DIGITAL SECURITY & GRANTCRAFT GUIDE

AN INTRODUCTORY GUIDE FOR FUNDERS

NETGAIN PARTNERSHIP

DIGITAL SECURITY & GRANTCRAFT GUIDE

AN INTRODUCTORY GUIDE FOR FUNDERS

Authors:
Michael Brennan, Technology Program Officer, Ford Foundation
Elizabeth Eagen, Program Officer, Open Society Foundations
Bryan Nuñez, Program Officer, Open Society Foundations
John Scott-Railton, Senior Researcher, The Citizen Lab, University of Toronto
Eric Sears, Senior Program Officer, MacArthur Foundation

In the digital age, grantmakers should be able to assess and, when appropriate, help address the digital security threats faced by grantees and grant applicants. Yet, because this is new terrain for most grantmakers, they are likely to experience a range of challenges. These challenges include:

- Not knowing where to start;
- Not understanding the language of information security;
- Feeling overwhelmed;
- Not knowing where to turn for advice;
- Being unsure of what to do in the face of digital security concerns;
- Clarifying and responding to interlocking acute and long term problems of digital and physical security;
- Convincing grantees to make changes in information technology where historically they have often been left to make their own decisions.

Good news: you can address, or at least mitigate, these challenges. The purpose of this guide is to help grantmakers both assess and address digital security concerns. The guide is divided into three sections.

- **Section 1** explores the scope of targeted digital threats against civil society and the constraints that hamper the ability to address them.
- **Section 2** describes how to conduct a digital security "triage" of grants to elevate the digital security of your whole grant portfolio; while playing special attention to the highest risk grantees.
- **Section 3** is the conclusion and provides suggestions for pathways to think more systematically about digital security as a part of grantcraft.

Digital security breaches can cause harm to grantees, as well as their clients, beneficiaries, and partner organizations. These threats also pose a risk to grantmakers and to the larger strategies of impacted organizations. Security leaks can compromise an organization's ability to carry out its work, and can erode trust between civil society actors. Though it can be difficult to get started, funders have an important role to play in starting conversations with grantees on digital security threats and ways to mitigate them.

Are you currently considering a proposal for digital security tools or training? If so, this is not the document for you. Evaluating a proposal that supports the development of digital security tools requires substantial technical expertise. It is therefore best practice to get an expert assessment from an information security professional. Seeking the advice of your organization's chief technology officer or someone in a similar position is often a good place to start. More information about digital security trainings is available in section three of this guide.

SECTION 1

SCOPE OF THE DIGITAL SECURITY PROBLEM

DIGITAL SECURITY THREATS TO CIVIL SOCIETY

A growing number of civil society organizations face many of the same targeted information security threats experienced by governments and the private sector. Some of the same threat actors that make front page news by stealing corporate secrets and infiltrating government computers are also regularly targeting civil society. At the same time, the cost of conducting digital monitoring is dropping and the technologies are being acquired by more government and non-state actors. This leaves open the possibility for these technologies to be further abused and turned against NGOs. Even organizations engaged in work viewed as non-threatening to governments and non-state actors face a more dangerous digital environment due to the rise in cyber-based crime. Despite these developments, digital security risks are not fully understood by many in civil society and organizations often lack the resources to effectively respond.

UNDERSTANDING TYPES OF DIGITAL SECURITY THREATS

We think of digital security threats in two ways—**passive monitoring**, such as a government tracking a person or an organization's metadata[1] and **remote intrusion**, such as the targeted malware attacks discussed above or phishing for purposes of stealing information. This framing is useful for grantmakers when considering when and how to potentially help grantees. While it can be difficult to demonstrate conclusively that the communications of civil society organizations have been specifically intercepted via passive monitoring (with exceptions), cases of remote intrusion (aka "hacking") have been well-documented. Once an organization has reached a baseline level of digital security against remote intrusion and credential theft, it will be better prepared to address more sophisticated patterns

REAL CASE STUDIES IN TARGETED DIGITAL ATTACKS AGAINST CIVIL SOCIETY ORGANIZATIONS

Example 1: The director of a NGO working on freedom of expression issues in an Asian country is reading emails when she spots a message from a funder. The sender appeared to be their program officer, and the email provides an update on an upcoming meeting with a request for feedback on an agenda that was attached to the email.

Example 2: In South America, an environmental activist receives an e-mail from the director of a journalism organization, with distressing news that her personal information has been exposed on a website. Would she like to check the link?

