Stronger NYC Communities Organizational Digital Security Guide

Introduction

Build Power - not Paranoia!

This work supported by Mozilla Foundation, the NYC Mayor's Office of Immigrant Affairs, NYC Mayor's Office of the CTO, and Research Action Design.

CREDITS

Project designed and lead by **Sarah Aoun** and **Bex Hong Hurwitz.**
Curriculum lead writing by **Rory Allen**.

Workshops, activities, and worksheets were developed by **Nasma Ahmed**, **Rory Allen**, **Sarah Aoun**, **Rebecca Chowdhury**, **Hadassah Damien**, **Harlo Holmes**, **Bex Hong Hurwitz**, **David Huerta**, **Palika Makam (WITNESS)**, **Kyla Massey**, **Sonya Reynolds**, and **Xtian Rodriguez**.

This Guide was arranged and edited by **Hadassah Damien**, and designed by **Fridah Oyaro**, Summer 2018.

More at: **https://strongercommunities.info**

Table of Contents

ORGANIZATIONAL DIGITAL SECURITY GUIDE

This guide provides tools and ideas to help organizational digital security workshop leaders approach the work including a full facilitator's guide with agendas and activities; for learners find a participant guide with homework, exercises, and a resource section.

01

INTRODUCTION

INTRODUCTION

ORGANIZATIONAL DIGITAL SECURITY WORK IS IMPORTANT, RIGHT NOW.

Imagine you've just helped organize an immigrants' rights rally. You gathered thousands of names and email addresses from supporters of all kinds: first-generation immigrants, allies, undocumented people, clicktivist sideline watchers -- and everyone in between.

Looking at your list, things going through your mind might include:

- **How do I care for the information these people have shared with us?**
- **Can I help my coworkers care for this list?**
- **What about getting the list of their names and emails to a trusted partner?**
- **How do I make sure this list stays private?**
- **Should I even worry about this with everything else on my plate as an organizer?**

Now, imagine the winds have shifted in government practices -- you're growing more concerned about privacy and security, and you're organizing harder than ever. What do you do?

It's time to build your power, without letting worry and paranoia interfere with your strategic choices.

Read on to learn more about how you can:

- **Raise awareness around concepts in organizational digital security**
- **Give facilitators frameworks to facilitate hands-on practice with security tools and tactics**
- **Advance participant's organizational security practices via awareness, contextual understanding, strategies, and practice**
- **Build relationships of trust and a community of practice between trainers and participants**

Build Power - not Paranoia!

THE STORY OF THIS ORGANIZATIONAL DIGITAL SECURITY WORKSHOP GUIDE

Why we started this project

Vulnerable communities across New York City are seeing an increase in online and offline threats. These have ranged from cyber harassment, phishing and fraud/impersonation to questionable uses of their data.

The Stronger NYC Communities (SCNYC) project was designed to advance the digital security capacities of community-based organizations that work directly with immigrant populations. Importantly, these trainings address the unique challenges of participant groups as they tackle evolving digital security threats to their organizations, and to NYC residents whose data they collect, store and share.

Who the project designers are

This project was led by a team from Research Action Design (RAD) with funding from Mozilla Foundation, core partnership with Mayor's Office of Immigrant Affairs and the Office of the CTO of the Mayor's office of NY. A cohort of ten trainers who serve non-profit organizations stewarded the project together with RAD, facilitating five workshops over the course of six months with 16 community based organizations serving immigrant populations. We acknowledge also that this and all work draws on prior experience with individuals and organizations in the technology for social justice field and social movement.

This guide gathers all of this work - coordination, approach, train the trainer content, workshop facilitation guides, and a workbook for participants...

We hope you get a lot out of these!

HOW TO USE THIS GUIDE

This guide remixes and releases this work with the intention of allowing others to recreate this series. It includes instruction on our approach, facilitation and organization methods, full workshop facilitation guides, a workbook for participants, and a resource and training library.

This guide contains four main sections:

- **A guide to creating and facilitating organizational digital security workshops focused on supporting targeted communities**
- **A facilitator's manual, including workshop agendas, activities, handouts**
- **A participants handbook, including workshop outcomes, homework**
- **A resource guide and glossary.**

Read through the whole Guide, or pull out guidance, content, training activities, or agendas as-needed!

