BUILD: BUILDING INSTITUTIONS & NETWORKS

CYBERSECURITY CAPACITY BUILDING

December 2020 Technical Assistance Providers "The Honest Mechanics" list

By Matt Mitchell,

contributors: Martijn Grooten, Matt Hansen, Runa Sandvik, Trinh Nguyen, Laura Tich



Introduction

In November of 2020, BUILD launched the <u>Cybersecurity Assessment Tool (CAT)</u>. When I was a cybersecurity provider to civil society groups, one of the most common questions I would encounter when working was "How does my organization measure up?" and "What are the next steps we should take?" We have worked on CAT for almost a year in order to provide answers to those questions. CAT is empathic, pragmatic, and helps organizations

find gaps in their cybersecurity capacity. CAT was never designed to be used alone, the best use of CAT is with the guidance of a cybersecurity expert.

Challenge: Finding a cybersecurity provider

To make the best use of the personalized recommendations provided by the Cybersecurity Assessment Tool, organizations should work with a qualified cybersecurity professional or service provider. However it can be difficult for a civil society organization to choose the right provider.

A transparent and scalable solution.

We are working on producing what I call the "Honest Mechanic Guide", a plain speak document and series of questions produced by the same team that built CAT. Finding an honest and reliable mechanic is difficult, much like finding the right cybersecurity provider for a nonprofit, NGO (non governmental organization), or CSO (civil society organization). The names in gold are the CAT team themselves who are all working consultants in cybersecurity. The names in silver are professionals we have worked with whom we feel have the skills needed to assist the unique threats and challenges nonprofits face when it comes to cybersecurity.

How to use this document.

The providers listed below can be contacted over email to see if they are available to speak about how they can work with your organization. Feel free to mention that you received their information from the Ford Foundation CAT team. While we can not guarantee that each provider will be available to assist you, we can vouch for their skills and commitment.

Where are the cybersecurity firms?

I often equate cybersecurity to medicine in that it is a large field made up of generalists and specialists. Just like how medicine has neurologists and cardiologists, cybersecurity has penetration testers, red teamers, blue teamers, vulnerability assessors, threat hunters, auditors, trainers, etc. Working with a cybersecurity firm can be expensive and

overwhelming so the CAT team is currently recommending organizations start with experienced Individual practitioners.

Runa Sandvik, runa@granitt.io

Languages: English, Norwegian
Region: Global, USA, Scandinavia

Area of expertise/focus: Journalists, high-risk individuals

Runa works on digital security for journalists and other high-risk people. Her work builds upon experience from her time at The New York Times, Freedom of the Press Foundation, and The Tor Project.

Laura Tich, tich@shehackske.com

Languages: **English, Kiswahili**

Region: Global, Global, Sub-Saharan Africa

Area of expertise/focus: Civil Society Organizations

Laura is an information security analyst and cybersecurity trainer with expertise in network security and open source intelligence. She is an advocate for Internet freedom and has worked on various projects around digital security for journalists and civil society organizations across Africa. She is a founder of SheHacks_KE, a community of women cybersecurity professionals and enthusiasts in Kenya.

Trinh Nguyen, trinhi@protonmail.com

Languages: English, Vietnamese

Region: Global, Global, South East Asia, USA

Area of expertise/focus: Civil Society Organizations, Pro-democracy orgs, training

Trinh is a holistic security and movement building trainer, currently serving as the head of operations for team community at ARTICLE 19. Trinh has over 15 years of training experience, previously working on campaigns for reproductive justice, anti-oppression, Internet freedom, and pro-democracy efforts in Vietnam. As a movement building trainer, she incorporates capacity building and cybersecurity tactics to help diverse grassroots pro-democracy and human rights movements achieve digital resiliency and organizational security.

Martijn Grooten, <u>martijn@lapsedordinary.net</u>

Languages: Dutch, English, German

Region: Global, Global, Europe

Area of expertise/focus: Civil Society Organizations, viruses, malware, & abuse

Martijn worked as an academic mathematician before finding himself with a job at a security company almost 14 years ago. He has a broad interest in security and was the editor of Virus Bulletin for almost six years. He is a regular public speaker and writer and currently works as a security consultant with a particular focus on helping vulnerable groups and people. He is a fellow of the Civilsphere Project and a special advisor to the Coalition Against Stalkerware.

Foz, <u>foz@riseup.net</u>

Languages: Portuguese, English
Region: Global, Global, Brazil

Area of expertise/focus: Civil Society Organizations, cybersecurity threats faced by

organizers and individuals.

Foz is a Brazilian hacker and expert on cybersecurity as it impacts civil society groups, nonprofits, organizers, and activists.

Karim Beldjilali, Info@karim.us.com

Languages: English, French

Region: Global, USA

Area of expertise/focus: Policy & Frameworks

Karim has 17 years experience in technology, information security and data protection with startups, nonprofits, and for-profits, having held positions in leadership to build nonprofits as well as technology security and risk management programs and policies as a hands-on leader and engaged partner by being strategic and collaborative. With work ranging from the New York Times and New York University to the Fund for the City of New York, he can contribute technical, managerial, collaborative, and mission-driven experience to mature organizations.

Brian Obilo, brianobie91@gmail.com Languages: English, French, Kiswahili Region: Global, Sub-Saharan Africa

Area of expertise/focus: Security engineering , Training

Brian is a seasoned cybersecurity engineer and digital security trainer who is passionate and knowledgeable about web, network and application security, penetration testing and conducting social engineering assessments to determine user security awareness in client organizations. Additionally, he's well-versed in developing and executing cybersecurity training and awareness programs and campaigns.