Example 3: In the Emirates, a human rights defender receives a text message alert with a news story relevant to his work. Meanwhile, in Mexico a journalist receives a string of text messages that look like news alerts, mobile bill alerts, and Facebook messages.

All three of these attacks were designed to trick the recipients into clicking links or opening files with malicious programs. In Example 1, the malware was hidden in a legitimate-looking document. In Example 2, the activist was shown a fake Flash Player update message. And in Example 3, visiting the link would have silently infected the targets' iPhones, using an expensive "zero day" vulnerability.[2] In each case, once the malware was on a device, it could silently spy on the victim, siphoning off personal data, activating camera and microphone, and tracking their every word.

Fortunately, the NGO worker in Asia sensed something was amiss and did not open the file. This prevented extremely sensitive information she had from reaching the hands of a government seeking to exploit it. Unfortunately, her program officer had been hacked by the government. In the second case the environmental activist's computer was compromised, exposing her personal information to hackers with interests closely aligned with a powerful government in the region. In Example 3, both targets sensed something was amiss, and did not click. In each case, the intended victims shared the suspicious materials with researchers, leading to the unmasking of major campaigns.

[1] Metadata is information that helps to describe other kinds of data. For example, a text book is full of metadata — the table of contents, index, copyright page, and citations can all be thought of as metadata. In the digital environment, examples of metadata include a person or organization's call logs and web browsing history.

[2] A "zero day" vulnerability is typically used to refer to a flaw in software that is not yet known to the vendor, and that could be leveraged by attackers to gain control of a system, or for other malicious purposes.

PASSIVE MONITORING VS. REMOTE INTRUSION

Passive Monitoring (aka "interception"): Can be analogized to a telephone tap placed on the Internet. This kind of monitoring is exceptionally difficult to detect, but has been historically practiced by developed nations. Increasingly, many less-developed nations are purchasing 'turnkey' products that provide them with these capabilities. Passive monitoring can target both the contents of communications, such as what is said, as well as **metadata** generated by communications, like the parties in a communication.

Remote Intrusion (targeted attacks): What people traditionally think of as "hacking," including the use of tools like malware and network intrusion to monitor activities on systems that an attacker does not control such as computers, mobile phones, tablets, and servers.

of threats across the board. Note that this guide does not prioritize issues like the defacement of websites, and online content, although this will likely be a topic of concern for some organizations.

Remote intrusion, or targeted attacks, can take a number of forms. For example, civil society organizations working on issues related to China are known to be targeted by sophisticated government-linked hacking groups that use advanced intrusion tools. Historically, many of these attacks have begun when victims are tricked into opening a document or link containing malicious code. Once the code has run on the victim's machine, the attackers use this point of entry to collect sensitive information. In other cases, attackers may directly target the computers and servers of organizations looking for weaknesses, such as a lack of software updates, and compromise the device without interacting with victims. Evidence suggests that governments in several Middle Eastern, African, and Latin American countries outsource their targeted digital attacks to non-state actors.

Meanwhile, many more countries are known to be customers of companies that sell commercial hacking tools. For example, there are over 70 known government clients of the Italian-based Hacking Team, while another 32 countries are known to have purchased FinFisher, which was developed by a German and UK-based company. Most recently, malware and zero-day exploits sold by NSO Group, an Israel-based company, were found being used in digital snooping against human rights defenders and journalists. While the tools are designed to be difficult to track, investigations undertaken by the Citizen Lab at the University of Toronto in countries ranging from Morocco, Mexico, the UAE, Ethiopia, Ecuador and Bahrain, have found evidence that governments have been using these tools against civil society groups.

Sophisticated phishing attacks, where victims are tricked into providing passwords or two-factor codes, have also been widely observed targeting civil society groups. These attacks can be highly personalized, and may involve messages masquerading as friends or colleagues of the target.

In addition to direct attacks, civil society organizations can become digitally compromised through interactions with third parties as well. For example, malware infected files can be exchanged between partner organizations, including between a grantee and a funder. As with CSOs, there is a growing body of evidence of successful targeted digital attacks against grantmaking organizations—and some of the attackers are the same as those targeting grantees.