Themes

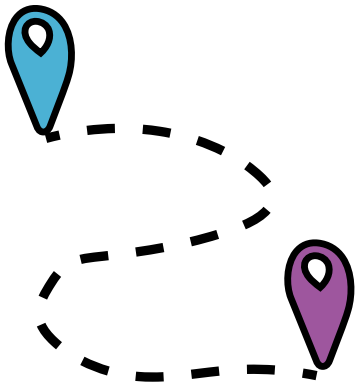
You will find in these guides activities for workshop settings to facilitate learning around:

- **Organizational Security Process:** From Risk assessment to policy writing
- **Tools and Tactics:** Hands on with tools and implementation strategies
- **Building Political Power:** Political history and collective approaches to increasing privacy and decreasing surveillance

ROADMAP

This guide will allow you to follow the organizational digital security workshop series we shared in NYC in 2017-2018, or mix-and-match to create your own workshops.

Whether you follow the workshop content we share closely, or create your own, here's your roadmap to doing this work.



Roadmap for Successful Organizational Digital Security Training

01 **Get a few people** to lead the digital security training project: facilitators and participant organizers. We recommend at least two facilitators per workshop, and more is ok!

02 **Prepare!** Read through the Prep, Design & Facilitation Guides, plan your workshop series timeline and start to book locations and trainers' meetings

03 **Participants!** Identify, invite, and pre-survey your **organizational participants**

04 Leader/facilitators **prepare for each workshop ahead of time** by assembling or using existing agendas, reading guides, print out handouts and activities etc.

05 **Host and lead the workshop(s)** making sure there's time for breaks and questions!

06 **Survey participants** to see how it went, what else they need, and how to improve - and debrief this information with the workshop leaders.

OUTCOMES FROM THIS WORK

Key outcomes from these workshops

1. Organizational Digital Security Process

Participants build capacity to steward digital security strategies in their organization. We share processes for building security into the culture of organizations and communities, beginning with risk assessments and following through to organizational policy creating and implementation. We address organizational change in a manner that sustains and honors the organization's own goals and processes, and respects the nature of this work as intensive, human-centered and emotionally charged.

2. Tactics and Tools: Hands-on and Implementation

Participants increase their practical skills with tools and implementation strategies. Topics range from document storage to device and account setup to change management in an organization.

3. 1-1 Support

Trainers accompany participants through the specifics of their organizational security processes. The training team directly supports the community-based organizations, offering online "office hour" skillshare sessions, and in-person support to facilitate the knowledge transfer and policy development by the community-based organizations.

4. Training of Facilitators

We build each other's capacities as facilitators through sharing knowledge and skill in organizational security and also through practical experience and development of facilitation skills.

5. Building a community of practice

Build relationships of trust and a community of practice between trainers and participants.

What's covered in the workshops

Workshop 1: Our work is political.

In Week 1, we introduce the principles of holistic security and the need for a holistic approach, and outline several goals we have for the coming weeks and months. We develop practices in all of these areas in the course of the following weeks.

Objectives:

- Build a shared understanding of how politics and power shape the technologies and practices of surveillance
- Discuss and share strategies for using collective action to shift the design of technologies and practices of surveillance
- Develop risk assessment as a tool to bring back to each organization
- Understand why and how to use 2-factor authentication, strong passwords, and password managers to reduce unauthorized account access
- Recognize phishing attacks and identify ways to change phishing-vulnerable behavior

Topics we cover:

- State Surveillance, Colonialism, and Racism: a Brief History
- Risk Assessment: What it is, how to conduct risk assessments
- Holistic Security: What it is, why it's important
- 2-Factor Authentication
- Password Managers

The workshops are for adult learners who have many priorities, are part of organizations, and are connected to the reasons for doing digital security work.

Workshop 2: Our work is both individual and collective.

In Workshop 2, hear from guest speakers working in law and immigration justice. We take a step back and deepen your understanding of how the internet works, paving the way for a look at safer browsing habits and VPNs.

