy digital security support ecosystem for civil society in the longer term**, and at interventions that build institutions rather than individual capacities. Digital technologies connect us, which means that a weakness at one point in the network can result in risks for another part, such as emails forwarded with viruses, or contact databases leaked by one person with another person's personal details in it. For institutions and organisations, this knock-on effect should have a big impact on how digital security support interventions are implemented.

As we describe in the report, digital security is deeply intertwined with other forms of security, such as physical and psychological. But civil society is currently less accustomed to noticing and knowing how to respond to digital security threats. Digital security can be far less tangible and visible than other types of security. Here, we outline here why it matters. We highlight different organisational needs around digital security and propose approaches for meeting those needs.

The digital security ecosystem is made up of many parts: in this report, we focus on the needs of civil society organisations. In the diagram below, we show a (non-exhaustive) view of how these needs intersect with other key parts of the ecosystem.

To understand what elements should be present within a healthy digital security support ecosystem, we focus on identifying **civil society organisational needs** from that support ecosystem. By first understanding needs, we can assess potential approaches and, in the final section, suggest recommendations for funders.

We believe that, above all, a healthy digital security support ecosystem is one that can meet those needs in a responsive way and can support civil society organisations to build healthy digital security practices over time.

SUMMARY

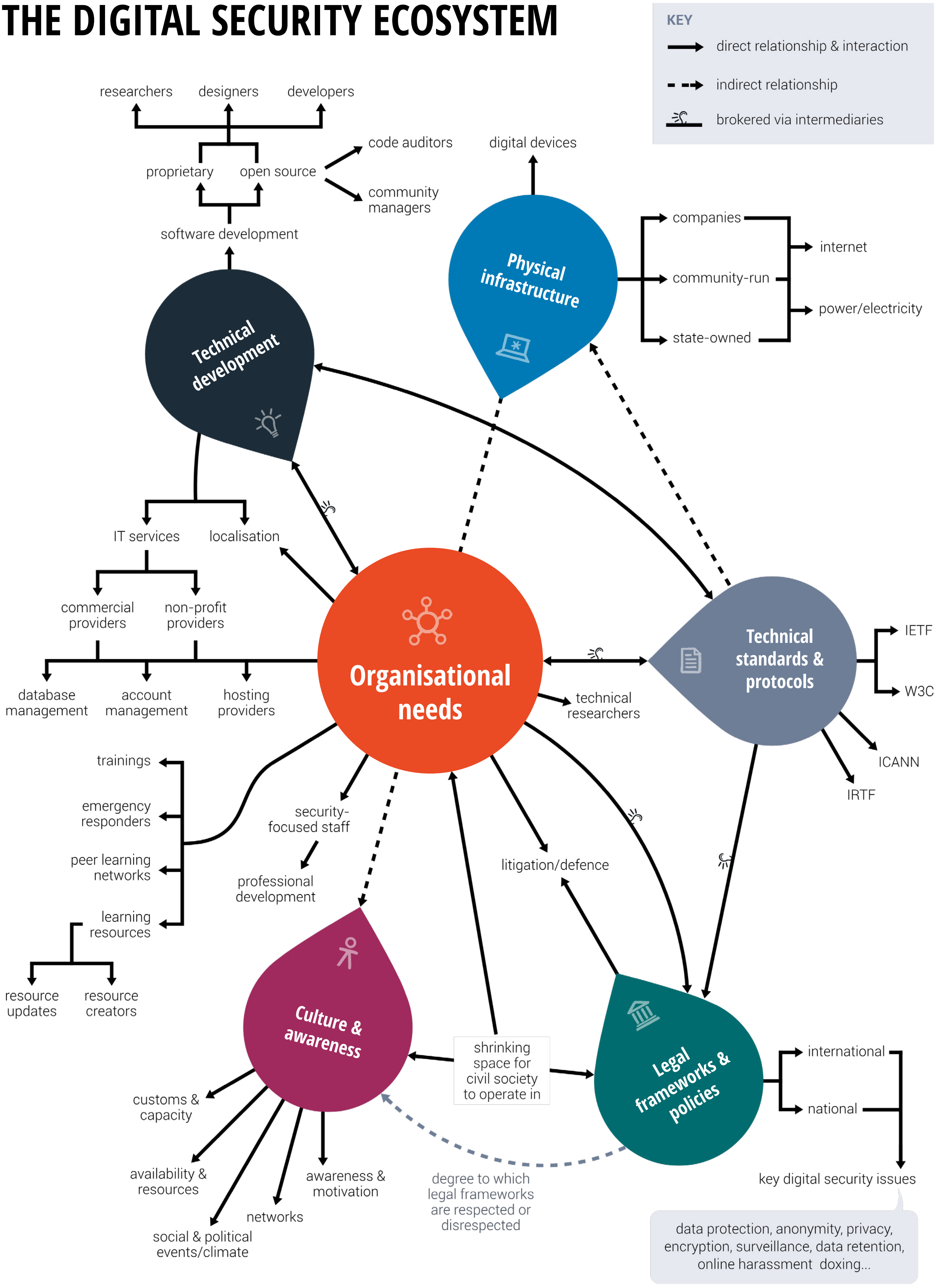
Section 1 - The Contextual Nature of Security presents contextual insights to situate the rest of the report. Here, we discuss basic understandings of digital security, consider political contexts, and take a brief look at current and past approaches to digital security support provision. This section frames the rest of the report, and provides an introduction to thinking about the role of digital security within a broad social and political context.

Section 2 - Organisational Journeys introduces a framework for understanding the journey that an organisation (a grantee) goes through in developing their digital security processes. This framework is outlined in a diagram on Page 17, and introduces three organisational archetypes. From 'unaware' organisations, for whom digital security is not at all a priority; to 'learning' organisations, who are beginning to see why digital security is important; to 'mastering' organisations, who have developed ways of implementing and operationalising digital security within their institution.

Insights in Section 2 are focused around these three archetypes, with the aim of emphasising how different kinds of digital security support are required for organisations who are at different stages of this cycle. Note, too, that this is very much a 'cycle' rather than a one-time 'process' — organisations continue on this cycle as they develop capacity in different digital security practices.

Section 3 - Recommendations draws from the insights of this research, and is particularly informed by The Engine Room's experience in this field.

THE DIGITAL SECURITY ECOSYSTEM



First published March 2018. Created by The Engine Room with support from the Ford Foundation, designed by Jason Li.

1. The Contextual Nature of Security

Perceptions of security, and necessary reactions are highly contextual. With this in mind, this report focuses on one context: that of the United States between January-September 2017. The majority of our informants and interviewees know the US context well. We also spoke with digital security experts working in an international context, all of whom referred at least once to digital security materials created in or for the US context.

The Engine Room has worked in and with both the US domestic digital security community and various international communities. Throughout this report, we aim to elevate the opinions and experiences of underrepresented groups in these communities, while also recognising the more traditional voices in the digital security space.

1.1 UNDERSTANDING DIGITAL SECURITY

To help readers understand how we see the role of digital security with regards to institution building, we developed this visual metaphor, with descriptions in the yellow boxes of similar aspects between 'fire safety' and 'digital security.'

Many vulnerabilities are embedded in an organisation's infrastructure: they are hard to see and take time to resolve. However, many organisations prioritize quick fixes that don't have a lasting impact because they are more visible and provide more instant gratification.

Institutional vulnerabilities in the digital space might stem from the way in which an organisation's website was set up right at the beginning – perhaps not using the most up to date software – or be related to daily practices in an organisation's operations, like making salary payments, or other financial transactions. Fixing these vulnerabilities often takes both a technical change and a behavioural change in the habits of staff, which takes much longer to implement and get used to.

CASE STUDY

INADEQUATE QUICK FIXES

Key learning: Perceived "quick fixes" for digital security often get priority, even though they might not be as helpful in the long term.