CIVIL SOCIETY'S DIGITAL SECURITY LIMITATIONS

Despite the growing threats against a range of civil society organizations, many face chronic capacity limits with information technology. These limits are not specific to digital security, but often reflect basic priority-setting by organizations with finite budgets and competing financial pressures. For example:

- Many organizations do not have a dedicated IT staff person to manage their computers, network and website.
- Often those who do have such a person have not hired someone with experience or competency specifically in information security.
- Many organizations also lack basic digital security policies to protect people and data, as well as updated and standardized devices, networked equipment and software.

These capacity limits can translate into security vulnerabilities. Cumulatively, this weakens an organization's overall security plan. These are key areas where grantmakers can help drive positive change by opening a conversation with grantees about their overall technology capacity.

Within civil society, an ecosystem of service providers, non-profit security trainers, advisors and technical tools has emerged as different groups work to enhance the digital security of civil society organizations. It may be tempting for funders to look for template solutions from this ecosystem. However, successful development and deployment of solutions to information security challenges often vary from organization to organization. It is therefore important that all funders increase their knowledge about information security and how to apply that knowledge in the context of specific grants. Now that you have a better sense of the digital security threats and resource challenges that civil society organizations face, the remainder of the guide will focus on the steps program officers and grants managers can take to help improve the landscape.

SECTION 2

TRIAGE AND ACT — ADVANCING MORE SECURE GRANTMAKING

This section introduces digital security triage into the workflow of a grantmaker, and it starts with a review of your existing grant portfolios. By implementing a systematic approach for assessing digital security, funders can encourage grantseekers and grantees to improve their digital security posture.

DIGITAL SECURITY MINDSET: MAKE HACKERS WORK HARDER

It is important to keep in mind that the purpose of digital security work, expenditures, time, and thinking, is not to try to stop attacks—but to make hackers work harder and therefore succeed less often. A determined attacker will try many strategies to access an organization's assets. Instead of thinking that one solution will make an organization unhackable, a more reasonable approach is to think of the process as adding cost to accessing sensitive information. If you have identified a clear or potential gap in an organization's security approach, this may speak to deeper organizational resource and capacity issues than are immediately apparent.

STEP 1 PERFORM A TRIAGE OR INITIAL ASSESSMENT

All civil society organizations face some degree of digital risk, so we recommend starting by dividing your grant portfolio and grants under consideration as **"some risk"** or **"high risk."** By undertaking a working digital security triage or initial assessment, you will be better positioned to focus your efforts on the most at risk organizations first.

These two categories are not intended to replace a systematic analysis of organizations' risks and threats, but to help make the problem initially more tractable for the grantmaker. These questions only address certain elements of risk. They are intended to be answered by you, the grantmaker, but we strongly encourage you to seek expert input wherever possible throughout the process. What follows are a series of questions aimed at addressing some likely areas of concern.

Is the GRANTEE high risk?

- Does the grantee believe they are at risk? Are key people working for the organization controversial, or viewed with hostility, by to the government or non-state actors?
- Is the grantee or its work considered controversial by government or non-state actors?
- Is the grantee a likely target for monitoring or digital attacks? Have they been targeted before?
- Does the grantee handle sensitive information of interest to a government or non-state actor or the information of threatened groups?
- Does the grantee act as a hub for collecting and/or disseminating information that could be viewed as controversial by a government or non-state actor?

Is the CONTEXT high risk?

- Are there known cases of digital targeting against civil society in this context, evidence of hacking, leaks of internal information from civil society organizations or cases of device seizures etc.?
- Is civil society in general and/or this grantee's work or field facing strong opposition and/or scrutiny from government or non-state actors?
- Is your foundation likely under scrutiny in the country or region where the grantee operates?
- Does the grantee work in a country in which digital surveillance by government or non-state actors is routine?

Is the PROJECT high risk?

- Will the project collect sensitive information, like names, addresses, phone numbers, banking information, gender identity, or other personally identifiable information?
- Does the project involve creating new technical infrastructure (e.g. a new database, website, etc.)?

- Does the project involve working with high risk groups or individuals (i.e. organizations or people facing threats of any sort from government or non-state actors, such as journalists covering sensitive topics, etc.)?

Answering "yes" to any of the questions above should initially put the organization in the "high risk" category. If you are unsure, it is probably best to assume the organization is "high risk." The purpose of this exercise is to lead you toward the organizations where you should initiate more in-depth discussions, identify priorities and surface patterns of concern across grant portfolios. Therefore, it is okay if you end up in a situation where most of your grants are initially categorized as "high risk." That list will likely shrink during the next step of the process where you recalibrate your list.