Objectives:

- Determine what data stewardship means to us as individuals and organizations
- Understand risks legal discovery poses to data privacy and security
- Deepen understanding of how networks and browsing work
- Gain familiarity with tactics and tools for network and browsing privacy and security
- Gain experience with VPNs
- Discuss motivation for increased browser privacy and security, and explore available tools

Topics we cover:

- Data stewardship and accountability
- Guest lectures: Speakers from NYCLU and Black Law Movement Law Project
- Understanding the internet: Networks, Wifi, Internet infrastructure and web requests
- Hands-on with VPNs

Workshop 3: Our work is about learning from and taking care of each other.

In Workshop 3, we shift focus to smaller group work, where we cover a range of hands-on topics from safer social media use to encrypted messaging. The majority of our work is in small groups, and we discuss organizational security and the elements for creating a security policy-making team in your organization.

Objectives:

- Support peer-sharing through facilitation and design of workshop
- Support participants at different levels by providing possibilities for reviewing topics and tools or engaging with new topics and tools
- Policy and Organizational Change: Make connections between topics we have covered and participants using workshop material to develop organizational policies and organizational security
- Provide concrete takeaways for participants to reinforce and deepen understanding and practice

Topics we cover:

- Organizational security principles to enacting change
- Breakout Sessions: Hands-on topics reviews (Password Managers, 2-factor Authentication, VPNs and how to use them, Secure browsing)
- Breakout Sessions: New concepts (Encrypted video calling, Safer social media use, Action safety planning, Encrypted Messaging, Action Filming & Documenting safely)

Workshop 4: We do our best work when our values and practices align.

We tackle policy development topics and introduce concepts around policy and values alignment. The goal is to shift the conversation from the tools and tactics of the individual to the wider lens of how practices can become policies at an organizational level. We also revisit our breakout groups in order to have in-depth conversations on organization-level issues such as dealing with reluctance/disrupted workflows when adopting new security practices, tackling accusations of paranoia or frustration with new methodologies, and identifying realistic and achievable goals for your organization.

Objectives:

- Guide organizational self-assessment of existing resources and practices
- Identify team members who will support and drive policy drafting
- Begin to articulate a stated security strategy/vision and identify existing areas of alignment and improvement with this vision
- Create introduction to policy drafting plans to take back to organizations

Topics we cover:

- What alignment of values and practices looks like
- Self assessment: Where are our organizations in their policy-drafting process?
- Policy development working groups: fostering security culture, identifying goals, addressing the disruption of existing workflows, tackling paranoia, choosing alternative tools, and revisiting risk assessments
- Strengths Inventory/skillshare: Successful organizational tactics and campaigns

Workshop 5: Our work is ongoing. This is just the start of a longer, sustainable process.

In our final workshop, we combine some final skill-building sessions on encrypted file storage and backups with a team activity on incident response, which brings together everything we have worked towards in the previous four workshops.
We also debrief and wrap up as a group, looking at the ground we've covered, and get feedback on participants' experience.

Objectives:

- Learn about file and disk encryption
- Understand the importance of backups/redundancy and encrypted file storage
- Revisit safer social media use and how to choose and evaluate tools
- Synthesize concepts such as risk assessment, organizational policymaking elements, and concrete tools and tactics in team-based incident response scenario
- Debrief workshop series and collect exit metrics, feedback, and discuss goals for the project

Topics we cover:

- Encryption
- Choosing tools
- Safer Social Media II
- Backups and secure file storage
- Incident Response

So you're ready to start coordinating an organizational digital security workshop?

Start here!

In this section, we share best practices on:

1. Inviting and engaging Sponsors and Trainers
2. Suggested Collective Commitments
3. Creating a Safety Plan
4. Gathering and sorting Topics - including topic examples
5. Inviting Participants

Define the project

Decide who will lead the trainings

Perhaps it's you who's reading this, or perhaps you're hoping to engage other people. If you want to bring others in, it supports them to make their place in the project super clear.

1. Define the roles

Clear asks of everyone make it easier for people to say yes - they know what they're signing up for! For a multi-workshop project you might need lots of support.

Some roles you may want to define, like SCNYC did, include:

- Project Manager or Lead Coordinator
- Curriculum and Materials Lead Developer
- Documentation
- Facilitator or Facilitation Team

Optional: Invite more facilitators

2. Share the playbook

It's important for all stakeholders and participants - including trainer / facilitators and participants - to have a shared understanding of process: What the workshops are trying to do, why, and how.

