



Security Risk Management for Activists

Practical Tips and Strategies



Activists generally function at the higher end of the risk tolerance threshold, and as such face a wide spectrum of security risks, from detention and other physical harm and threats, to digital surveillance and harassment.

These can challenge both personal security and the effectiveness of campaigns.

Creating a Security Culture and normalising routines where security becomes an embedded part of daily activist work is therefore crucial to ensuring effective and collective Security Risk Management.

This Risk Focus piece will explore some of these key elements including:

- **Physical Risks**

- **Digital Risks**

- **Psychological Risks**

- **Practical Mitigation Strategies**

Physical risks are complex, evolving, and often intentionally designed to silence activism. These can include surveillance in public spaces, harassment, arrest and detention, and targeted attacks.

Impact: physical safety, freedom, emotional well-being, and ability to sustain activism.

Requirements: monitoring and adaptation of security strategies to manage and mitigate.

Digital risks for activists are multi-faceted and evolving, including threats from surveillance, hacking, phishing, social media monitoring, and targeted doxxing (publicly revealing personally identifiable information about an individual or organisation without their consent).

Impact: activists' privacy, safety, and ability to organise effectively in hostile environments.

Requirements: robust digital security measures, awareness, and resilient communication strategies to mitigate.

Psychological risks to activists are cross-cutting and include depression, anxiety, stress, burnout, compassion fatigue and trauma from lived experiences.

Impact: activists can become hypersensitive to injustices, feel morally obligated to continue their work, and face exhaustion, emotional detachment, and loss of motivation.

Requirements: a special focus on mental and emotional wellbeing strategies from professional support to peer-to-peer initiatives.

Practical Mitigation Strategies can include:

- **Ongoing Risk and Stakeholder Identification and Mapping:** this will allow activists to anticipate, understand, and respond proactively to threats as well as prepare practical mitigation strategies to reduce harm and strengthen resilience.
- **Training:** this will equip activists with essential knowledge, skills, and practical tools needed to effectively and safely engage in actions and campaigns.



Emergency Preparedness: This can include memorising key emergency contacts, being aware of one's rights, ensuring that a lawyer or support group is ready and briefed, and establishing safe words or codes to signal danger.



Long-term Preparedness : this can include ensuring plans are in place for administrative needs and to support and liaise with family members and loved ones in case of long-term absences (such as detention for example).

- **Digital Hygiene:** This can include securing devices with strong passwords and encryption, regularly updating software, using separate or "clean" devices for sensitive tasks and managing social media with pseudonyms and privacy settings to reduce exposure.
- **Wellbeing Support:** this can include a combination of self-care practices, emotional support systems and professional support which can collectively help sustain activist commitment and resilience over time.

At **ILS**, we support human rights activists and organisations in navigating these landscapes - helping build ethical, secure, and effective security risk management frameworks even for the most challenging environments.

👉 **Let's talk.** If you or your organisation are looking to strengthen your security framework we'd love to hear from you.