Digital Democracy Initiative

TRAINER'S

Module

DIGITAL SAFETY, READINESS AND OPERATIONAL RESILIENCE

ADI SOUTH ASIA accountabilitylab

Table of Content

1. Introduction

This module brings together a set of sessions designed to help civil society organisations understand and navigate the realities of digital democracy, risk, and resilience in South Asia. It treats digital spaces not as neutral tools, but as contested environments where power, visibility, and vulnerability intersect. Across the sessions, the module traces a clear arc: from understanding how digital participation shapes civic life, to recognising the safety gaps that emerge when access grows faster than protection, to mapping concrete digital risks and building practical systems of cybersecurity, data protection, and secure communication.

The module does not approach digital safety as a narrow technical field. Instead, it frames it as an operational and political necessity for organisations working on rights, accountability, and public-interest advocacy. It looks at digital democracy in practice, the structural nature of threats such as surveillance, harassment, and disinformation, and how data, platforms, and communication channels can be weaponised against civil society. At the same time, it remains grounded in the day-to-day realities of organisational work: how files are stored, how accounts are secured, how staff communicate, and how campaigns are run. Each session is structured to deepen understanding while offering concrete, context-aware guidance that organisations can translate into practice.

By the end of this module, participants should see digital safety and cybersecurity not as external add-ons, but as integral parts of their advocacy, organising, documentation, and narrative-building. The module aims to equip them with the language, concepts, and frameworks needed to assess their own exposure, make informed decisions about tools and workflows, and build an organisational culture in which digital resilience is shared, intentional, and sustainable.

2. Who this module is for

This module is designed primarily for staff and leadership of civil society organisations, networks, and informal collectives who are already engaged in, or increasingly dependent on, digital tools for their work. It is particularly relevant for organisations operating in South Asian contexts where civic space is constrained, online discourse is polarised, and digital environments are shaped by surveillance, harassment, and disinformation. The content speaks directly to practitioners who manage campaigns, run programmes, document rights violations, engage with media, or coordinate communities through digital channels.

It is equally relevant for journalists, researchers, and advocacy groups whose work exposes them to elevated levels of digital scrutiny and hostility, especially those working on sensitive issues such as governance, corruption, minority rights, gender justice, or state accountability. While the module assumes no deep technical background, it does assume participants have regular exposure to digital platforms, communication tools, and data-handling responsibilities. It is written for people who make strategic and operational decisions about how their organisations show up online, how they store and share information, and how they protect the communities they work with.

The module is also useful for programme managers, digital leads, and organisational focal persons tasked with improving internal policies and practices around digital safety, cybersecurity, and data governance. For them, it offers a coherent framework that connects high-level concepts like digital democracy and civic space to very practical questions of passwords, backups, storage choices, and secure workflows.

3. Session 1: Digital Democracy in Practice

[Presentation Attached: Session 1 - Digital Democracy in Practice]

3.1. Introduction

Digital democracy in South Asia has evolved into a defining layer of civic participation, activism, governance, and public discourse. It is no longer an optional space for civil society organisations; it is the environment in which influence is shaped, rights are negotiated, and communities seek visibility. This session helps trainees understand how digital participation works in practice, why it matters for CSOs, and why digital safety is the underlying condition that determines whether digital democracy can function meaningfully for vulnerable groups.

3.2. Understanding digital democracy

Digital democracy refers to the use of digital tools, platforms, and networked information systems to enable participation, accountability, and civic engagement. In the South Asian context, this concept extends beyond voting technologies or civic portals. It encompasses the sprawling online ecosystem ewhere public debate, mobilisation, rights advocacy, watchdog work, and state–citizen interaction now unfold. Digital democracy is expressed through online petitions, hashtag movements, civic reporting, crowdsourced documentation, investigative journalism, policy advocacy campaigns, and the ability of citizens to scrutinise power structures through independent digital media.

Key takeaway: In the region's socio-political landscape, digital participation has become both an equaliser and a battleground.

3.3. Why digital participation has become central to civil society

Civil society organisations in South Asia have historically faced barriers of geography, resources, literacy, and access to mainstream media. Digital spaces have opened pathways that allow CSOs to bypass traditional gatekeepers, reach dispersed communities, mobilise rapidly in moments of crisis, and amplify voices that otherwise remain marginalised. Online platforms provide scale and immediacy, helping CSOs shape public narratives around rights, transparency, gender, climate justice, minority protection, and democratic freedoms.