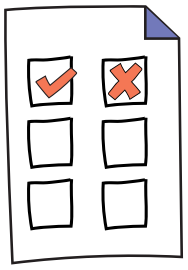
Sharing the playbook of agreements around how the workshops will operate and how we got to the topics being covered is a step - even better, use facilitation techniques (like we discussed in the last section) to invite dialogue and contributions to the topics and commitments to generate buy-in and group alignment on them.

3. Create a timeline, deadlines, and delegate tasks

Help everyone stay on the same page and move as a team - make sure folks' availability works for the plans and make clear asks.

For example, we mapped out all the workshops and preparation meetings at the beginning of the series, about two months before starting, so that everyone was able to find and secure their availability.

Collective Commitments, Workshop Agreements & Values



Collective Commitments, Workshop Agreements & Values should be co-created at the beginning of the series with the leadership and trainer/facilitators. Once you have participants -- bring them into the process and ask if they have more Agreements to contribute. Finally, returned to these at the beginning of each workshop if you're making this a series.

These are ones used in the Stronger Communities project. Feel free to use them as well as a starting point, or completely design and customize your own.

Everyone is an expert

- The implementing team, trainers, participants, and organizations all have valuable skills, knowledge, and experience to share. We are committed to making space and creating activities that allow all to share their expertise. We are committed to crediting all contributors.

Any question is a good question (but get to the point)
"One Mic" - don't interrupt
Harm reduction

- The practices taught should reduce, not provoke anxiety, and should allow for a series of incremental improvements that fit with organizations' needs.
- Organizations will be met where they are at without judgment or evaluation, and will not be given a 'security prescription.'

Consent-based sharing practice

- Make sure that private details stay private, while important information travels out
- Often expressed as: "what's learned here leaves here, but what's said here stays here"

Don't use jargon and spell out acronyms

- Design holistic and sustainable strategies
- The practices that are developed should be sustainable, should contribute to a sense of organizational self-care, longevity and groundedness, and should honor and reinforce the organization's goals and needs.

Build Power, not Paranoia!

Be political

- Racism and the practice of mass surveillance are interwoven with colonialism and the apparatus of the state.
- A goal of these workshops is to build political power and understand how movement-building and collective action are as much a security strategy as any technical tactics.

Creating a Safety Plan

You need to be aware that gathering a group of people who care about and/or who may be immigrants creates the possibility of being targeted for surveillance - or other nefarious activity.

Knowing this, it is in your and all your participants' best interest to create a safety plan.

This can include:

1. **Getting emergency contacts for everyone participating, and sharing under what circumstances they would be used**

2. **Defining an Incident Response Plan. Here's the one we used:**

- In case of any safety or security incident, [project coordinators] will send communication via the [trainers email list]. They will first get consent of any people involved in the event before sharing.
- If an incident relates to just a single person, they will work with that person's emergency contact to support the person.
- If the incident impacts more than one person, the workshops themselves, etc, [project coordinators] will escalate to inform project sponsors.

3. **Getting and sharing Workshop Site Safety Information, like:**

- Point of Contact for the training site: Name, Mobile, Email, Relationship to program
- Safety route out of the building/Safety plan for building
- Policy of who you will and won't let in [in particular, look for a policy disallowing different government agencies to enter without a warrant]
- What are our rights in that building?

4. **Inviting participants to activate their own safety networks, for example sending them an email like this one:**

Dear Participants,
As part of our safety planning for the workshops, please share information with a manger or a colleague at work about your participation in Weds' training. If participating in this workshop is sensitive for you, please also set up a relevant check in system with your point of contact – ex. Check in when you arrive at the workshop, check in when you leave, check in when you get to your next destination.

5. **Identifying Legal support networks available to you**

6. **Sharing with everyone involved that there is a Safety Plan**

Workshop Topics

In the last chapter we gave you a snapshot of the workshops this Guide covers.

Here's a pared-down list you can use when planning your workshop and preparing to ask participants what they might want to learn.

Organizational digital security topics we covered, and which participants asked for are:

- **Encrypted Messaging (Signal, WhatsApp)**
- **Full Disk Encryption on computers**
- **2-Step Verification / 2-Factor Authentication**
- **Organizational Security Policies**
- **Security Workshops and Trainings**
- **Risk Assessments**
- **Password Managers**
- **Encrypted Email**
- **Encrypted Documents**
- **Encryption Tools**
- **Privacy-friendly browser extensions such as HTTPS Everywhere, Privacy Badger**
- **Regular Software and Operating System Updates**
- **Regular Data Backups**
- **VPN**

And of course - Invite Participants and see where they are at!