STEP 2

RECALIBRATE

After completing an initial triage, you will need to recalibrate the list of "high risk" organizations to determine whether or not they should remain "high risk" or be moved to "some risk." We suggest you begin by contacting each organization that you identified as potentially "high risk" and discuss the concern(s) that placed them there. Through this, you might discover that your concerns are being addressed or that they are unwarranted. It is also an opportunity to gauge the organization's interest and willingness to address the concern(s) you have identified, should they remain salient. You might also consider contacting other funders to see if they share concerns similar to yours. Now is also a good time to have a discussion with the organization about their general approach to digital security. To do that, we recommend you start the conversation by asking the seven questions listed under "improving the digital security of all organizations" found within Step 3 below.

STEP 3

REACT

With an initial triage complete and a working division among "high risk" and "some risk" grants, you are now ready to start considering more strategic support that aims to help improve the information security practices of the organizations you work with. Begin with high risk organizations, since the challenges they face can potentially have wide reaching and devastating effects. *In the worst case scenario, digital attacks can compromise the physical security of the organization's staff as well as the people with whom they work.*

IMPROVING THE DIGITAL SECURITY OF HIGH RISK ORGANIZATIONS

We recommend grantmakers consider a three-part approach for addressing the needs of high-risk organizations:

- **Find an expert in information security** who can do a needs and threats assessment and audit. If you are not sure how to find an information security expert, a good place to start is talking to the head of your IT department, who may have immediate ideas and/or refer you to a programmatic colleague who has faced a similar situation.
- **Support the development of information security policies and practices** that include setting out a framework for investing in IT experts and equipment. This might also include strategies to separate how highly confidential information is handled, versus normal communications.
- Depending on your relationship with the organization, **consider funding the resulting plan for addressing the organization's digital security gaps, including, where necessary, upgraded equipment and iterative digital security training, as well as issues of communications security.**

The approach described above focuses on the techniques for protection against remote intrusion, malware, phishing and other attacks against organizations' digital communications and data. How you approach potentially helping a high risk organization will vary on a case-by-case basis, depending on whether an organization is seeking a grant or is a current grantee, and legal considerations, among other factors. What follows are a few potential next steps for grants under consideration and grants that have been made that are determined to be high risk.

For grants under consideration: As a first step, if you are not sure whether the grantee is willing to take seriously the digital security concerns that have surfaced, you should seriously consider whether to make the grant. Should you proceed with a grant, consider providing additional support that incorporates the tripartite approach outlined above. Consider including evaluative benchmarks for the grant that require the organization to demonstrate how it is fixing digital security gaps, be they policy and/or infrastructure gaps, in a sustainable way and condition future grant payments on such requirements.

For grants that have been made: If a grant has already been made, it might be necessary to consider a supplemental grant or, if allowed by your foundation, to spend administrative funds to aid grantees identified as high risk. In either case, we suggest using the tripartite approach outlined above and we encourage you to ask for help from someone with digital security expertise. Consider including evaluative benchmarks that require the organization to demonstrate how it is addressing digital security gaps, be they policy and/or infrastructure in a sustainable way.

You may find it helpful to consider digital security as part of a holistic package of security improvements for an organization. In some cases, high risk organizations may already be receiving support for physical security issues. As these are often the most salient, the digital security dimension might be overlooked or neglected.

IMPROVING THE DIGITAL SECURITY OF ALL ORGANIZATIONS

Improved digital security should be an aspiration for all civil society organizations, not just those at highest risk. While potential and current grantees will have different levels of risk, below are seven questions that you can ask of all organizations to help them improve their digital security. The questions below focus on specific pitfalls that are important at the time of writing. They are intended to get a conversation started, rather than cover all possible issues. For each, we highlight a potential solution. Asking these questions and listening closely to the answers of the grantee can give you a better sense of how strong their grasp is of their organization's digital security, and determine whether to escalate any of your concerns to a trusted advisor on digital security issues.

We think asking these questions should be part of the standard process of grantcraft. Even organizations that are low risk for politically motivated digital attacks face other risks, including financial fraud or other data breaches. Such risks could be mitigated in part by following these steps (at the time of writing).