However, this rising influence has also made CSOs increasingly visible to powerful state and non-state actors. Surveillance, targeted harassment, smear campaigns, censorship, and coordinated digital attacks have become common tools used to weaken civil society's reach. As digital visibility has expanded, dependency on platforms has also deepened, making digital participation not only central to civil society work but also inseparable from the political risk landscape.

3.4. The South Asian context

South Asia is marked by complex political histories, strong majoritarian currents, fragile civic freedoms, and deeply polarised online discourse. This environment shapes how digital democracy functions. Internet shutdowns, content takedowns, data localisation pressures, opaque algorithmic moderation, and disinformation campaigns create an unstable terrain for civil society. In Pakistan, India, Bangladesh, Sri Lanka, and Nepal, CSOs increasingly operate in a dual reality where digital platforms provide unprecedented reach yet simultaneously expose them to vulnerabilities.

Digital participation has particularly expanded among youth populations who are mobile-first and highly connected, creating new channels for political expression. Yet the region's uneven digital literacy, gendered access divide, and infrastructural challenges shape who gets to participate and whose voices remain excluded. Digital democracy in South Asia is therefore a contested space, shaped by both empowerment and risk.

3.5. Why digital safety is the foundation of digital engagement

Digital democracy cannot function if civil society actors are not safe. Every layer of digital engagement relies on secure access, protected identities, resilient systems, and the ability to communicate without fear of surveillance, retaliation, or loss of critical data. Without digital safety, online organising becomes vulnerable to disruption, campaigns collapse under coordinated attacks, staff fall prey to phishing and social engineering, and sensitive information can be weaponised by hostile entities.

Digital safety is not a technical add-on but the structural base that allows CSOs to participate freely. When digital safety fails, digital democracy fails for civil society actors. This is especially true in South Asia where CSOs often deal with high-risk communities, politically sensitive issues, human rights documentation, and evidence-based advocacy that can attract state pressure. A secure digital foundation protects not only organisations but also the communities they represent.

Key takeaway: The quality of civic engagement in any digital democracy is inseparable from the degree of safety citizens experience online. When people cannot participate without fear of surveillance, harassment, or retaliation, the democratic promise of the digital sphere collapses. Digital safety, therefore, becomes the actual foundation upon which meaningful digital democracy rests.

3.6. Power, visibility, and exposure

One of the central dynamics of digital democracy is the trade-off between visibility and vulnerability. As CSOs gain digital influence, their exposure increases. Online platforms reward visibility, but visibility invites attention from adversarial actors. The more a CSO engages online, the more essential it becomes to invest in threat modelling, behavioural safety practices, secure communications, and organisational resilience.

Digital participation has also placed CSOs in direct competition with coordinated disinformation networks, troll armies, and influence operations that aim to drown out independent voices and distort civic debates. This dynamic makes digital safety work not merely protective but strategic, helping organisations maintain agency and credibility in contested digital environments.

3.7. Case study: South Asian digital mobilisation

Examples across the region illustrate how digital participation has altered civic landscapes. The Aurat March in Pakistan, the farmers 'protests in India, the Aragalaya movement in Sri Lanka, and student-led activism in Bangladesh all relied heavily on digital organising, networked mobilisation, and online narrative shaping. These movements also encountered aggressive digital harassment, smear campaigns, account takeovers, doxxing incidents, and surveillance attempts. Each case demonstrates that digital democracy operates only when there are sufficient digital safety and operational resilience to withstand pressure.

For instance, research from Media Matters for Democracy in Pakistan shows a growing pattern of self-censorship among women journalists, many of whom increasingly avoid posting their work online due to persistent harassment, intimidation, and gendered cyber-bullying.

3.8. Practical implications for CSOs

For civil society professionals, understanding digital democracy means recognising that their work now occurs in an environment shaped by algorithms, data trails, platform governance rules, and adversarial online behaviour. Effective participation requires knowledge of digital footprints, platform policies, information integrity threats, and secure operational practices. Building digital resilience becomes synonymous with enabling civic participation.

Organisational policies must evolve to match this reality, incorporating secure communications, internal access controls, safe social media practices, data minimisation, and contingency planning for account compromise or network disruptions. Every staff member, from leadership to field workers, becomes a stakeholder in digital safety because each online behaviour carries implications for the organisation's collective security.