Identify & Invite Participants

Community groups you're part of, organizations you have connections to, and/or social groups you interact with are all great places to find participants.

For the SCNYC project, we invited organizations to send two participant representatives per organization, so as to generate internal support for the participants and distribute learning using a train-the-trainer model. This also allowed us to scale our impact, as we focused on organizations that had community reach and were valued leaders in their work.

If you're not directly connected with community groups, note that given the nature of digital security focused on supporting targeted communities such as immigrant groups, you will certainly want to partner with trusted persons and/or organizations.

Assess Participant needs

See a sample Organization Needs Assessment Worksheet in the next chapter: ***Evaluation.***

Once you've identified and invited participants and gotten a yes, you may want to survey them to assess where they are currently with their digital security concerns, practices, and needs to understand how you might best serve them and compare their knowledge before and after for evaluation.

Facilitation & Workshop Design Techniques

A workshop is an intentional space, created for learning, changing points of view, and people leave with clear actions to take. Part of the power of a workshop is in its design and its leadership.

In this section, you'll learn:

- **Facilitation Practices: General and Advanced Pro-tips**
- **An intro to Open Space sessions - and how to run them**
- **How to hold space for the Emotional Aspects of the Work**

General Facilitator Practices

This is a quick list that trainer/facilitators might want to read and remind themselves with before any workshop session.

Checking in
Use a few minutes at the beginning of the workshop and after beaks to bring everyone together (for example, with an icebreaker). This allows facilitators to both understand the energies that people are arriving with and request that participants focus their attention on the workshop.

Participants in the lead
Whenever possible, ask participants if they want to share their knowledge and experience rather than explaining something yourself. The workshop has to have meaning to our participants and be driven by their needs and experiences, so the more they drive it, the better.

Open Space
Open-space sessions are a format for holding self-organized sessions around a certain topic or theme. In general they are open-ended and emphasize the knowledge, emergent creativity, and resources of the participants who are present, rather than a predetermined idea of what should be discussed and decided.

Keeping energy up
Bring snacks and beverages and encourage a room setup where it's easy to get up, stretch your legs, and grab a drink or a bite during the session.

Co-facilitate
Agree with your co-facilitator(s) on methods to communicate around the energy and needs in the room including:

- **Responding to questions in the room.** For example, as a co-facilitator you could raise your hand and ask guiding questions of the lead facilitators when you know participants have questions.
- **Maintaining a calm pace and slowing down.**
- **Taking a break or doing an ice-breaker.**
- **Keeping time.**

Be prepared
Prepare yourself and with your co-facilitator(s) to facilitate a clear space for learning and building. Read through the handouts and facilitation guide ahead of time. Prepare your facilitation with your co-facilitator(s), knowing what roles you will take in the workshop.

Prepare for the Emotional aspects of security work
Especially, avoid paralysis (a/k/a 'security nihilism') by making sure to identify strengths at the same time as identifying challenges/risks.

Open Space

In your workshops, we suggest employing the principles of open space meetings while addressing specific topics in digital security.

Running an Open-Space-Like Session

A lot of the work we did was focused on small group conversations.

If you want to run these types of sessions, here is a guide to help you get started.

Background: Open-space sessions are a format for holding self-organized sessions around a certain topic or theme. In general they are open-ended and emphasize the knowledge and emergent creativity of (and resources) of the participants that are present, rather than a predetermined idea of what should be discussed and decided.

Setup:

- Chairs in a circle so that we can all see each other and reduce hierarchy of seating placement.
- Writing/documenting materials available (paper, markers, whiteboard, handouts, etc).

The principles of open-space workshops:

- "Whoever comes is the right people.
- Whenever it starts is the right time.
- Wherever it is, is the right place.
- Whatever happens is the only thing that could have happened. Prepare to be surprised!
- When it's over, it's over."

And finally, "If you're in a situation where you're not contributing or learning, you're free to move to a different space." Your participants should feel free to stay in the space as long as it is serving them, and should feel safe moving to a different space (non-disruptively!) if they so choose.