1. **Question: How is your email hosted?**
   - **Why is this important?** Email is a key part of most organizations' operations, yet it can be difficult or expensive to securely manage.
   - **Pitfall to look out for:** Self-hosted servers, emails managed on a variety of different platforms, and the widespread use of personal email accounts.
   - **Potential solution:** Managed email services for business. Managed solutions improve operational security by outsourcing security concerns to the provider instead of the organization. If organizations host or manage email themselves, be sure they have the internal technical capacity to do so effectively. Importantly, managed services may impact what jurisdiction the e-mail is held in, and are subject to privacy policies. You may wish to familiarize yourself with these issues.

2. **Do you have a policy of "two factor" authentication on work accounts?**
   - **Why is this important?** Passwords are a basic security measure, but when used alone are vulnerable to phishing and hacking.
   - **Pitfall to look out for:** Lack of additional login security, such as not using two factor authentication (e.g. an authenticator app, tokens, or SMS-based authentication). It may be useful to first ask about some of their most sensitive accounts (social media, email, financial services), though multi-factor authentication is important in general.
   - **Potential solution:** Implementing two factor authentication security for organizational accounts. Many service providers such as Google and Facebook offer two-factor authentication as an option waiting to be enabled. In an enterprise context, two factor is also available via some third party providers (e.g. Duo Security). A growing number of cases suggest that some governments intercept two-factor SMS messages, and we suggest you encourage grantees to use the authenticator apps available for phones (e.g. Google Authenticator). Grantees seeking a more robust level of security should use a physical two factor authentication "security key" such as a YubiKey.

3. **Are your devices that store work information encrypted?**
   - **Why is this important?** Devices should be encrypted so that if devices are lost, stolen, or confiscated, confidential data is protected.
   - **Pitfall to look out for:** Lack of "full disk" encryption on devices that handle work information or lack of awareness of the benefits of device encryption.
   - **Potential solution:** A policy of full-disk encryption for work devices, including phones and computers, including on any personal devices where work-related information is stored.

4. **Do you document digital security incidents?**
   - **Why is this important?** Mature organizations are likely to have experienced some form of digital

security incident during normal operations. Without good documentation, it can be difficult to quickly identify when an incident is occurring, even a large-scale breach.

- **Pitfall to look out for:** Lack of policies and procedures for documenting digital security threats. You can start by asking for post-incident reports from previous attacks or breaches. Other examples of problematic practices include discarding potentially malicious emails (rather than logging them and sharing with an IT specialist) or a failure to log alerts of suspicious activity.
- **Potential solution:** We suggest organizations work with an information security expert to establish a basic practice of documenting incidents as this information will be useful to a digital security expert an organization might hire to address a security breach. Such documentation should include, for example, recording suspicious login attempts on accounts, saving suspicious emails, and documenting any loss of control of work devices.

5. **Do you have a plan to respond to a crisis (e.g. Do you have a plan for what to do if your email is hacked)?**
   - **Why is this important?** Suffering a breach can be disruptive and costly, but the costs increase dramatically if there are no plans in place for mitigating the damage and if key information is not regularly backed up.
   - **Pitfall to look out for:** Lack of a crisis response plan in case of a breach, lack of backups for data.
   - **Potential solution:** Implementing an organization-wide encrypted backup policy, and developing a basic response plan.

ENCRYPTED COMMUNICATIONS

The best way to secure your digital conversations is by using end-to-end encrypted communication tools, but they are not a panacea.

A growing number of people and organizations are rightly concerned about the possibility that their sensitive internal conversations might be exposed to surveillance by state and non-state actors. As a result, many organizations undertake frustrating experiments with end-to-end encrypted e-mail. Email encryption is difficult to master and can be risky as it requires that all parties using it follow a strict protocol, otherwise the contents of a message can be exposed.

As a stopgap, we suggest that organizations move their most sensitive internal and external communications to an end-to-end encrypted chat provider. At the time of writing, we recommend trying out Signal, a well-respected and carefully developed mobile and desktop encrypted chat provider that also supports voice calls. Signal also lets you set messages to auto-delete, protecting you if your device is confiscated or stolen.

Other more popular mobile apps, like WhatsApp also offer-end-to-end security, but may collect more metadata than Signal. Organizations may wish to balance the practice of using these more popular apps with the greater amount of metadata retained, and should do this in consultation with a digital security expert.

Encryption Does Not Mean Anonymity

End-to-end encryption does not make you anonymous, and metadata about who you are talking to and where you are located can still be collected with surveillance. However, it can be a dramatic improvement over unencrypted communications because what you write or speak cannot be eavesdropped on.

