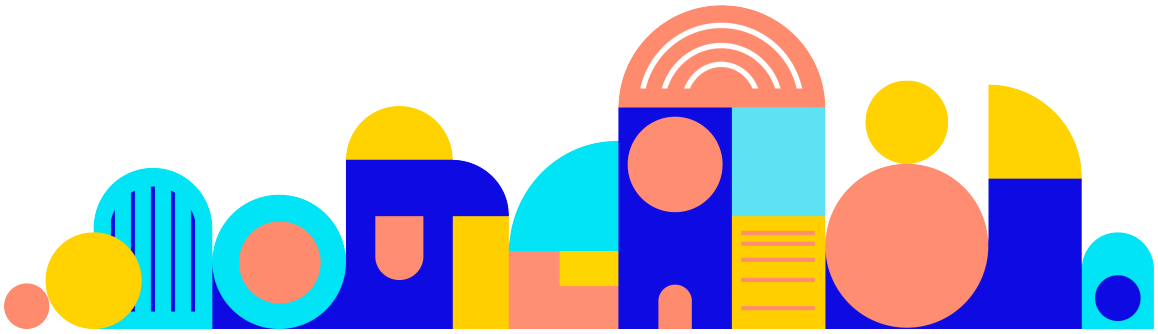

Digital Security Exchange

Organizational Partnerships Program

Program Scope

The goal of Digital Security Exchange's (DSX) Organizational Partnership Program is to pair civil society organizations with credible and trustworthy digital security providers and trainers who can help organizations keep their data and networks safe from exposure, exploitation, and attack.

The program is composed of two approaches for incoming organizations: Either (1) active participation in an organizational partnership program that pairs organizations with digital security providers and strategic thinking from DSX staff; or (2) a simple pairing and introduction (a "handoff") between an organization and a digital service provider.

The Organizational Partnership Program (OP) is composed of three (3) primary participants;

- A civil society organization
- A digital security trainer/provider
- DSX

Each of these entities has, depending upon the approach desired, different levels of communication and commitment.

This program will iterate as it progresses, based on feedback and learnings from DSX staff and our partners.

Our programmatic objectives include:

- The successful connecting of organizations to providers, matching needs and characteristics to capabilities and experience
- Increasing the awareness and implementation of security best practices
- Increasing organizations' capacity to implement such best practices;
- Creating a network of organizations that share experience, information, resources, best methods to keep data secure.

About Digital Security Exchange

DSX is committed to establishing itself as a credible, trustworthy, digital security matchmaking and advocacy resource. We strive at all times to maintain a "do no harm" approach to the organizations and providers we work with. One of the ways in which we maintain that approach is by being deliberate in the technologies we use -- prioritizing security and privacy above all else -- and our commitment to transparency in how we work and communicate. This includes transparency in how we develop, fund, and maintain our processes, systems and services as well as a data retention policy that preserves organization privacy.

There may be organizations or individuals who request information from DSX in order to augment or direct their own security practices, and who desire that DSX does not retain any identifying information. We will honor this need for anonymity and, when requested, will retain no or minimal data, including any records of interactions between DSX and partners or connections between organizations and providers. The exception is for "handoffs," in which we

may retain contact information until such time as a contact confirmation has taken place. In those cases, records are expunged once we have confirmed minimal contact.

Our commitment to organizations:
We believe that the work of civil society organizations is vital to the continued progress and health of our society. We will only match organizations with providers we trust and who have been vetted to work collaboratively within relevant communities; whose values align with our own; who have shown a commitment to and experience working with vulnerable communities; who have worked previously with our staff, Advisory Committee members, and other DSX providers; and who have demonstrated expertise in customized approaches to digital security. For more on who we work with and why, refer to this section of our About page.

Our commitment to providers:
We believe in supporting the growth of healthy communities, which, as a successful by-product of our matching program, decreases the vulnerability of civil sector organizations as a whole. When appropriate, we gather information from participating organizations on the efficacy of recommended actions and share anonymized results with providers to inform future solutions. As mentioned above, we have a strict privacy policy and we collect and share no data on organizations and providers who request it.