Further reading on Open Space design:

http://www.michaelherman.com/cgi/wiki.cgi?OpenSpaceTechnology
http://www.openspaceworld.com/users_guide.htm
https://en.wikipedia.org/wiki/Open_Space_Technology
http://www.communityplanning.net/methods/open_space_workshop.php
http://www.openspaceworld.org/files/tmnfiles/OSTResearch2000.htm

Prepare for the Emotional aspects of security work

Creating the organizational climate that's open to security work means being in alignment with these principles, and maybe others that you hold as well.

- **Manageable, incremental improvements.** People won't adopt to a shock to the system in terms of a barrage of new tools, procedures, or devices; they will feel stressed, frustrated, and disempowered. People are also creative; frustration around new tools or procedures is a natural breeding ground for 'shadow architecture' (i.e., more convenient but less secure workarounds that people adopt when they're frustrated or overwhelmed). It can be hard to balance the urgency and importance of the information you're conveying with the rate at which folks can absorb it, but proceed slowly and check in as you go.

- **A culture of welcoming all questions.** Both in the training space and in each organization's space, there needs to be a safe and well-communicated culture for bringing up questions. If everyone else seems to be following a high-level conversation, it can be difficult or intimidating to ask a question like 'what is encryption?', or it can seem disloyal or skeptical to ask 'why do we even need to do this at all?', but both types of questions need to be welcomed - both to make sure everyone understands and can follow any new organizational practices, and because sometimes, dissenting or reframing questions can actually prompt the most important realizations and tactics.

- **Appropriate pacing.** Some topics will spark more of a discussion with some groups than others. Trust this and use your judgment in reworking the sessions.

- **Avoiding paralysis**/'security nihilism' by making sure to identify strengths at the same time as identifying challenges/risks. We will continually revisit the stories of both internal and collective resilience (which is why we're doing this work in the first place!). Our strongest tactics remind us of our existing strengths.

- **Checking in as we go.** it's more important to cover material well than it is to push through all of it. If people are stressed or overloaded, they won't learn. Pay attention to the energy in the room and change plans if necessary.

Facilitation and Design approaches

These workshops are for adult learners who have many priorities, are part of organizations, and are connected to the reasons for doing digital security work.

Methods we wove into the design and facilitation of the workshops included:

- Participatory design - getting all engaged and involved
- Pop education - drawing from people's existing knowledge
- Intersectionality - acknowledging that people are complex and bring multiple identities and experiences into the room

A few facilitation resources

ADIDS: Adult learning methodology by LevelUP: Activity & Discussion, Input, Deepening, and Synthesis
https://www.level-up.cc/before-an-event/preparing-sessions-using-adids/

Anti-Oppression Resource and Training Alliance (AORTA)
http://aorta.coop/portfolio_page/anti-oppressive-facilitation/

Facilitating Group Learning: Strategies for Success with Adult Learners, by George Lakey

Popular Education
http://www.practicingfreedom.org/offerings/popular-education/

Training for Change
https://www.trainingforchange.org

EVALUATION

EVALUATION

Often, evaluation is a key way we're able to generate trust in - not to mention funding for! - our work as trainers. Don't overlook it. Instead, use evaluation as a way to make sure your workshops are as useful as possible for your participants.

Setting a rhythm of surveys

Setting a cadence of regular, brief surveying helps your participants expect to be surveyed, and can increase return rate. It also helps you as a workshop leader remember to survey and evaluate -- and gives you data you can use to measure outcomes (something our sponsors and funders tend to like) and improve future workshops.

If you delivered a pre-Workshop assessment when you invited your participants (see the previous section), you are already off to a good start.

Delivery notes for facilitators

- **Evaluate early and often!** It gets people used to it, and gives you lots of ideas and participant-focused guidance to learn and improve from.
- **A written evaluation** works best if you hand it out before the end of a workshop session and build in about 10 minutes for people to fill it out before they have to leave. Also, shorter surveys get longer answers to the particular questions.
- **A verbal evaluation** is great for asking deeper questions, and can be connected to an ongoing 1:1 meeting or administered in a pre-scheduled time.

You can print the following pages

SAMPLE EVALUATIONS

Below are four evaluations. Here's when and how you'd use them.