Beware—Encryption is Not a Panacea

For end-to-end encryption to be effective, it must be undertaken as part of a carefully calibrated plan, rather than on an ad-hoc basis. We are familiar with cases in which high risk groups placed an emphasis on encrypted chat and communications, but failed to secure their computers and devices. This resulted in breaches that included the contents of encrypted communications, siphoned directly from their devices, where they were not encrypted.

6. **Do you have a plan for improving your digital security?**
    - **Why is this important?** Digital security is a critical component of overall organizational security, and a digital security plan is necessary for improving good digital security practices.
    - **Pitfall to look out for:** The organization lacks a plan for taking stock of or improving digital security.
    - **Potential solution:** The organization should work with an expert to undertake an assessment of the digital security threats they face, as well as their digital security capacity gaps. A series of security policies (e.g. password management, administrative roles, travel policies, etc.) should be created based on the assessment and a realistic plan should be created to implement the policies (Step 3: React provides some suggestions about how to go about such a process).
    - Note: Having received a digital security training or making use of digital security tools may be useful, but is never a panacea.

7. **Does the organization use genuine (non-pirated), up-to-date software and operating systems on computers and mobile devices?**
    - **Why is this important?** Out-of-date software, or software that is not receiving regular updates are much more vulnerable to malware and other security issues. Pirated software often cannot be updated, and can also come pre-loaded with malicious software. This is not an academic concern. Recent attacks against Mexican and Emirati civil society used a vulnerability in iPhones that has since been patched with an update. Un-updated phones are still vulnerable.
    - **Pitfall to look out for:** Organization is using pirated or un-updated software.
    - **Potential solution:** Consider subsidizing the purchase of genuine software. In addition, many technology companies have free or low cost programs to provide software (including MS Windows) to registered non-profits.

Funders should help organizations develop and prioritize a culture of digital security. Asking the questions outlined above will help begin that process. There are, of course, many others. In the interest of time, we have not covered most issues in network security and administration. There are many important issues, but we think that if organizations successfully address the seven described above, they will have made a meaningful improvement.

Finally, we have created an annex with special guidance for digital security and international travel given that some funders support organizations that undertake regular international travel.

SECTION 3

CONCLUSION – THINKING MORE SYSTEMATICALLY

This guide has sought to provide you with: 1) an overview of the evolving nature of targeted digital threats against civil society; 2) a three-step process for tentatively ranking the risk a grant poses from a digital security perspective; and 3) approaches for helping to improve the digital security posture of organizations, depending on the level of risk they face. While taking initial steps to help improve the digital security of all the organizations you work with is important, security is an evolving challenge and will need to be tracked through the lifetime of a grant, especially when you are working with high risk organizations. What follows are several best practices that we believe should be mainstreamed within grantcraft.

1. DO NOT START BY FUNDING PIECEMEAL DIGITAL SECURITY ACTIONS

An organization will become more resilient in the face of digital security threats if a systematic and evidence-based approach is taken from the beginning, instead of a patchwork of general tactics. Funders should begin by developing a working assessment of the level of digital security risk an organization faces, then work with the grantee to systematically address the challenges that are identified. Importantly, this will likely require advice from outside experts, and may require some coordination among funders. Example outputs could include improving digital security policies and practices or making changes in an organization's technological infrastructure.

2. COLLABORATE ON SHORT- AND LONG-TERM PLANNING WITH GRANTEES

Many civil society organizations will be outside of their expertise when engaging in digital security planning, and may find a conversation about this with a funder to be a challenge. Requesting that grantees write a brief self-assessment of their own security challenges that accounts for mitigating both digital and physical threats is one way to

TRAININGS: NOT A SILVER BULLET

Paying for a training is not the same thing as paying for a solution to a grantee's security problem. While trainings may help to increase awareness within an organization of digital security issues, and may suggest steps to take, provided alone they are unlikely to result in systematic changes in the **different behaviors, technologies, and habits necessary for security**.

Some training providers make extensive efforts to tailor their curricula to each organization, the specific threats they face, and the resources they have to address them. However, many trainings are not designed to be so specific. This can create the problem that recommendations are mismatched with an organization's culture and threats, and, in some cases, create conflicting information and messaging around security issues. Is can cause problems for IT staff working diligently with a slightly different approach to security, or promote faddish security tools, like a secure messaging app that is unlikely to be widely adopted. In the worst case, trainings can be sources of incorrect or confusing messages around security and can deepen the digital threats a given organization faces.