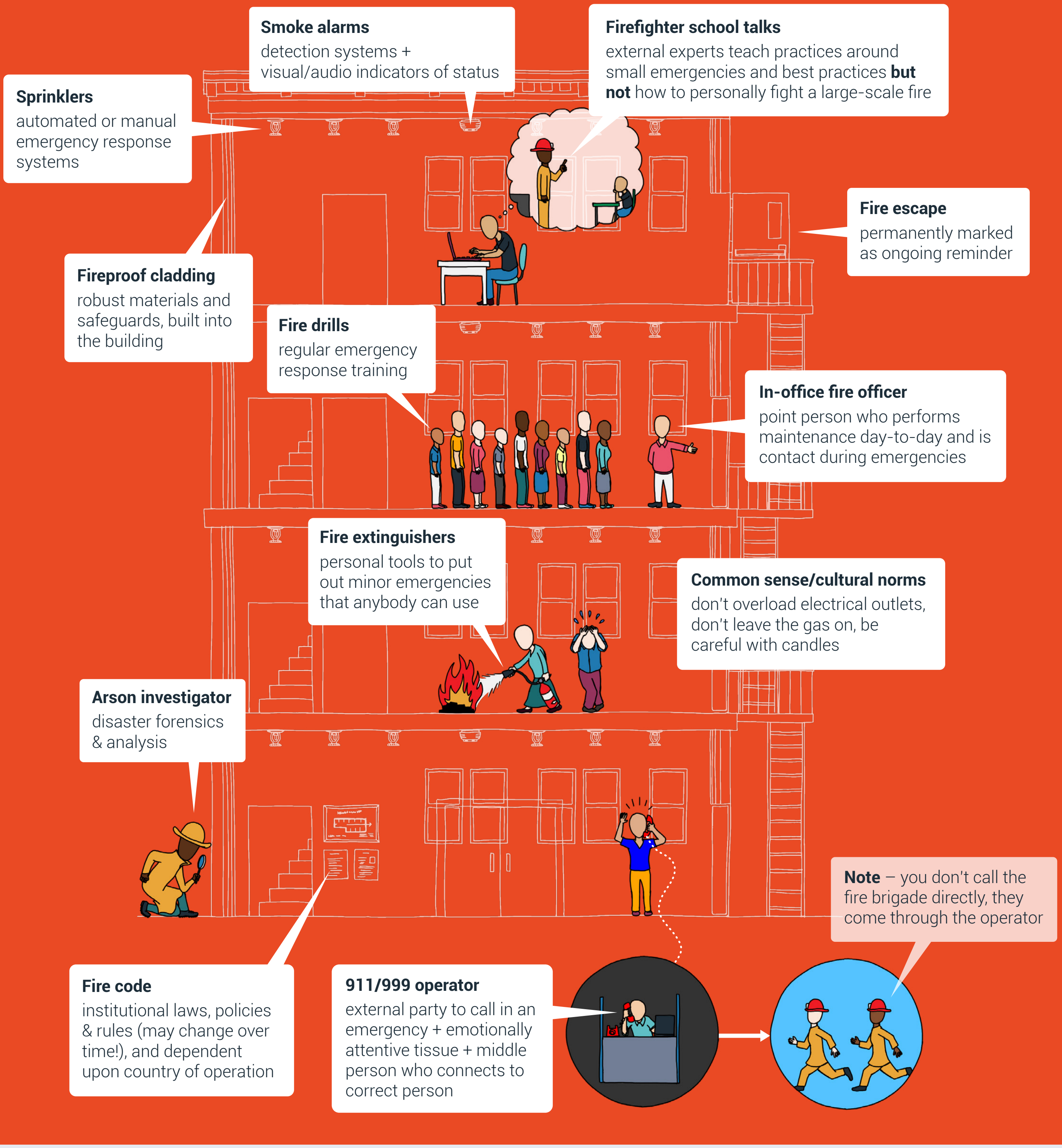
One organisation ran a community crowdfunding campaign with the framing of "helping staff boost their digital security." They used the money to buy new iPhones for staff, but didn't cover key security issues, like:

- Policies for putting work accounts on personal phones
- Mobile device management guidance
- Development and/or enforcement of any kind of security policy

Buying new iPhones for staff is a tangible, quickly achieved outcome of raising money. But without a longer term security focus, the new devices may not ultimately contribute to a healthier digital security practice within the organisation itself.

This can be observed in a higher demand among organisations for one- or two-day trainings rather

Digitally Securing Your Organisation Is Like Preparing Your Office For A Fire



Smoke alarms
detection systems + visual/audio indicators of status

Firefighter school talks
external experts teach practices around small emergencies and best practices **but not** how to personally fight a large-scale fire

Sprinklers
automated or manual emergency response systems

Fire escape
permanently marked as ongoing reminder

Fireproof cladding
robust materials and safeguards, built into the building

Fire drills
regular emergency response training

In-office fire officer
point person who performs maintenance day-to-day and is contact during emergencies

Fire extinguishers
personal tools to put out minor emergencies that anybody can use

Common sense/cultural norms
don't overload electrical outlets, don't leave the gas on, be careful with candles

Arson investigator
disaster forensics & analysis

Note – you don't call the fire brigade directly, they come through the operator

Fire code
institutional laws, policies & rules (may change over time!), and dependent upon country of operation

911/999 operator
external party to call in an emergency + emotionally attentive tissue + middle person who connects to correct person

Digital security is often understood as a **personal** action – but for healthy digital security practices to be effective, they have to be **shared**. Like fire safety, you can think about digital security at different levels:

- Within an institution's infrastructure: ensuring your operational infrastructure is secure, from email hosting to finance software.
- Understanding different levels of response: different levels of digital security threats require calling different experts (external, or in-house.)
- Culture and knowledge: building up literacy around digital security on an ongoing basis, to develop a culture that prioritises security and safety.

First published March 2018. Created by The Engine Room with support from the Ford Foundation, illustrated by Jason Li.

than longer-term budget commitments towards methodical roll-outs of new policies. Organisations can also prioritise trying out a new technology tool over investing in boosting technical infrastructure. Many interviewees highlighted both civil society and funders' preference for quick "shiny" fixes.

DILEMMA

POLITICS OF DIGITAL SECURITY

Understanding the role of digital security within an organisation can make a difference to how it is perceived.

Digital security as a technical intervention

For some support providers, digital security support work was perceived as "apolitical", and primarily centred around technical interventions to support various political missions rather than political in and of itself. Support providers who work with communities that they are unfamiliar with, or who play a purely technical role in, for example, carrying out analysis of potential instances of malware, perceive their role as separate from any kind of politics, and purely as a technical intervention.

vs.

Digital security is a part of a political fight for justice

For other interviewees, digital security is inherently a political act, based on the belief that "surveillance is a desire to control poor populations of colour". People we spoke to with this view highlighted that privacy and security mean very different things for populations who are under different levels of surveillance from the moment they are born. In the United States, this includes poor communities, those relying on state support, and people who are disproportionately targeted by state forces (such as African American populations), to name only a few.[1] For these interviewees, starting from this point results in a justice-centred approach to digital security.

Our take:
We believe that particularly in the United States, centring race is essential to understanding the security threats and challenges faced by communities of colour in particular. Digital security – just like any other type of security – changes depending on the social and political position of the person, or community, under threat. Particularly in the United States, communities of colour are subject to vastly different types and levels of surveillance than predominantly white communities, and this needs to be taken into account when designing security support interventions.

Applying a lens of racial justice to design of support ensures that these needs and asymmetric threat models are appropriately acknowledged and proactively planned for. This is just one example of how having security support providers who are intimately familiar with the context of those they are seeking to support, can make a big difference to how effective the support will ultimately be.

CASE STUDY

RAPIDLY CHANGING TECH POLICIES

Key learning: When messaging app WhatsApp changed their policies around security, users were left confused by conflicting messages coming from the media, and WhatsApp themselves, around the app's suitability for their needs.

As of February 2016, 1 billion people were reportedly using WhatsApp[3]. In mid-2016, the messaging app company rolled out default end-to-end encryption to all users on all devices. This decision was an important step towards the normalisation of end-to-end encryption as a standard for messaging apps[4], but they didn't include end-to-end encryption for group messaging – creating confusion for users. However, it is important to note that users' privacy and security needs stretch beyond end-to-end encryption of content. This was demonstrated when WhatsApp announced in August 2016 that it would share users' phone numbers and last time of usage with Facebook, which had acquired WhatsApp in 2014[5].

The way in which company policies changed rapidly around WhatsApp's contact management and encryption meant that people who wanted to practice good digital security received mixed messages about its suitability. For readers of the Guardian newspaper in the UK, this was further confused by reports claiming that there was a "backdoor" in WhatsApp (a term subsequently amended to "vulnerability" by the reporter), which were heavily criticised by a group of leading security researchers.[6]

Policy changes and technical developments can result in confusing messages for users of certain tools or practices, even those wanting to improve their digital security practices.

1.2 CHANGING CONTEXTS

Learning and mastering digital security requires consistent learning rather than a one-off effort, because the digital security ecosystem (and one's own threat model) can change quickly.

As Martin Shelton writes - "digital technology doesn't die – it just ages really, really fast. Even the richest digital security resources become quickly out-of-date."[2]

Mission-driven organisations' lack of resources for ongoing learning means that many rely on trusted intermediaries to update them on what new developments mean for their work[7]. These intermediaries are typically institutions or individuals with time and resources to monitor the latest developments, understand their implications for civil society, and 'translate' them into a format that makes sense to civil society.

Interviewees suggested that another consequence of this fast-changing landscape was that recipients of one-off support interventions felt confused or overwhelmed by changing advice they received.

Recommended best practices for digital security change fast as a result of political changes, legal changes or increasing awareness of technical vulnerabilities.

Many interviewees working on support provision in the United States mentioned a definite spike in interest around boosting digital security practices following the 2016 national election. To describe this in terms used in the digital security world, this was because people's threat models changed: the potential ways in which their safety and security could be compromised or attacked, changed as a result of the political context changed.

However, interviewees' opinions were largely split around whether this initial interest translated into a longer-term change in behaviour, or in the way their advice was received.

Responsive funds – such as Ford's Digital Security Surge Fund – were described as being very helpful in allowing organisations to make flexible, agile responses to rapidly changing contexts.

This also speaks to the need for digital security support to be focused around supporting the uptake of critical thinking and self-assessment, rather than recommending particular tools that could age quickly.

1.3 POLITICS AND CRIMINALISATION OF DIGITAL SECURITY

At a time of shrinking civic space in the United States, and indeed across the world[8], digital security measures are becoming increasingly important for organisations seeking to hold those in power accountable. But particularly of late, digital security support has become a target for governments wanting to crack down on civil society.

The case of the Istanbul 10 is an extremely worrying development in terms of how governments and others perceive digital security. It politicises the issue of protecting oneself when using digital technologies to a worrying degree, particularly for those working in civil society.

The targeting, detention and arrest of digital security trainers explicitly for their work marks a clear change in how digital security support has been treated by repressive governments. The case of the ten rights defenders in Turkey is still ongoing, and whether this case means that digital security workshops will become more of an explicit target, or whether this is a one-off, is yet to be seen.

Digital security support needs to be planned carefully for the context in which it will be implemented.