Background and Current Landscape

There are approximately 1.5 million non-profit organizations registered in the United States (as of 2016), and 63% of those organizations have experienced a data breach (characterized as hacking, theft, inadvertent errors, or third-party breaches). These data breaches can result in resolution costs that range between under $50,000 USD to over $500,000 USD depending upon the nature of the compromise.

When civil society organizations form, the focus is often on minimally-viable services and tools needed to carry out the organization's mission. Digital security and best practices for data retention and access are often deprioritized due to lack of awareness, funding, expertise, and infrastructure. In addition, given that the majority of civil society organizations are composed of paid and volunteer staff who access information via various personal and organizational devices and networks, convenience and accessibility is often prioritized over security.

The current climate and the need for organizations to have an online presence that eases the friction between themselves, the communities they serve, and their sources of support means that there is more opportunity for malicious or capricious attacks on organizational data.

Distinguishing the Organizational Partnership Program from other industry programs or activities.

DSX recognizes that civil society has become more aware of the potential risks of unsecured networks and a lack of standard security practices across all actors.

We believe we occupy a unique space in that we seek to facilitate connections and collaborations between organizations that need help, and providers who would serve them,

establishing trusted connections with providers familiar with the missions, common vulnerabilities, and workflows of civil society groups.

Program Goals

The goal of DSX is to increase the digital safety and security of community-based organizations, local and national organizers, and those who are working to advance social, racial, political, and economic justice in our communities and our world.

The Organizational Partnership Program achieves this by:

- Working with organizations in need of digital security assistance to connect with participating providers.
- Providing support for building awareness, capacity, and skills to organizations who wish to jumpstart or accelerate their digital security work.
- Providing resources for building security into organizational development.
- Building stronger connections within and between civil society organizations and digital security experts.
- Having a measurable, positive impact on securing civil society *by*
  a. Creating ways to share expertise and other resources among participants
  b. Establishing goals and measures to evaluate program impact on organizations
  c. Guiding organizations and individuals on security best practices
  d. Reducing the opportunities for hacking / DDoS /common security holes for civil society organizations
  e. Increasing the awareness and implementation of security best practices of civil society organizations.
- Generating meaningful user feedback on ways to improve the CDR platform.
- Learning, improving, and customizing the resources and best practices recommendations for organizations based on individual characteristics, needs, regional capacities, and language accommodation.
- Developing resources and opportunities for organizations to fund their security initiatives.
- Onboarding new organizational partners and providers and developing new partnership cohorts.
- Organizing successful handoffs.
- Gathering feedback to develop and fine-tune a decision diagram for self-driven digital security solutions that are customized for field and organizational characteristics and needs.
- Increasing year-on-year participation requests.
- Increasing referrals by participants.
- Assessing and improving participant satisfaction.

Deliverables

In addition to the goals listed above, DSX will summarize our learnings via annual reports, which may include case studies, summaries of findings, and analyses of threats and vulnerabilities.

Program Roles, Responsibilities, Minimum Requirements

DSX recognizes that participation in the Organizational Partnership Program is voluntary and that its success depends upon establishing cooperative relationships with participating organizations and providers.

1. Organizational Partnership Program Staff
   The Partnership Program staff are responsible for overall program development and management. Specific duties include:
   a. To reach out to and build relationships with and amongst civil society organizations and providers.
   b. Addressing all inbound communication about the program.
   c. Maintaining records (anonymized and encrypted as needed) about participation and outcomes of the program. [*Privacy and Data Security Policy link*]
   d. Collecting, analyzing, disaggregating, and managing data for reports and evaluations.
   e. Extracting feedback and lessons from participant experiences and evaluations, enabling continuous improvement for the platform (CDR) and program.
   f. Developing strategies for program evolution, impact, satisfaction, and retention.

2. Organizations
   The participating organizations pledge to:
   a. *Openly share* (dependent upon selected approach) organizational strengths, weaknesses, and abilities/resources.
   b. Allocate appropriate and adequate resources in order to act upon the recommended plans.
   c. Engage in dialogue with DSX Partnership Program staff and partners (amount and level of dialogue dependent upon selected approach).