Threats against civil society organizations are serious and can sometimes be highly sophisticated. In some cases, the threat actors targeting civil society organizations are the same groups targeting governments or corporations. In the face of such threats, it would be considered irresponsible by a corporate board or a government oversight body to simply provide a short "digital security training" to employees, without investing in more systematic measures. There is a risk of developing a problematic way of thinking about digital security for civil society that results in a separate and unequal approach that is overly weighted towards trainings, and neglects the insights from other sectors that face similar threats.

help start a conversation. Importantly, high risk organizations will almost always need to develop short-term and long-term plans for their security and require assistance from an expert. While an outside expert may initially be important in helping organizations address their digital security gaps, the philosophy of grantmaking should focus on enabling organizations to continue to invest in their security so that they become more institutionally resilient in the digital age.

3. COLLABORATION BETWEEN FUNDERS

Lack of donor coordination on digital security threats facing civil society organizations can inadvertently escalate the problems grantees have instead of helping to resolve them. Therefore, whenever possible, donor collaboration is essential. We suggest you start by identifying other donors in your field who share similar concerns that you do about digital security and begin information sharing with them about any digital security concerns you have in relation to the field or with specific shared grantees. From there, you can develop coordinated approaches to advancing digital security at both the individual grantee- and field-level. Such an approach is likely to improve outcomes for your grantees, while also saving time and money.

4. ENCOURAGE ORGANIZATIONS TO MAKE ITERATIVE IT CAPACITY IMPROVEMENTS

IT capacity is rarely static; it is an evolving and iterative process. Below are some ideas for how grantmakers might encourage grantees to improve their IT capacity.

Hiring or sharing the time of a competent IT professional with information security expertise may be one of the single most important steps towards holistic security for an organization. This is particularly important for high risk organizations that might face targeted digital attacks. Lack of competent IT support has long-term costs in inefficiencies with how technology is used and what technology is selected by an organization. Concerningly, it often means that security issues go unaddressed.

Not all organizations will be able to hire an IT staff person with information security expertise. Yet there are still steps organizations can take short of that. Encouraging an organization to move towards cloud-based and managed services can reduce the administrative and security burden for specific services, such as document storage, web-hosting, and email.

In other cases, organizations may wish to collectively hire a trusted IT person or organization who can provide assistance to multiple organizations. This may help address several issues at once, such as data sharing around threats, and ensuring that attacks targeting one organization are noted, and other organizations in the same space provided with protection. As a funder, you may wish to identify such a trusted IT resource and draw on your network and contacts to vet the individual or organization. In other cases, you may wish to partner with other grantmakers to identify and support shared IT capacity.

In addition, it is good practice to ensure that grantees have sufficient funds for equipment, including software licenses. It is a widespread practice that civil society organizations make use of pirated software and operating systems as a cost reducing measure. This opens them up to a range of serious threats that could be mitigated simply by paying for licenses.

CONCLUSION

Digital security threats are constantly evolving. We have attempted to calibrate the questions and process to the problem as we see it today (February, 2017). However, we anticipate that sources of risk and threats, as well as the basic technologies used within civil society, will continue to evolve. We welcome your feedback on this version of the document, as well as input for future versions. Please direct feedback to Eric Sears at the MacArthur Foundation (esears@macfound.org).

ANNEX

SPECIAL NOTE ON INTERNATIONAL TRAVEL

International travel presents unique challenges for organizational and personal security. Staying connected is essential, but border crossings, hotels, and unfamiliar networks are all sources of risk. Any organization whose staff travel regularly should consider developing a travel security policy.

Both grantmakers and grantee organizations should consult with an expert to develop a travel policy tailored to their specific needs. Such a policy may include some of the following examples (this list is not exhaustive):

RISK	POLICY
Private data seized at a border crossing	Travel with loaner laptops and devices that do not contain sensitive materials.
Device stolen	Use full-disk encryption (see: Question 3 above) and always completely power down devices when you are not using them.
Device infected with malware in hotel or meeting room	Do not leave devices unattended

There are many other specific security approaches that belong in a travel security policy, such as the use of Virtual Private Networks (VPNs). However, we strongly believe that these should be approached carefully, and staff trained to understand their protections and limitations.