For example, particularly in politically restrictive countries such as Turkey, it is clear that digital security provision should be planned carefully. This might mean supporting activists to travel outside their country of origin to receive training (a common approach in efforts to support Syrian activists, who travel to Turkey, or among Turkish activists, who might travel to Georgia). It could also involve taking more precautions when travelling to certain countries.

Examples: Although digital security workshops themselves not been targeted previously, governments around the world have revealed their lack of understanding of digital security and data management through legal policies and statements:

CASE STUDY

THE ISTANBUL 10

Key Learning: digital security is being increasingly criminalised and politicised by repressive states. This paints a worrying trend for the future.

On July 5th 2017, a digital security workshop in Turkey for women rights defenders was raided, and eight participants and two trainers were detained, among them the director of Amnesty International in Turkey; a German citizen, Peter Steudtner, and a Swedish citizen, Ali Gharavi. To the best of our knowledge, this is the first time a digital security workshop has been targeted so explicitly by law enforcement anywhere in the world. After 113 days in prison, all ten were released pending trial – two of the participants were issued travel bans, and the digital security trainers were able to leave the country.[9]

Misunderstanding the role of encryption: Leading government officials have displayed their lack of understanding of how 'encryption' actually works – demonstrating that they don't have a solid grasp on the technical aspects, but perhaps more problematically, that they also do not understand that encryption is important for many aspects of everyday life. Contrary to some of the quotes below, we all depend on encryption – for example, to safely interact with your bank online, and to ensure that strangers can't see your passwords when you type them.

- In July 2017, UK Home Secretary Amber Rudd labelled "so called" end-to-end encryption a "problem" because officials can't access the content of messages sent via platforms using encryption. She requested that technology companies work more closely with the authorities, so that they are able access more information when needed[10].

- In July 2017, Australian Prime Minister Malcolm Turnbull called for a ban on end-to-end encryption, stating that "the laws of mathematics are very commendable but the only law that applies in Australia is the law of Australia[11]."

- In August 2016, then-Interior Minister of France Bernard Cazeneuve stated that "messaging encryption, widely used by Islamist extremists to plan attacks, needs to be fought at international level[12]."

- In February 2016, after the San Bernardino attack in California, the FBI urged Apple to help "unlock" an iPhone used by one of the two attackers. Apple refused the request to create a "backdoor" to get around its own safeguards, although the FBI subsequently claimed they had successfully unlocked the phone without Apple's cooperation[13].

Failing to see the importance of investing in digital security: As discussed in this report, digital security is contextual and core to the ability of an organisation to achieve its mission. For governments, relying on unvetted volunteers would be an incredibly risky way to bolster their own digital security (and would potentially put their own systems at risk).

- In October 2016, Germany's Interior Ministry unveiled plans to set up a "volunteer cyber fire brigade" ("Cyber Feuerwehr"), and ask local companies to lend their IT experts for up to 20 days a year as part of a volunteer cyber fire brigade[14].

Digital security is a part of a holistic security context, which also includes physical security, psychosocial security and operational continuity. Focusing solely on digital security can ignore the bigger picture, and result in redundant or harmful security advice.

For many mission-based organisations, particularly those working in high-risk environments, digital security forms just part of their security needs, as identified by Alice Nah et al.[15] Psychosocial approaches consider psychological factors together with the social environment for individuals, and consider how they intersect to affect the physical and mental wellness of individuals.

Ease and comfort of use is important, too. Digital security advice that is focused on the technical aspects but ignores the usability component can be unhelpful. As Jessy Irwin outlines[16], there is a balance between security and convenience – noting that many of the most secure options out there fall short on the convenience.

To appropriately assess and understand those needs, physical and psychosocial security concerns need to be taken into consideration together – essentially, a holistic approach[17].

1.4 LEARNING FROM THE PAST

As the support community has learned from past activities, best practices around digital security support have evolved over time.

As the use of digital technologies has increased, digital security interventions and practices have evolved. The field is still relatively new – but there are already aspects that we can learn from what has and hasn't worked in the past, and ensure that we build upon those learnings as the digital security support community grows.

The table below summarises trends of how these practices have changed over time, based on our interviews and analysis.

However, it is worth noting that different digital security support providers might well disagree with this analysis, particularly on choosing software tools.

Theme	Older Approach	Current approach
Approach	Do no harm	Harm reduction[18]
Software tools	Free and Open Source Software only	Dependant upon context and capacity of users, which might result in actively choosing a proprietary option
Frequency	One-off trainings, often from trainers unfamiliar with the context or culture[19]	Long-term interventions to boost capacity of the community in question
Solutions suggested	One size fits all, using "global" resources	Prioritising different contexts needs different solutions

DILEMMA

CHOOSING YOUR SOFTWARE

Digital security support goes hand in hand with Free and Open Source Software (FOSS)

For adherents to this view, recommending any software solutions that are not FOSS is seen as irresponsible. Digital security support providers who promote solely FOSS solutions believe that anything else is detrimental in the long run. The short-term wins of ease of use and convenience are, in many ways, being offset by the losses in control and privacy, and for some, using the proprietary solution is of itself a digital security misstep. For example, any software that stores your data in 'the cloud', could in the worst of cases be made available to law enforcement, and thus put the organisation and potentially people reflected in that data, at risk.

VS.

Digital security support should build upon existing practices. If this means recommending proprietary software solutions, then that is the most responsible action to take.

In a way, this approach balances out a tension between having more control over your technology, with potentially not having the in-house capacity to wield that control, or fix the bugs that come along with it. Proprietary solutions are often easier to set up and more user-friendly.

Our take:
We take a pragmatic approach to software solutions, noting that wherever possible, open source options are, in the long run, the better choice for organisations fighting for social justice. Technical decisions are political ones, and the usability of open source tooling will not improve unless more people dedicate resources towards using and improving that experience. That said, we have also seen cases where digital security trainers have recommended open source solutions to organisations which, upon these solutions breaking or not being used exactly as envisioned, ultimately put them more at risk[20]. With this in mind, we encourage a case-by-case assessment of software tools, taking into account the current working environment of the organisation, their internal capacity, and their political goals. Ultimately, organisations should be empowered to make the best decision for them, so we strive to provide them with well-balanced information and support them in whatever they decide to do.

CASE STUDY

NON-PROFITS USING PROPRIETARY TOOLS

Although this is a potentially unpopular opinion among some digital security experts, some proprietary tools can be more usable and accessible for non-profits – whether that's because the open source versions require more technical skills to set up, aren't as user-friendly, or for other reasons.

We can't comment on the security status of this specific tool, but one interviewee told us that the Salesforce CRM, which offers a non-profit version at 76% the cost of the commercial one, has vastly helped both their work and the work of many peer organisations in the sector. They trust the security team protecting Salesforce, and suggested that it had never been hacked, perceiving it to be as "secure as secure can be."

"We're all in on Salesforce CRM... they created a specific version of it for non-profit use. It's been the most impactful development in the sector. It's the fourth largest enterprise company in the world: it has never been hacked, it's as secure as secure can be."

HIGHLIGHT

COMMERCIAL PROVIDERS

Commercial providers are filling a gap in the digital security and tech services space. Some are focused explicitly on providing services to non-profits, but most have a broader mandate, serving a variety of clients.

The role of commercial providers in this ecosystem

Interviewees suggested various roles that commercial providers could play:

Providing direct support through paid contracts: opinions were largely split on whether commercial providers were providing useful digital security support to the non-profit sector. Generally speaking, organisations with stronger political identities – for whom their partners, their politics and their technical choices, form part of their identity and thus their work – rejected commercial providers as not understanding the context in which they were working. For others, however, commercial providers were filling a gap in the support ecosystem.

> *Caveat:* Interviewees generally agreed that the quality of support provided by commercial providers to non-profit clients was lower than expected. One interviewee speculated that this was because non-profit clients were among the smallest and lowest-paying clients, and as a result, were a lower priority for the provider.

Providing voluntary expertise: others, notably those with private sector expertise, noted that the skills learned for technical workers in the private sector were vastly more advanced than those working solely in non-profits. Opportunities for technical advancement were more pronounced; there were more opportunities to learn from peers and work in technical teams, rather than as the sole technical advisor; and the private sector attracted smart, skilled workers.

They also noted, however, that non-profits could likely never compete in terms of salary and benefits offered by the private sector, and as such, suggested that the most realistic way to tap into that expertise was through creating for people with private sector jobs to contribute.

Understandings of security threats around the world are limited by blind spots, which have been created as a result of researchers' focuses on particular areas or awareness-raising campaigns in a defined area.

This means that global analyses focused on areas affected by issues such as high incidence of malware do not always represent the global picture accurately. A variety of factors feeds into this, such as funding resources available for research on particular geographic areas, combined with higher literacy among civil society in those areas, meaning they are more likely to flag particularly worrying threats; or an increased focus due to political events, or increased awareness or responsiveness of security threats in certain regions if they are perceived as 'higher profile' incidents around the world.

Even when digital security support has been provided, it is often incomplete. In many cases, monitoring and evaluation mechanisms are either not included or do not provide useful information to allow for iteration and improvement.

In the past, metrics around digital security support have focused on easy-to-gather data such as number of visits to an online resource, or number of attendees at a particular digital security training. Neither of these data points indicates the way in which the support was received, or the impact that the support had in the long term.

CASE STUDY

LIMITED RESEARCH FOCUS AREAS

Key learning: Current understandings of technical threats are driven by research investment investment and understandings of digital security in specific geographic areas, rather than being an indication of areas with a higher frequency of incidents.