Brian is a Tech and Society Fellow at The Mozilla Foundation who is committed to fostering the operational resilience of civil society organizations by advancing cybersecurity capacity building and promoting cyber awareness and cyber resilience approaches.

Jamie Tomasello, <u>jtomasello@gmail.com</u>

Languages: English Region: Global, USA

Area of expertise/focus: Policy & Frameworks, Strategy

Jamie has been addressing information security and compliance issues for over 20 years at internet service providers, security companies, law firms, and non-profit organizations. Jamie has led teams responsible for incident response, vulnerability management, security awareness, policy development, risk assessments, vendor security assessments, and audits. Jamie is a Certified Information Privacy Professional (CIPP/US and CIPT).

She provides assessments of organizations' digital security and operations, from staff's interactions with funders, intermediaries, clients, and other stakeholders to identify gaps and risks to vendor security reviews. She provides recommendations on best practices and security controls to adopt and implement, including guidance on crafting policies and procedures based on findings from a gap analysis and risk assessment. Jamie also assists organizations in establishing security and resiliency goals and can help with hiring of technical staff. She works closely with executives, engineers, lawyers, non-profit activists and organizers to ensure solutions are implemented in a practical, sustainable way to achieve outcomes aligned with their organizations' risk while keeping the cultural context of the affected teams or communities in mind.

Felix Atandi, felix@cybertembo.com

Languages: English, Kiswahili

Region: Global, Sub-Saharan Africa

Area of expertise/focus: Forensics, Incident Response, Threat Intelligence

Felix is a diligent cybersecurity professional who has been consistently praised as efficient by his peers, co-workers and management. Over the course of his career, he has developed a skill set directly relevant to audit risk, governance, digital forensics and

cybersecurity. Felix has a Masters degree in Computer Forensics and Cybersecurity from the University of Greenwich.

Felix collaborates with technical vendors and information security analysts to provide early indicators and warnings and contribute to predictive analysis of malicious activity. He also gathers and assesses internal business needs and creates custom solutions to resolve issues like system slowdowns, malware and ransomware outbreaks and process bottlenecks. In addition, he coordinates and collaborates with other multi-skilled teams of cybersecurity professionals in the security operation center to provide cost-effective security solutions for clients. He providing data protection and data privacy services including advisory consultancy as well as technical support with data protection tools and technologies, and carries out regular risk assessments and internal and external audit plans.

Maurine Chepkoech, <u>basoichepkoech@gmail.com</u>

Languages: English, Kiswahili

Region: Global, Sub-Saharan Africa

Area of expertise/focus: Training & Education

Maurine is an effective, talented cybersecurity engineer. She has shown great passion in her work through mentoring with organizations including E-Kraal Innovation Hub, Digisafety, SheHacks_ke, AnitaB.org, and KamiLimu. Additionally, she is an inspiring leader in her community through the various groups that she proactively manages.

Maurine is currently a cybersecurity researcher at E-Kraal Innovation Hub in Nairobi. Her primary role is to perform security assessment and penetration tests for clients' web applications, mobile applications, and networks and create comprehensive reports of her findings and recommendations. She also co-leads Digisatey, a training and mentoring program on accessible online security under the Mozilla Open Leaders X program. As a team, they believe in raising awareness of digital safety and empowering new voices of cyber champions in Kenya. She is passionate about mentoring, which she undertakes

with several women-in-technology groups in Kenya.

Sarah Aoun, sarah@opentech.fund Languages: Arabic, English, French Region: Global, MENA, Lebanon, USA

Area of expertise/focus: Training & Education, Strategy, Incident Response

Sarah Aoun is a Lebanese activist and human rights technologist. Currently, she is the Chief Technologist at the Open Technology Fund. She works with activists, journalists, and high-risk communities on security and privacy. She has given numerous trainings on operational and digital security, and has worked with several groups and NGOs to set up organizational security practices. Sarah currently sits on the board of the Internet Freedom Festival. She was also a Ford-Mozilla Open Web Fellow (2017-2018), an Internet Freedom Fellow (2016-2017), and is currently an advisor to GJS, the Human Rights Foundation, and Reset. You can find her between Beirut and Brooklyn.

Lobsang Gyatso Sither, lobsang@tibetaction.net

Languages: English, Tibetan Region: Global, Tibet, Asia

Area of expertise/focus: Training & Education, Strategy, Incident Response

Lobsang is a Tibetan technologist who has worked for more than a decade in the Tibetan community working with different civil society organization and individuals for digital security needs ranging from digital security training, content development, and digital security policy development to implementation and infrastructure deployment.

Lobsang works on developing digital security practices focused on identified threats and implementing such practices through policy and training. He finds that digital security is a balance among threats, capacity, mitigation and culture (office or cultural). Finding that balance is a process that he has worked on when working with different groups. He has also worked with organizations on tool deployment and to better understand their needs as well as capacity and then deploying a tool/service that would provide better digital

security and needed technical resources. Another aspect of his work is research on targeted attacks and creating incident response workflows for combating such types of attacks, whether individual or community-based.

Mario Felaco, mario@conexo.org

Languages: English, Spanish Region: Global, Latin America

Area of expertise/focus: Training & Education, Strategy, Incident Response

Mario entered the space from the technical side when volunteering with civil society organizations. When he and his associates identified the need, they started working on the development of software tools and then focused on organizational security. They are now developing Conexo as a Latin American hub for security assistance and training for organizations and new auditors/trainers.

Mario assists vulnerable communities and organizations (like NGOs, journalists, activists, and human rights defenders) with their holistic security with a focus on the digital side. He and his colleagues achieve that by performing security audits (based on SAFETAG), training, and assisting with the long-term implementation of security measures. They also train new auditors and trainers and develop new software tools for the security space.