1. Intake Assessment - To intake organizations or participants into a workshop or workshop series. Feel free to customize the following intake assessment, which is keyed to organizations who are sending one or more participants to the workshop. You might use it for a verbal intake over the phone or on a video call, or send it as an email or as a document you have someone fill out and return, as it's a bit long for a form.

2. Training Evaluation: Written - use this as a handout at the end of the first or second workshop to touch base with participants and see what they're getting out of the workshop.

3. Mid-Series Evaluation - Can be a verbal check-in or a handout. Use this after the second or third in a series of workshops to see if the participants are getting what they need, and to guide changes to your content or approach if needed.

4. Exit Survey - a full check-out survey, designed to be sent as a form or given as a handout to dive deep into outcomes and transformations the participants experienced from a series of workshops.

1. Intake: Organization Representative Assessment Worksheet

Purpose of this assessment

- Develop a program that is grounded in the goals of participating organizations
- Develop understanding of participating organization and how it will implement change
- Gather participating organization's goals
- Assess any major areas of concern

Organization Blurb / Mission+Vision:

Current Main areas of work:

Organizational Structure: What is the organizational structure? Who manages IT? What do they manage (ex. Servers, email, wifi?

Organizational Change: How will you bring the processes and learning from this project into your organization? Who else will you work with to make decisions and implement?

Organization Goals: What are your organization's goals for participating in this program?

This assessment template developed by RAD for this SCNYC includes best practices learned from Association for Progressive Communications (APC), Security Positive, and Wellstone.

Current Practice: How does your organization address safety concerns?

Greatest Concerns: What are your greatest concerns regarding your organization's members, staff, supporters' safety?

Risk Assessment Storytelling

- What security issues have you or members of the organization already experienced?
- What happened? Where? How? What was the threat?
- What was the impact of that incident/threat: to self, the community, the work?
- What did you do in response to the threat? How did others help?

Mapping Questions

- What kinds of data do you work with?
- Data gathered on members? Grantees? Partners?
- What is the most sensitive data you work with? And how do you take care of it?
- What software and tools do you work with (ex. Google Suite, Office 365, Dropbox)?
- What are your backup processes?
- Do you have any concerns about how you gather or manage data?
- What software and tools do you use to communicate with staff / volunteers / clients / members?
- What software tools do you use to communicate with staff / volunteers / clients / members?
- What is the most sensitive communication you do? And how do you take care of it?
- What kinds of devices do people use for work (ex. desktops, laptops, mobiles)? What security protocols do you have in place for these?
- How do you secure your offices (ex. Doors, cabinets, offices)?
- Do you have any specific concerns about your offices?

2. Training Evaluation

- During this workshop, what worked for you? Please be specific, with examples:

- What didn't? Please be specific, with examples:

- What key takeaways did you get out of the workshop?

- What do you need more of to support you applying strategies, tactics, and tools from the workshop in your organization?

3. Mid-Series Workshop Evaluation

- Since your first workshop, what practices or tools did you implement?

- What else do you need support with?

- Is there anything you want to contribute?

- What are your goals for the rest of the training? Have they changed?

4. End of Workshop Series Exit Survey

Please select the topics, if any, you were familiar with, ***BEFORE*** the Stronger Communities Workshop began.

- 2-Step Verification / 2-Factor Authentication
- Encrypted Documents
  Encrypted Email
- Encrypted Messaging (Signal, WhatsApp)
- Encryption Tools
- Full Disk Encryption on computers
- Organizational Security Policies
- Password Managers
- Privacy-friendly browser extensions such as HTTPS Everywhere, Privacy Badger
- Regular Data Backups
- Regular Software and Operating System Updates
- Risk Assessments
- Security Workshops and Trainings
- VPN

Please select the topics, if any, you are familiar with now, ***AFTER*** the Stronger Communities Project.

- 2-Step Verification / 2-Factor Authentication
- Encrypted Documents
- Encrypted Email
- Encrypted Messaging (Signal, WhatsApp)
- Encryption Tools
- Full Disk Encryption on computers
- Organizational Security Policies
- Password Managers
- Privacy-friendly browser extensions such as HTTPS Everywhere, Privacy Badger
- Regular Data Backups
- Regular Software and Operating System Updates
- Risk Assessments
- Security Workshops and Trainings
- VPN

What is the most important thing you feel you have learned in the Stronger Communities project?