One interviewee who previously worked as a security researcher highlighted that areas of focus for research "create a narrative" that will produce more along these lines. For example, interviewees suggested that because there are more resources dedicated to understanding digital threats faced in Mexico or Syria, people working in those areas become more aware of the threats they might face. Accordingly, they build up more capacity to recognise those threats, again strengthening this narrative.

1.5 RETHINKING EXPERTISE

Technical expertise is just one kind of expertise required within a healthy digital security support ecosystem. Being able to listen well, diagnose problems and provide emotional support is an essential (and under-valued) element of the digital security support ecosystem.

When someone feels threatened, initial reactions are centred around fear – so having someone to respond with emotional support in the form of listening, understanding what the problem is and what kinds of responses might be appropriate, are key. But under the current model, technical experts are often the first port of call for people who are in need of digital security support. This has a number of detrimental consequences:

- It conflates the emotional and technical support required upon being the target of an attack.

- It means that all kinds of digital security support requests go to technically skilled people, even those that don't require technical support, potentially hampering the coordination and provision of adequate support

- It decreases the chances that non-technically skilled people will feel empowered to take on key roles with regards to digital security, thus maintaining the relatively homogenous status quo in the digital security space.

- It devalues the contribution of non-technical experts working in the broader digital security ecosystem, and reduces the effectiveness of the ecosystem as a whole, creating bottlenecks around technical experts.

HIGHLIGHT

THE HERO MODEL

During our interviews, we asked for recommendations of other people we should talk to. Many interviewees recommended us speaking to the same individuals, who clearly play a key role within the support provision community, and who have wide networks.

The number of times that these people were recommended to us suggests that they are likely to receive a lot of requests for support, and, more broadly, that this approach of support provision cannot be scaled.

One interviewee described this structure as having a "hero model" where particular people are seen as the "heros". This makes it difficult for newcomers to join these support providers, and creates bottlenecks around how much support they can provide. Some of the recommended individuals explicitly identified needing more support from community managers, or people who could triage requests – suggesting that **the hero model isn't working for anyone, least of all them.**

As of 2017, a particular serious consequence of the **hero model** has come to light: that of abuse of power. A concentration of power without accountability checks and balances in place is unhealthy in any community, and the cases alleging sexual assault that have been reported in the last few months demonstrate that point, with devastating consequences[21].

Multiple interviewees told us about the need for support providers who had enough technical expertise and confidence to speak with people when they needed digital security support or were feeling threatened. Many had first- or second-hand experience of coming into contact directly with people who prioritised technical solutions over emotional ones, and the resulting negative effects on their motivation and well-being.

Some labelled these roles as “translators” or “technological guardians”, while others described them as “matchmakers” who could understand needs and facilitate the relationship between a more technical support provider and a recipient. Still others described the role simply as an “intermediary” between tool developers and end users who can aggregate patterns and figure out major pain points.

The lack of diversity in the digital security support community means that tools, resources and spaces are created predominantly for certain types of users, and not for others. This is to the detriment of their use and effectiveness.

Interviewees cited barriers in providing useful resources for the communities they worked with – “there are so many communities where there are no tools in the local language, or no tools appropriate for the context – like tools that need a strong internet connection to work, or tools that can only be accessed on desktop.”

Others mentioned that the most prominent use cases that get raised come from a relatively homogenous, white, male-dominated community, meaning that the problems that are worked on might not be the most pressing digital security problems, but rather those that affect people present in the digital security community. The support community was described as being like an “inner circle” of people who “have time to go to conferences, travel internationally, and create resources” – making it hard for newcomers, especially less well-resourced ones, to join.

CASE STUDY

CONTEXT-DRIVEN SECURITY SUPPORT

Key learning: Digital security support providers who are able to understand the issues of the communities they seek to support are sought-after and perceived as better able to deliver appropriate digital security support.

The Proteus Fund is an intermediary funder based in the United States that channels funding from foundations and individual donors in strategic ways to support progressive advocacy work.

The Security & Rights Collaborative is an initiative of the Proteus Fund that raises money for and grants funds to foster Muslim, Arab, and South Asian (MASA) organising and policy/advocacy efforts in the U.S. and provides strategic support and technical assistance to the wider MASA field. In 2016 and 2017, the SRC sought out digital security support for their grantees, and described how they prioritised finding a support provider who could be “someone from the same community because they could connect more – there’s a shared experience”, particularly with regards to understanding the intersection of physical attacks with digital attacks for MASA organisers and communities. They wanted “not only a digital security expert, but someone who is able to really engage with our grantees”, and ended up choosing a South Asian American Human Rights group to lead a project on digital safety and security.

2. Organisational journeys

To properly assess and understand the **digital security support ecosystem**, we sought to first understand **civil society needs** from this support system, from an organisational and institutional perspective.

We prioritised a problem-first approach, seeking to identify needs and behaviours around these. In response to this, we identify here three typical organisation archetypes, classifying them in terms of the priority they give to **promoting healthy digital security practices:**

- Unaware: where digital security is not a priority
- Learning: where digital security has been identified as a growing priority
- Mastering: where digital security is a high priority

Digital security is multi-faceted, meaning that an organisation could move from "Unaware" to "Learning" to "Mastering" in one particular aspect, but still be classified as "Unaware" in another aspect.

Example: A civil society organisation realises that someone is trying to access their Wordpress site, which has hundreds of users with various levels of user permissions.

- [UNAWARE] In the past, they've welcomed anyone who wanted to contribute to their site, and having a Wordpress account is part of the onboarding process.

- [LEARNING] They realise that having so many accounts means their system has more vulnerabilities than necessary. They aren't sure which accounts are still active and who actually needs certain user permissions, so they carry out an audit to understand the current status.

- [MASTERING] They make a policy to define what kinds of users need what kinds of permissions. They explain this to everyone in the organisation, along with the motivation for this policy, and everyone is on board with implementing it. From now on, new users are assigned the lowest level necessary of permissions, they review user accounts every few months, and they regularly delete inactive accounts.

In this way, they have moved along the cycle of healthy digital security practice in one particular aspect, but there are many more behaviours to encourage and support.

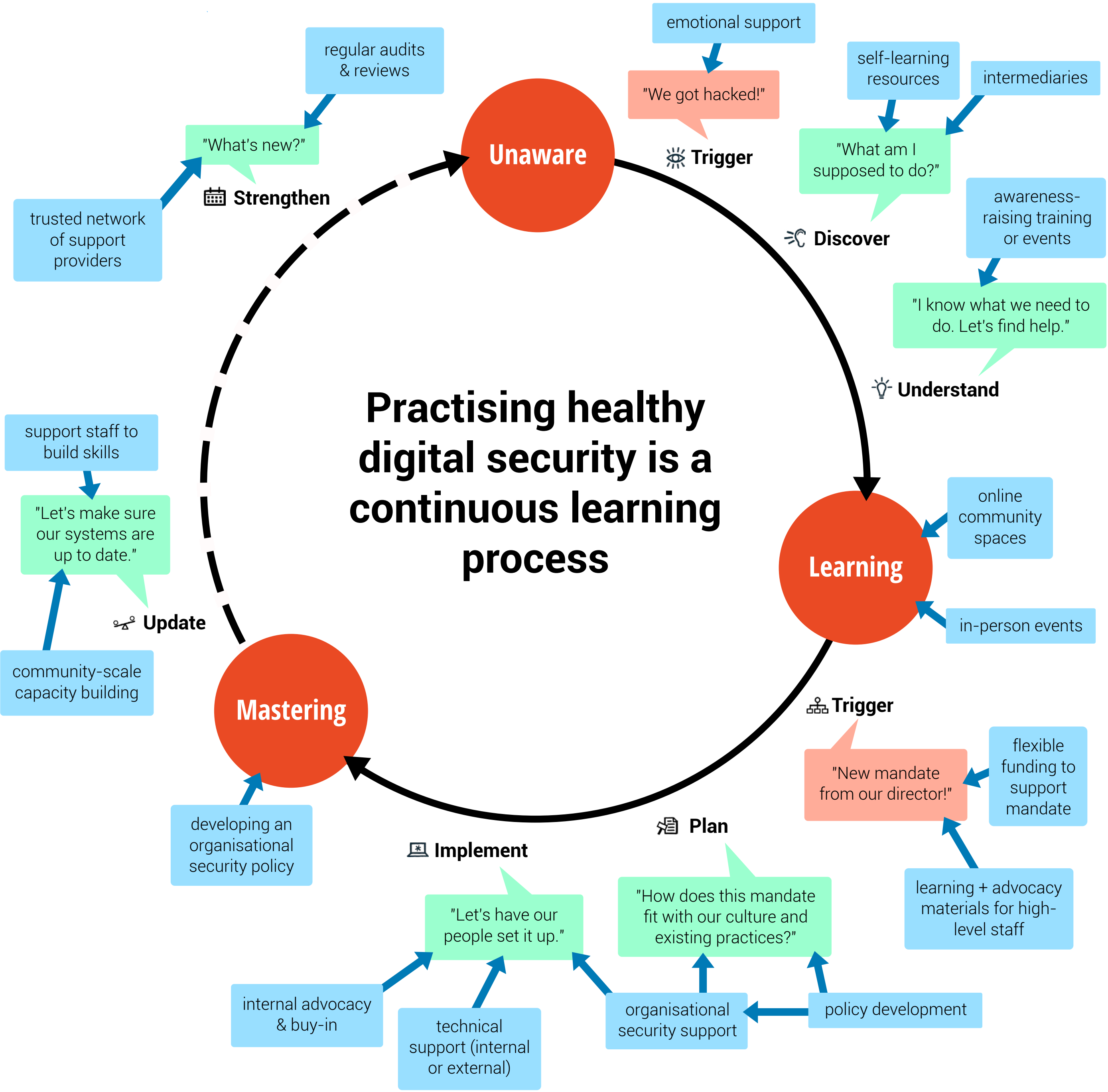
Example: A civil society organisation learns that a peer organisation has recently been the target of a phishing attack – an email was sent to multiple members of the organisation, pretending to be a company that they engaged with regularly. They're not sure whether this was a targeted attack, but all the same, they worry that they might be subject to the same kind of attack.