3. Providers
   The Providers are the trusted digital security partners of the program and pledge the following:
   a. Recommendation of plans that are appropriate to the organization's levels of expertise, funding, resources, and timeline.
   b. Commitment to the recommended plan and the connected organization.
   c. Engage in open and constructive dialogue with Partnership Program staff and organizations.
   d. Do no harm as they develop and implement digital security solutions for participating organizations.
   e. Continued communication with organizations for a mutually agreed-upon time after the conclusion of the recommended plan.

Minimum requirements for Providers and Organizations

Provider
Harmonious data retention policies to that of DSX.
Agreement to provide a minimum level of committed action.
To participate in learning and feedback sessions with DSX.

Organization
Commitment to relationships and security practices.
Values must align with DSX's stated values.

Program Methodology

Approach 1: Cohort program definition and timeframe

DSX desires to create program cohorts (active groups of partner organizations receiving strategic thinking from DSX staff and connecting to participating providers) in order to maximize learnings and foster greater information sharing among participants. For this approach, the DSX staff will be coordinating and facilitating cohort meetings and communication, providing a baseline of interaction and a collaboration space. We will be observing the activity within the cohort to support its work, make improvements to the program, and develop resource guides.

There are 2 cohorts envisioned for the initial year:
1. March – August 2018
2. September 2018 – February 2019

Each cohort consists of organizations, providers and DSX staff members.
Participants in the cohort are asked:
a. To complete the memorandum of understanding and the cohort addendum [link].
b. To implement and adhere to the recommended practices and CDR platform within the 6 months of the program (organizations).
c. To attend and participate in a minimum of two (2) webinar sessions, which include the welcome/introduction and onboarding to the CDR platform.
d. To respect the confidentiality and disclosure agreement of the cohort.
e. To utilize the platform (CDR) and provide feedback to DSX.
f. To participate in intake and outtake sessions.

An example of the cohort approach is:
1. Organizations reach out to DSX for help, providing their background, current problems, desired outcome and timeframe and enlisting to join a cohort.
2. DSX staff respond to the request, gathering additional information (as needed) and answering any questions about the program and the specific requirements for participation in the cohort approach.
3. Organization completes the MOU and cohort addendum.
4. DSX assesses the needs of the organization and makes a match with the appropriate provider.
5. DSX makes the introduction between the organization and the provider.
6. Organization and provider may execute a written agreement.
7. DSX provides organization and provider with login credentials for the CDR platform.

8. All parties attend initial/kick-off webinar session, share background, experiences, goals.
9. Providers and organizations agree on a recommended approach and initiate work.
10. All parties attend webinar session at the conclusion of the cohort term and participate in exit interview.

Approach 2: Handoff

Throughout the lifecycle of DSX, there will be organizations that will contact DSX and request a match made to an appropriate provider but will choose not to participate in the cohort program. In those situations, we will evaluate the organization need and the provider expertise and make the appropriate introductions. We will also typically retain organization information for follow-up and feedback purposes.

However, we also recognize some organizations' need for privacy and/or anonymity. Should an organization request anonymity, we shall retain organizational data only until such time as we have confirmed that contact between the organization and provider has been made, at which point we will permanently purge that data.

A example of the handoff approach is:

1. Organizations reach out to DSX for help, providing their background, current problems, desired outcome and timeframe.
2. DSX staff responds to the request, gathering additional information (as needed) and answering any questions about the program.
3. DSX assesses the needs of the organization and makes the match with the appropriate provider.
4. DSX makes the introduction between the organization and the provider.
5. After confirming contact between organization and provider, DSX may follow up with both parties to learn about recommended plans, outcomes, feedback.

Conclusion

DSX believes that the establishment and successful execution of the program will reduce the friction for civil society organizations in understanding the security landscape, developing, implementing, and maintaining effective solutions and practices, and connecting with other organizations and digital security providers.