Which of the following were the ***MOST*** helpful, interesting, or positive parts of the Stronger Communities project? (You may select more than one)

- Whole group discussions
- Lecture/Instruction
- Demos
- Online office hours/clinics
- Guest speakers
- 1:1 Support in person
- Phone checkins
- Small group (2-3 person) discussions
- Other:

Which of the following were the *LEAST* helpful, interesting, or positive parts? (You may select more than one)

- Small group (2-3 person) discussions
- Guest speakers
- Lecture/instruction
- 1:1 Support in person
- Demos
- Whole group discussions
- Online office hours/clinics
- Phone checkins
- Other:

If you selected items on the last question, can you please elaborate on why those things were not helpful, interesting, or positive?

Do you have any comments or suggestions on things that would have made our workshops more helpful to you?

My organization talks about digital security practices with employees (in staff meetings, trainings, etc).

Not very true Very true
1 2 3 4 5

My colleagues are open to changing their digital practices.

Not very true Very true
1 2 3 4 5

My supervisors / managers are open to changing their or digital practices.

Not very true Very true
1 2 3 4 5

My organization has a full-time IT person.

Yes
No

This is the area I feel my organization does **BEST** at with regards to organizational or digital security:

This is what my organization most urgently needs in order to strengthen its digital security:

After completing this program, are you now more or less confident about how your organization handles its data?

- Much more confident
- Somewhat more confident
- No change in confidence
- Somewhat less confident
- Much less confident

Activity & Handout Glossary

A quick reference for facilitators to pick out handouts or activities to use in workshops.

Handout List

Handout name	Used in workshop	Participants find it...
Risk Assessment Walkthrough	1: Principles & basics of holistic security	Facilitators print and bring as prep for workshop 1, it's attached to the Facilitator Guide
NYCLU NY ECPA Fact Sheet (2017).pdf	2: Data Security	Attached to the Participant Workshop Guide. Facilitators also have a prompt to print it for participants.
Ways to Protect Your Cell Phone (2017).pdf	2: Data Security	Attached to the Participant Workshop Guide. Facilitators also have a prompt to print it for participants.
Practices in Organizational Holistic Security - Preparedness Assessment	3: Organizational Digital Security	It's in the Participant Guide for Workshop 3
Handout: Organizational Security: Towards a Policy Development Process	3: Organizational Digital Security	Facilitators print and bring as prep for workshop 3
Aligning Values and Practices Adapted from Cultural and Digital Security Practices by Kyla Massey	4: Policy & Procedure	In Workshop 4 Facilitators' Guide and Participant Workshop Guide.
Addressing Proficiency Gap	4: Policy & Procedure	In Workshop 4 Facilitators' Guide and Participant Workshop Guide.
Alternatives to Google Docs	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Are you just being Paranoid? One Sheet	4: Policy & Procedure	In Workshop 4 Facilitators' Guide

Handout name	Used in workshop	Participants find it...
Intergenerational Working Group Handout	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Creating Prioritized Goals Worksheet	4: Policy & Procedure	In Workshop 4 Facilitators' Guide
Open Space Mini-Workshop Tool Handouts	5: Incident Response & Wrap up	In Readings & Resources
Incident Response Scenario	5: Incident Response & Wrap up	In Workshop 5 Facilitators' Guide

Activity Glossary

Activity name	Used in workshop...	Facilitators find this...
History of Surveillance	1: Principles & basics of holistic security	In Workshop Facilitators' Guide for Workshop 2
Holistic Security Process: Risk Assessment	1: Principles & basics of holistic security	In Workshop Facilitators' Guide for Workshop 2
What we know: Mapping exercise	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Data My Organization Collects	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Internet Structure (Matching Cards)	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Browsing / Browsers	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
VPN Demo	2: Data Stewardship and Security	In Workshop Facilitators' Guide for Workshop 2
Putting it Together: Organizational Security Process	3: Organizational Digital Security	In Workshop Facilitators' Guide for Workshop 3
Open Space Mini-workshop	3: Organizational Digital Security	In Workshop Facilitators' Guide for

Stronger NYC Communities Organizational Digital Security Guide

Build Power - not Paranoia!

Visit: https://strongercommunities.info