- [UNAWARE] In the past, staff members would click on links from external companies without checking the legitimacy of that link, or of the sender.

- [LEARNING] They realise that this might put them (and the communities they work with, as they hold sensitive information about those communities on their work computers) at risk. As a first step, they ask everyone to forward emails which mention this company to a malware researcher who they are working with, and they carry out awareness raising trainings to help staff members notice triggers that

DIGITAL SECURITY CYCLES FOR ORGANISATIONS

🟥 **triggers**
🟩 **organisation status update**
🟦 **support interventions**



Practising healthy digital security is a continuous learning process
Unaware
emotional support
"We got hacked!"
Trigger
self-learning resources
intermediaries
"What am I supposed to do?"
Discover
awareness-raising training or events
"I know what we need to do. Let's find help."
Understand
Learning
online community spaces
in-person events
Trigger
"New mandate from our director!"
flexible funding to support mandate
learning + advocacy materials for high-level staff
Plan
"How does this mandate fit with our culture and existing practices?"
organisational security support
policy development
Implement
"Let's have our people set it up."
internal advocacy & buy-in
technical support (internal or external)
Mastering
developing an organisational security policy
Update
"Let's make sure our systems are up to date."
support staff to build skills
community-scale capacity building
Strengthen
"What's new?"
regular audits & reviews
trusted network of support providers

Digital security is multi-faceted, meaning that an organisation could move from **Unaware** to **Learning** to **Mastering** with regards to one particular practice, but still be classified as **Unaware** in another practice.

First published March 2018. Created by The Engine Room with support from the Ford Foundation, designed by Jason Li. This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

can indicate phishing attacks rather than emails from the actual sender.

- [MASTERING] Detecting phishing attacks becomes part of the regular onboarding process for new staff members; all staff members know who to forward suspected attacks to, and how to detect phishing emails, and they publish a step-by-step guide for anyone who needs refresher information – also documenting and demonstrating their process to inspire other peer organisations to do the same.

Example: A civil society organisation holds personal data about the immigration status of people they work with, and the political context changes drastically with regards to immigration. This means that the data they hold is suddenly very sensitive, and could put a lot of people at risk if it were made public somehow – and that they now have more adversaries who are potentially seeking to obtain this data.

- [UNAWARE] Previously, they understood that this data could be sensitive but they decided that collecting data on immigration status better equipped them to understand their communities, and be able to serve their needs. They stored it on a shared hard-drive, but as the organisation grew, more and more people ended up needing access and made copies on their own computers for ease of access.

- [LEARNING] They realise that in the current climate, even holding this data is dangerous. They get in touch with an de-identification specialist who comes recommended from one of their staff members, who looks at a subset of the data and advises them to delete most items except for the ones they really need. They ask all staff members to delete all the data from their own computers, explaining why this is so important. They follow the advice of the specialist and save the remaining data on two hard-drives which they encrypt with passwords that only a couple of people in the organisation know.

- [MASTERING] From now on, they practice 'data minimisation' – only collecting the data they really need. To get access to the database, staff have to ask one of three people to put the password in, and the database is vastly reduced from the original version. They routinely change the password, and both hard-drives are kept in physically secure facilities.

In this way, they have moved along the cycle of healthy digital security practice in one particular aspect, but there are many more behaviours to encourage and support.

2.1 UNAWARE ORGANISATIONS

Story: An archetypal ***unaware*** *organisation has no core tech staff members. Their staff don't consider themselves as 'tech-literate' enough to address issues of digital security, and they have low or no awareness of digital security and no budget dedicated to digital security. When it comes to technology, their priorities are convenience and/or past experience – tools that people are already familiar with. They tend to use out-of-the-box tech solutions, and as an example, they might not have turned on Two-Factor Authentication, if it's not automatically done.*

Getting to grips with digital security

The biggest barrier limiting the building of better digital security practices among civil society was a general lack of understanding of what digital security entails.

The consequences of this gap in understanding are far-reaching, and include:

- General under-prioritisation of digital security within organisational priorities (budget, staff, policy implementation) – often done without realising how digital security intersects with and affects implementation of other core priorities.

- Insecure and unsafe digital technology practices within organisations (for example, sharing passwords, storing sensitive data in easily accessible places, or not updating software regularly).

- Inappropriate partners or commercial providers being contracted to provide technical support, potentially leading to inappropriate advice or unsustainable security practices.

- Lack of support for individuals within an organisation looking to boost digital security practices – whether that be professional development opportunities for those responsible for digital security, or the unintended creation of barriers for those individuals to implement better digital security practices within an organisation.

ATTACKS FACED BY NON-PROFITS

Interviewees described seeing first or second-hand various types of threats faced by non-profits, including:

- Crypto-ransomware, where files are taken control of and only released upon payment via particular malicious software (known as malware). If this happens, the person under attack sees a message asking for a ransom to be paid in order to regain access to their computer and files.

- Data breaches, either general or specifically at particularly opportune moments, like in the weeks before a major community event.

- Physical raids on offices

- Legal threats – using particular legal instruments to shut organisations down or point out to authorities that an organisation might be overstepping their 'non-lobbying' status (ie. 501(c)3 organisations in the United States)

- Phishing emails[22]

- Targeted malware

- General viruses – from a field-wide survey conducted by Idealware with the Immigration Advocates Network in June 2016 on the technology needs of immigration rights groups, 20% of participants said that their organisation's computers had been infected in the past year with viruses.[23]

Many interviewees told us that digital security has traditionally been perceived as a purely technical act and intervention, with many resources or tools seen as inaccessible or unfriendly to those without technical backgrounds. Interviewees identified tech and security as "intimidating and out of their realm", while technical digital security experts were described as being "not very approachable".

This approach was also prevalent in the way in which digital security communities are perceived. This creates a barrier for newcomers looking to join and learn from digital security-focused communities..

For mission-based organisations in the unaware category, spending money on digital security is a low priority. Other, more visible priorities take precedence (like directing money to affected communities, or staff). This affects the impact that funders can have when they want their grantees to spend money on digital security but do not explicitly earmark those funds. If support after awareness isn't encouraged, considering digital security can feel like a box-ticking exercise to the grantee.

Strengthening an institution's digital security can often be far less tangible and visible than supporting either other types of security (for example, physical security) – or directing resources towards affected communities.

Moving from Unaware to Learning

Generally speaking, there tends to be a particular trigger that spurs this transition. This might be any of the following:

- Experiencing an attack or digital security breach first-hand – motivation starts from a place of fear

- Learning of peers experiencing digital security breaches

- Dramatic changes in political context, resulting in dramatic changes in how an organisation perceives their own position.

Useful types of support

When people or organisations are moving from "Unaware" to "Learning" (particularly if it is motivated by fear or risk of attack), experts who can provide emotional support are more helpful as the first port of call than technical experts.

Community managers, and first responders who can successfully triage needs are particularly necessary at this stage, for a number of reasons:

- To provide a more welcoming experience for individuals + organisations who are moving from "Unaware" to "Learning".

- To reduce the amount of work falling to technical experts, and enable them to work on the cases in which their particular technical expertise is most relevant.

- To make support provision more scalable and accessible to newcomers, and to increase the likelihood of newcomers entering the provision space.

CASE STUDY

UNDERSTANDING EMOTIONAL NEEDS

Key Learning: emotional support can be just as valuable and needed as technical interventions in addressing digital security threats.

People from within the Global Voices network sometimes reach out to core staff after experiencing digital security breaches or threats. Their Advocacy Director shared a key learning, after having dealt with multiple people who required support:

"We've learned that when people when reach out they need to be heard, not to be told to do a technical thing."

The approach of focusing only on technical experts was highlighted most clearly in our interview phase, during which many interviewees recommended the same (largely technical) experts as providing useful digital security support, or as experts we should speak with.

For digital security resources to be effective at the stage of moving from "Unaware" to "Learning", they need to be practical, actionable and achievable. Many existing resources around digital security are written for largely "general" audiences, and in their attempt to appeal to everybody they end up appealing to nobody.

Particular critiques raised mentioned that some resources describe tasks and digital security support as "easy" or "simple", thus making people who struggle with those tasks feel like they are not qualified enough to move on to further steps.

CASE STUDY

SECURITY WITHOUT BORDERS

Key Learning: Dedicated community management is a key part of developing healthy communities – and carrying out good community management requires a different set of skills to contributing technical expertise to the community itself.

Security Without Borders was set up in 2016[24], and was cited by many as a hugely useful resource. It is an open collective of hackers and security professionals who provide technical assistance to civil society and activists that are dedicated to the protection of fundamental human rights. It was founded with the goal to enable security professionals (from the private sector) to play a collaborative role in civil society[25]. One of the core team members told us:

"There was a lot of dysfunction at the beginning, with hundreds of people wanting to do stuff. It took a while to have that phase out, and now we have a core people that are committed to remain... There's a bigger priority: figuring out how to deal with people. We haven't found a good way to manage ourselves and others. We do it in our free time and none of us are good community managers."

Their diagnosis: **having a community manager** would vastly increase their effectiveness as a network, helping them to:

- Design effective processes for intake.
- Have initial triage calls to understand what people's needs are, and the type of expertise or security support they need.
- Organise people who want to contribute their expertise and design lightweight but helpful for them to contribute their expertise.

Resources aimed explicitly at beginners exist, and many of them seem to have been created relatively recently (in the last year or so). Notable examples include Martin Shelton's Signal for Beginners[26], or, more recently, Citizen Lab resources Net Alert, with "easy tips for keeping your accounts safe[27]", or their

Security Planner, encouraging people to "'improve your online safety with advice from experts."[28]

Resources and digital security support provision does not currently recognise generational differences in needs and approaches, and tend to be aimed at younger audiences. This creates a barrier for people in positions of leadership at organisations who are from older generations, and who have few options available designed explicitly for their experience.

In many organisations, people in positions of leadership are older people with more experience of the sector, and potentially (though not always) less experience of technology to their younger colleagues. For internal champions looking to push digital security higher in an organisation's priorities, convincing those at the highest decision-making levels of the organisation can be a big barrier.[29]

Trust is key. Building a healthy support ecosystem requires civil society organisations to build up relationships with support providers as an ongoing practice. This is because,for many groups (particularly mission-driven, or vulnerable communities), digital security support provision is dependent upon existing trust relationships.

As Bex Hurwitz from Research Action Design told us, the first port of call for organisations needing any kind of support – particularly security-related support – is people that they trust. As a result, some support providers build this in explicitly to the way in which they provide support, making sure to "keep moving at a pace where we can keep and build trust over time."

Interviewees noted a reluctance among communities they worked with in reaching out to organisations perceived as focusing on digital security, saying "it's unlikely that folks would go out of their way to find resources, or reach out to folks focused specifically on digital security."

Strengthening digital security support provision capacities in frontline communities requires supporting their well-being over time, as well as boosting their technical knowledge. In order for people to feel comfortable learning about digital security, they need their general human resources needs to be taken care of, such as regular financial income, and general labour rights.

2.2 LEARNING

CASE STUDY

– BOOSTING TECHNICAL CAPACITY AND HUMAN RESOURCES

Key Learning: Healthy digital security practices and community contributions can be boosted by taking general well-being into account, through operational support and human resources support.

Wellstone is a progressive advocacy organisation that trains community organisers, student activists, campaign staff, progressive candidates and elected officials. Through their Movement Technology program, Wellstone also work with organisational partners to train their staff or members in digital security.

They prioritise both boosting technical capacity and providing human resources support , focusing on logistics and community care. Their focus on the operational backbone of network- and community-building allows them to ensure that their staff and adjunct trainers can get paid on time, and can receive support on the logistics of carrying out a training, as well as other human resources support that enables them to stay in the community.

Of note, too, is that Wellstone were one of few security providers we spoke to who provide financial support for people to attend their trainings and build their skills. Usually, getting the chance to attend a training, or a training-of-trainers, is presented as an unpaid opportunity to boost one's skills.

Story: Within a typical organisation at the 'learning' stage, at least one staff member is aware of the importance of digital security, and is looking for ways to boost digisec within the organisation. Their priorities are internal advocacy as well as boosting own knowledge and skills. They might have received a training or two, and be feeling a little overwhelmed with advice and uncertainty about *how to implement it. They use existing/online resources to learn more about digital security.*

The trigger for moving from "Unaware" to "Learning" is often convincing leadership of the importance of digisec and getting their active buy-in; finding budget from a project to work on the issue; or another outside factor such as peer-pressure, or funder-pressure. At this stage, self-learning resources are helpful, as are in-person events, documentation from peers of how they have addressed issues of digital security, and more.

Support interventions

The typical way in which resources and guides around digital security are produced often fails to reflect the speed with which their content can change. Without a dedicated community to keep them updated, static resources go out of date fast. As a result, it can be difficult for users to know if existing resources are still applicable.

Producing new resources without a long-term, ongoing plan for updates and clearly stated ownership and accountability structures, is not contributing to a healthy support ecosystem.

Resources have typically been produced as static PDF files, or more recently, as websites, or articles. Due to the quickly-changing nature of the digital security space, content requires regular updates, and a way of flagging unsuitable content. However, few are rarely explicitly labelled with their latest date of update.

Interviewees we spoke with cited the most popular digital security support resources as being Security in a Box[30] (SIAB), by Tactical Technology Collective and Frontline Defenders, and Surveillance Self-Defense[31] (SSD) by the Electronic Frontier Foundation. In the case of SIAB, however, some interviewees mentioned not knowing if or who was still updating the content (as a metric, at the time of writing in January 2018, the latest blog post is from April 2016) – or, having emailed the contact address given to notify them of out of date advice, and not receiving a response.

Many of these concerns could be addressed with a comprehensive communications plan alongside the resource itself. As we found through our desk research, websites sharing resources are often not kept up to date or shared with information that would vastly increase their usability, such as "date of last update." As of 2017, best practices around sharing resources include envisioning an "Expiration Date" for the resource itself[33]; and having a clear and actively maintained process for reporting errors in the content.

CASE STUDY

PRODUCING RESOURCES IN MORE DYNAMIC, EASY-TO-UPDATE WAYS

Key Learning: digital security resources need updating regularly; so producing them in formats that are easy to update and share (such as websites, rather than PDFs) is a good design principle.

One interviewee told us of how they initially began producing digital security resources as PDFs to pass around the community. At one point, a translator got in touch to tell them they had completed a translation of one of the resources. However, the guide that had been translated was four years old, and entirely out of date.

Not being able to flag the content as out of date (particularly for PDFs which might be emailed around as attachments, independent of the website they are hosted on) – meant that resources had been wasted in translating the guide. After this incident, the interviewee now prefers to create resources as webpages, and link users to it so that if things do change, the page can be updated and users will see the most up to date version.

It is also worth noting, that though these guides are written for a general audience, interviewees from outside the United States and Europe mentioned that much of the advice given was not relevant in their contexts, as well as some support providers who work explicitly with frontline civil society organisations. Many existing resources are not specific about their target audience, but make a number of assumptions which exclude particular communities. One interviewee told us:

"In reality, there's nothing in traditional digisec for a lot of the groups I work with. I've done digisec trainings in US, and there is very little you can tell trans women of colour doing sex work about digital security – physical security needs to be baked in from the start, and it's not in traditional digisec."

Some efforts have been made by other groups to meet these more context-specific needs, such as:

- Hackblossom's DIY Cybersecurity for Domestic Violence[33]
- Cibermujeres, a digital self-defense guide for women human right defenders that work in high-risk environments.[34]
- How to Encrypt and Urgently Wipe your Data Securely for activists working in the Gulf region[35]

(Note: the above is a non-exhaustive list of context-specific digital security advice, intended to illustrate the concept rather than provide all possible resources.)

Additionally, some resources are emerging that are designed in a more interactive way, allowing viewers to receive advice tailored to their specific contexts, such as Security Planner by Citizen Lab[36]. At the time of writing in January 2018, the planner is available in English only, with Spanish and French-language versions planned. It also follows the above-mentioned best practice of clearly noting the date of last update.

Learning about risks and threats faced without having the agency or capacity to implement solutions against those threats is unhelpful. Just becoming aware of risks can lead to more fear and/or stop people from engaging with data and technology at all.

Interviewees described how receiving digital security support without thought as to their existing capacity or knowledge can "scare people into paralysis and turn into fear-mongering." Another described how they saw civil society organisations being encouraged to attend webinars and trainings by funders, despite the fact that they didn't have capacity to attend large numbers of one-off events or implement any of the practices that were recommended.

Organisations seeking to boost their own digital security capacity need to be able to invest in their operational infrastructure. Otherwise, they will not be able to invest in solutions they might find out about. This could be addressed by explicit support through core grants.

Organisations receiving core support at the 'learning' stage might well have extra demands related to their technical infrastructure or digital security, which often might not fit into project budgets. Without core funds to invest in these solutions, they will struggle to be able to operationalise digital security support, and develop a digital security-minded organisational culture.

For example, according to a study done by Idealware and the Immigration Advocates Network on the technology needs of immigration rights groups, 26% of staff share a computer, and nearly 52% don't back files up regularly.[37]

Digital security, together

Due to the networked nature of digital technologies, digital security practices need to be framed as collective actions over time in order to be effective. Individual actions are not enough.

Existing resources and digital security advice often provides support that is only helpful if those around you are also practising the same behaviour, focusing on the individual rather than the group.

Examples of this individual-focused advice are, for example:

- Set up PGP – but if you're the only one using it, PGP will not be helpful for you or those around you

- Download Signal – similarly, if none of your contacts are on Signal, you can use it but your conversations won't be encrypted.

- Encrypt your hard-drive – if lots of people have access to the same information and none of them also encrypt their hard-drive, one encrypted hard-drive will not ultimately secure the information.

For digital security support interventions to form part of healthy institution-building, they should be framed not as one-off interventions, but as part of an organisational security approach.

As Becky Kazansky writes about her work with digital security approaches for women human rights defenders, "Encouraging an emphasis on the individual as the primary locus of responsibility for protection from harm had the convenient effect of deflecting attention from its causes."[38] In contrast to promoting individual actions, taking an organisational security approach acknowledges the collective nature of digital security, and builds upon existing culture, context, habits and practices to build up long-term organisational capacity. It also takes context into account and enables people to design interventions which connect healthy security practices with the mission of the organisation.[39]

CASE STUDY

BOOSTING ORGANISATIONAL SECURITY

Key Learning: Providing community space for people responsible for boosting digital security of organisations is a good way of facilitating learnings across borders and organisations, and providing peer support for people who often find themselves working alone.

The orgsec community[40] is a community of practice that works to strengthen human right defenders and civil society organisations' awareness, ability and confidence in thwarting security threats. The first convening of 15 practitioners took place in early 2016, and since the network has grown to include over 100 members from all over the world.

Organisational security support comprises a complex, evolving and multifaceted process that cycles organisations through a series of phases: discovery, strategy, implementation, and trust-building, accompanied by an orgsec practitioner over a series of months or, in some cases, years of support.

Now, it is an invite-only listserv which acts as a discussion group for sharing experiences and building standardised, accessible approaches to organisational security. They share resources, challenges, best practices and learnings from their various approaches and ongoing work.

Moving from "Learning" to "Mastering"

There is a serious lack of institutional support for people from underrepresented communities who are providing digital security support for their communities and organisations. The lack of support makes it difficult for them to engage with the broader digital security community – and as a result, their work and expertise are not valued and appreciated by the community.

Providing institutional support and opportunities for professional development for people operating outside of the most visible digital security support providers will enable them both to grow in their ability to provide support, but also in diversifying the digital security community as a whole.

Organisations who have gone through a digital security learning cycle could also think about boosting better longer-term health of communities they are a part of. This might mean:

- Taking time to document the process they went through
- Actively supporting or mentoring peer organisations that have less advanced digital security skills
- Sharing learnings in community spaces to raise awareness of digital security needs, for peer organisations and others
- Providing spaces for people from under-represented communities to learn more about digital security and move into the 'provision' space

2.2 MASTERING

Story: With a typical organisation who is at the 'mastering' stage, there is buy-in from leadership of importance of digital security and appropriate budget dedicated to ensuring that the organisation has secure systems and technology support. For some organisations, this might mean having an internal person on staff who is mandated with digital security for the organisation, and policies have been developed (and followed) around data management, with staff willing to compromise slightly on ease of use for security reasons. This kind of organisation is willing to invest funds (such as on commercial providers) if that's the best option, and strives to make intentional choices around tech tools and systems.

Continuous learning

Moving into operationalising and implementing healthy digital security practices can mean very different things for different organisations. Generally, it will be a cyclical series of practices rather than a one-off action. As a result, organisations at this stage need to dedicate continuing resources to digital security and be aware that there is always more to learn.

Good advice for one organisation might be useless for another. This makes judging the quality of support very context-specific.

See visual metaphor. If the building you are in has no sprinkler system installed, receiving the advice "turn on the sprinklers" in case of an emergency makes no sense. Instead, the advice needs to be designed for the context in which the person is in, in order to be useful and operational.

There is a perceived lack of availability of funding for maintenance and long-term support. As a result, organisations will pitch new interventions rather than ongoing ones, despite ongoing interventions often being more useful.

One interviewee told us that the key learning for supporting organisations to implement digital security practices is to make digital security "as much of a priority as budgets, financing, and staffing questions."

This perception was also raised by those working in areas of technical infrastructure, who mentioned that they found fundraising difficult. In turn a lack of resources made it difficult for these groups to be able to provide support to the civil society groups who depend upon them.

CASE STUDY

DIGITAL SECURITY THREATS IN NEPAL

Key Learning: Understanding cultural and social context can drastically change the digital security advice offered in the face of threats.

Citizen Lab's report, Targeted Threats[41], looked at the digital security threats faced by various organisations. Below, they describe one digital security support intervention carried out by organisations in Tibet:

"For example, some Tibetan groups have been promoting a "Detach from Attachments" campaign that encourages users to move away from sharing documents through email attachments and shift to alternative cloud-based platforms like Google Drive. The campaign uses a mix of humor and references to Tibetan culture and is a good example of user education that is connected to a specific threat model and local context.... based on what we have seen, the campaign could be effective against some of the current threats against the Tibetan community. More than 80% of malware submitted to us by Tibet Groups used a malicious email attachment. Furthermore, for two of the Tibet Groups in our study, simply not opening attachments would mitigate more than 95% of targeted malware threats that use email as a vector."

For these Tibetan groups, adjusting their practices to respond to their most prominent threat – that of phishing attacks transmitted through email attachments – would be an effective way of practising healthy digital security practices. In order for the digital security support community to know this, however, they would need to understand the context in which these groups are operating, and how to encourage these behaviours in a culturally appropriate way, as the "Detach from Attachments" campaign seems to do.

3. RECOMMENDATIONS

Recommendations in this section focus on what funders could do to support and encourage the development of a healthy digital security support ecosystem.

These recommendations are drawn from interviews with digital security support providers, digital security experts, and recipients of digital security support, with a particular focus on the United States. All recommendations are responses to problems raised consistently and repeatedly by interviewees, suggestions directly from multiple interviewees, or drawn from digital security challenges observed over time through The Engine Room's own experience over the past six years as a support organisation for civil society.

3.1 RECOMMENDATIONS FOR FUNDERS

This report seeks to paint a picture of what the current gaps are between digital security support and civil society needs with a view to informing better philanthropic practices across the board.

Digital security must be prioritised by philanthropy writ large, in order for civil society to continue growing its dependence upon technology in a way that doesn't put them, and the constituencies they seek to support, at risk.

Build digital security in as a core issue within grantmaking

As digital security continues to be a key concern, proactively gathering information from grantees (particularly high-risk grantees, but also others for whom digital security may not yet be on their radar) would send a signal that funders at all levels are taking security seriously.

The Digital Security & Grantcraft Guide[42] is an excellent example of what is possible when funders at more advanced stages tackling an issue produce actionable insights for other foundations. It is also a good example of an organisation sharing their learnings after having progressed along the "unaware -> learning -> mastering" cycle, by defining a potential path for progression for other funders to see.

More could be done to encourage uptake and use of the guide among other funders – such as webinars with networks or groups of funders, like the one held for the Transparency and Accountability Initiative, or more development of actionable materials from the guide for other grantmakers to use.

Better supporting existing grantees

The following suggestions are aimed at elevating and supporting organisations who do invest in their organisations to contribute to community-wide learning.

- **Reward organisations who make great strides in security** and continue to invest in their growth, by increasing their core funding over time. Build in mechanisms to flag who these organisations are.
- **Support them in conducting better monitoring and evaluation mechanisms for digital security support providers** beyond simply counting the number of people attending an event, or the number of downloads of a particular guide.
- **Encourage these organisations to document the process** of how they have boosted their organisational security capacity, providing examples for other peer organisations, and

contributing to community-scale knowledge and capacity building.

- **Actively prioritise security support**: include security as a core area of support when working with organisations to craft general support budgets.

Informing investments in the digital security support space

As mentioned in this report, types of support have evolved over time. Philanthropy could learn from these evolutions and adjust the types of interventions that are supported as a result.

- **Reduce funding for generalised guides and generalised resource websites:** as described in this report, “all-purpose” resources are not meeting the needs of any particular group, with many finding them not specific enough for their context. Instead, identify key communities and groups in need of resources, and institutions best placed to understand their needs and design resources accordingly.

- **Fund projects that interlink investigation into attacks on civil society, strategic litigation, technical development, and user-centred support:** digital security is not a standalone support mechanism, and needs to be linked with other key institutional foundations to be successful.

- **Support better user experience of privacy-respecting tools:** one major barrier to the uptake of open source tools is the fact that they are not perceived as user-friendly. Though digital security support should be focused on processes rather than tools, it is possible to support the ecosystem by ensuring that there are tools available that are regularly maintained, audited, and have actively built in a smooth and accessible user experience.

As mentioned in the report, investing in the supply side of traditional end user security training is insufficient to support security gains for social change organisations. Trainings can be an awareness-raising intervention, but in terms of practical support, often fall short. In particular, trainings can be a waste of time and resources for organisations if they:

- are not part of a larger strategy of support and change

- are limited to highly technical interventions

- do not address the usability and technology needs of social change organisations

- do not connect to cultural, political, and social needs

- leave a participant feeling overwhelmed, alone within their organisation, or unsure of how changes in end user use for the individual connect to organisational solutions.

As a response to that, we encourage trainings only if and when they are a part of a longer-term support mechanism and ecosystem strategy.

Coordination between funders

Interviewees cited receiving conflicting or overlapping information from funders regarding digital security as a barrier to knowing what to do next.

- **Encourage better coordination between funders** of support provided to grantees, and support advice offered. Interviewees mentioned a lack of coordination between funders resulting in grantees receiving conflicting advice, or sometimes being encouraged to go to multiple trainings within a short amount of time, but without support for implementation.

- **Synchronise efforts with other foundations (beyond of just Chief Information Officers) on investigating and preventing attacks and training staff** - in the same way that staff are increasingly being supported to understand financial management, communications and strategy. Beyond gathering a database of attacks on a foundation-by-foundation basis, there may also be space to do the same for a wider network of funders, enabling a more comprehensive analysis of the civil society space and consequently, better-informed response strategies.

CONCLUSION

This report focuses on understanding digital security from an organisational perspective, and suggests ways in which the digital security support ecosystem could evolve to meet civil society's needs. Civil society's reliance on digital technologies is growing, and our approach to digital security needs to grow in parallel. It is clear that digital security is contextual – one size, or set of advice, does not fit all. Culture, customs and behaviour affect the way in which digital security support is provided and received.

Above all, it is clear from this work that the support ecosystem needs to grow and value different types of expertise. This expertise needs to be triaged by people with the contextual and technical knowledge required to know who to recommend, ensuring that different kinds of experts can plug in where they are most helpful. We need better ways of understanding the impact of digital security support; more people who feel comfortable talking about digital security; and context-driven approaches to boosting digital security.

For civil society organisations to continue operating at scale, we must begin developing healthy behaviours around digital security at all levels, from using and developing user-friendly, secure technology tools, to storing data securely, and, above all, developing an organisational culture that integrates digital security. For that to happen, we need the digital security support ecosystem to evolve, learn from past mistakes, and be increasingly comprised of the communities it aims to support.

METHODOLOGY

This report is based on a review of the current digital security ecosystem, relevant literature and resources, and interviews with recipients of digital security support and digital security support providers (including individuals working as digital security experts, trainers, (commercial) IT providers and funders). The research was complemented by desk research throughout the process.

The interviewees were identified through The Engine Room's networks, recommendations from interviewees, and on the basis of desk research. The majority (23) of interviewees work in the United States, while the remaining group of interviewees (12) work internationally. The interviews were conducted in English, from June through August 2017. A total of 35 semi-structured interviews were conducted, and the interviews were complemented by observation of digital security workshops and trainings; attendance at various events where digital security support was discussed, and informal conversations with a wide range of people.

This report aims to identify the gaps and needs in the current digital security support ecosystem in the United States. The results are based on a small sample of interviewees, and is therefore not comprehensive. However, we hope that the report can contribute to a better understanding of the current digital security needs of civil society in the United States.

ACKNOWLEDGEMENTS

We offer our sincere thanks to the many people who generously offered their time and wisdom to us during this project; those with whom we conducted official interviews, who contributed to the body of research we read, appreciated and built upon, and who we spoke to us in informal conversations.

People who were interviewed for “Ties That Bind”, and gave their consent to be included in this list, are: Micah Anderson; Sarah Aoun; Jack Aponte; Matthew Burnett; Michael Carbone; Claire Downing; Ryan Gerety; Daniel Kahn Gillmor; Claudio Guarnieri; guido; Bex Hurwitz; Lisa Jervis; Dragana Kaurin; Dia Kayalli; Noah Kelley; Mark Kiggundu; Tania Lee; Josh Levy; Rickke Mananzala; Jordan McCarthy; Matt Mitchell; Azeenarh Mohammed; Ken Montenegro; Joshua Peskay; Lisa Rau; Aliya Rahman; Jonah Silas; and Dan Staples.

The Internet Freedom team at the Ford Foundation offered invaluable support and guidance throughout the process, and we are grateful for the opportunity to have worked on this project. Any errors remain the authors’ responsibility alone.

NOTES

[1] For more on the role that race, sexuality and gender play in surveillance, refer to Rachel E. Dubrofsky and Shoshana Amielle Magnet (eds.) Feminist Surveillance Studies. Duke University Press, 2015: https://www.dukeupress.edu/feminist-surveillance-studies.

[2] Martin Shelton, Current Digital Security Resources, 19 December 2016: https://medium.com/@mshelton/current-digital-security-resources-5c88ba40ce5c.

[3] Activate, 2016 Tech and Media Outlook, 2016: http://www.slideshare.net/ActivateInc/activate-tech-and-media-outlook-2016/2-Over_the_next_ five_years.

[4] ICRC, The Engine Room and Block Party, Humanitarian Futures for Messaging Apps, January 2017, p. 20: https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

[5] Sean McDonald, WhatsApp, Trust, & Trusts, 27 August 2016: https://medium.com/@McDapper/whatsapp- trust-trusts-980ec18d71b2#.cs9pv6hxp.

[6] Natasha Lomas, "Security researchers call for Guardian to retract false WhatsApp "backdoor" story", TechCrunch, 20 January 2017: https://techcrunch.com/2017/01/20/security-researchers-call-for-guardian-to-retract-false-whatsapp-backdoor-story/.

[7] A report released by Citizen Lab in 2014 identified needing to keep up to date with new technical developments and context-specific risks as being "challenging and time-consuming" for the civil society organisations they worked with. Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society, 11 November 2014, p. 122: https://targetedthreats.net.

[8] See, for example: Camila Bustos, "The Shrinking of Civic Spaces: What is Happening and What Can We Do?", Dejusticia, 17 April 2017: https://www.dejusticia.org/en/the-shrinking-of-civic-spaces-what-is-happening-and-what-can-we-do/.

[9] https://globalvoices.org/2017/10/26/after-113-days-behind-bars-istanbul10-human-rights-defenders-are-released-on-bail/

[10] Matt Burgess, "The 'real people' using encryption for privacy protection", Wired, 1 August 2017: http://www.wired.co.uk/article/uk-encryption-whatsapp-amber-rudd.

[11] Jeremy Malcolm, "Australian PM Calls for End-to-End Encryption Ban, Says the Laws of Mathematics Don't Apply Down Under", Electronic Frontier Foundation, 14 July 2017: https://www.eff.org/deeplinks/2017/07/australian-pm-calls-end-end-encryption-ban-says-laws-mathematics-dont-apply-down.

[12] Reuters, "France says fight against messaging encryption needs worldwide initiative", Reuters, 11 August 2016: http://www.reuters.com/article/us-france-internet-encryption-idUSKCN10M1KB.

[13] Eric Luchtblau and Katie Benner, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", New York Time, 17 February 2016: https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

[14] Kai Biermann, "Innenministerium sucht freiwillige Cyberfeuerwehr", Zeit Online, 6 October 2016: http://www.zeit.de/digital/datenschutz/2016-10/bsi-cyberangriff-it-sicherheit-feuerwehr-cyberwehr.

[15] See "For some HRDs, technology is not the root of their risk." Nah, Alice M., et al., "A Research Agenda for the Protection of Human Rights Defenders." Journal of Human Rights Practice, 2013, p. 415.

[16] https://theoutline.com/post/2489/two-passwords-are-always-better-than-one

[17] Tactical Tech, Holistic Security: https://holistic-security.tacticaltech.org/.

[18] The Electronic Frontier Foundation's Security Education Companion takes an explicit harm reduction approach, and provides a useful summary of some key principles: https://sec.eff.org/articles/harm-reduction

[19] For more on different types of trainings, see Waters, Carol. "Digital Security Trainers: Practices and Observations." Publication. Tactical Technology Collective, 2015. Web. 14 June 2017.

[20] For more information, see "Digital Security Concerns" in: The Engine Room, Technology Tools for Human Rights, September 2016, p. 10: https://www.theengineroom.org/wp-content/uploads/2017/01/technology-tools-in-human-rights_lower-quality.pdf.

[21] Trigger warning for detailed descriptions of sexual assault: https://www.theverge.com/2017/10/13/16473996/morgan-marquis-boire-citizen-lab-sexual-assault. https://citizenlab.ca/2017/10/open-letter-sexual-assault/

NOTES (CONT.)

[22] Described in more detail in Citizen Lab's Targeted Threats report. Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society, 11 November 2014: https://targetedthreats.net.

[23] Immigration Advocates Network and Idealware, Technology Needs Among Immigrant Rights and Immigration Legal Services Organizations: A Survey of the Field, August 2016: https://www.immigrationadvocates.org/link.cfm?25937

[24] Media.ccc.de, Hacking the World (33c3), 28 December 2016: https://www.youtube.com/watch?v=KF860QYZzUE.

[25] Security Without Borders, Transmission 1, 13 May 2017: https://securitywithoutborders.org/blog/2017/05/13/transmission-1.html.

[26] Martin Shelton, Signal for Beginners, 18 November 2016: https://medium.com/@mshelton/signal-for-beginners-c6b44f76a1f0#.3bocimnxj.

[27] Net Alert: https://netalert.me/.

[28] https://securityplanner.org/#/

[29] See "Barriers to sustained learning and implementation", Waters, Carol. "Digital Security Trainers: Practices and Observations." Publication. Tactical Technology Collective, 2015. Web. 14 June 2017

[30] Tactical Tech and Front Line Defenders, Security-in-A-Box - Digital security tools and tactics: https://securityinabox.org/en/.

[31] Electronic Frontier Foundation, Surveillance Self-Defense: https://ssd.eff.org/en.

[32] Matt Mitchell, Digital Security training resources for digital security trainers, Winter 2017 Edition, 19 November 2016: https://medium.com/@geminiimatt/security-training-resources-for-security-trainers-winter-2016-edition-4d10670ef8d3.

[33] Hackblossom, DIY Cybersecurity for Domestic Violence: https://hackblossom.org/domestic-violence/.

[34] https://cyber-women.com/en/#about

[35] https://bahrainwatch.org/amanatech/en/advice/how-to-store-and-wipe-your-data-securely

[36] https://securityplanner.org/#/

[37] Immigration Advocates Network and Idealware, Technology Needs Among Immigrant Rights and Immigration Legal Services Organizations: A Survey of the Field, August 2016, p. 8: https://www.immigrationadvocates.org/link.cfm?25937.

[38] Kazansky, Becky. "FCJ-195 Privacy, Responsibility, and Human Rights Activism." The Fibreculture Journal, 26, 2015: Entanglements–Activism and Technology (2015).

[39] For more on digital security as a set of practices, see Kazansky, Becky. "Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices." Publication. Tactical Technology Collective, 2015. Web. 14 June 2017.

[40] Orgsec community: https://Orgsec.community.

[41] Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society: https://targetedthreats.net/.

[42] Michael Brennan, Elizabeth Eagen, Bryan Nuñez, John Scott-Railton and Eric Sears, Digital Security & Grantcraft Guide: an Introduction Guide for Funders, March 2017: https://www.fordfoundation.org/library/reports-and-studies/digital-security-grantcraft-guide/.

THE
ENGINE
ROOM