Further reading and verified external resources

- Tactical Tech – The Influence Industry and digital civic engagement https://tacticaltech.org/projects/the-influence-industry/
- EFF – Surveillance, digital rights, and user protection https://www.eff.org/issues
- Access Now – Digital rights crisis response and internet shutdown documentation https://www.accessnow.org/keepiton/
- Citizen Lab – Research on surveillance, spyware, and information controls https://citizenlab.ca/research/
- CIVICUS Monitor – Tracking civic space conditions globally https://monitor.civicus.org/
- Media Matters for Democracy — Report on self-censorship of women journalists https://mediamatters.pk/media-matters-for-democracy-launches-a-new-study-examining-the-impact-of-online-harassment-on-women-journalists/

4. Session 2: The Safety Gap — When Digital Access Outpaces Protection

[Presentation Attached: Session 2 - The Safety Gap When Digital Access Outpaces Protection]

4.1. Introduction

Across South Asia, digital access has expanded rapidly, bringing millions of people online and integrating digital tools into the everyday functioning of civil society. But this expansion has not been accompanied by equally strong safeguards. The result is a widening gap between how much CSOs rely on digital platforms and how little protection they have against threats that emerge from those same platforms. This gap is not theoretical, but it directly shapes how safe organisations are, how effectively they can operate, and how freely civic actors can participate.

Session 2 examines this "safety gap," why it exists, and how it systematically increases risk for civil society organisations, activists, and journalists.

4.2. Understanding the safety gap

The safety gap refers to the growing difference between the level of digital engagement that civil society must maintain to function in modern public life and the level of security, privacy, and resilience it actually possesses. In South Asia, CSOs depend heavily on digital tools for outreach, mobilisation, documentation, coordination, and fundraising. Yet most organisations lack adequate protection against digital surveillance, data exploitation, cyberattacks, coercive requests for information, and targeted harassment. The gap is structural, not individual; CSOs are pushed into digital spaces that were never designed with their safety needs in mind.

4.3. Why access does not equal protection

Widespread connectivity is often mistaken for empowerment. But access without safeguards exposes CSOs to a series of risks that are deeply intertwined with the political and social environment of the region. Increased visibility exposes staff to threats. Digital records make organisations more traceable. Heavy reliance on social platforms gives adversaries more entry points. Low digital literacy increases vulnerability to social engineering and manipulation. CSOs that depend on local storage, which is common across the region, face additional threats during physical raids or device seizures.

Key takeaway: The narrative that "more access automatically creates more democracy" collapses when examined through the lived experiences of CSOs who face disproportionate targeting.

4.4. South Asian examples of the safety gap

The safety gap appears across the region in different ways. In Pakistan, journalists and activists often face coordinated online harassment campaigns that exploit their digital footprints, leaving them no real recourse on platforms.

In India, for instance, the safety gap has been sharply illustrated by verified spyware attacks against human rights organisations and activists. A joint investigation by Amnesty International and the Citizen Lab documented a coordinated campaign in which Indian human rights defenders were targeted with

highly intrusive spyware, including Pegasus, delivered through tailored phishing messages designed to compromise their devices.

This operation affected lawyers, activists, and researchers working on politically sensitive issues, and the findings were published with technical evidence confirming malicious infrastructure linked to commercial surveillance tools. The episode demonstrated how quickly digital participation becomes a liability when protections do not keep pace with access, and how civil society actors are often the first to experience the consequences of such state-aligned surveillance.

In Bangladesh and Sri Lanka, digital spaces have repeatedly been weaponised during periods of political unrest, elections, and social crises, creating hostile environments that directly undermine civil society work.

Research and documentation by organisations such as CIVICUS Monitor, Access Now, and Article 19 show how online disinformation campaigns, coordinated harassment, platform manipulation, and internet restrictions intensify during moments of political tension, shrinking civic space precisely when public engagement is most needed.

In Bangladesh, activists and journalists have faced digital intimidation alongside restrictive cyber laws that amplify fear and self-censorship, while in Sri Lanka, periods of protest have coincided with online manipulation, surveillance concerns, and episodic internet shutdowns. Across the wider South Asian region, these dynamics disproportionately affect women, minorities, informal collectives, and youth-led organisations, who experience heightened harassment, identity-based abuse, and exposure without corresponding legal, technical, or platform-level protections. This pattern illustrates how digital exposure, when unaccompanied by safeguards, systematically marginalises already vulnerable civic actors rather than empowering them.

The safety gap is not uniform. It affects some groups more severely than others. Women face gendered harassment that is explicitly designed to silence them. Youth-led or unregistered organisations face threats because they often operate without dedicated technical support. Groups working on sensitive issues like enforced disappearances, religious minorities, or state accountability face risks of targeted surveillance. These gaps compounded together create a systemic disadvantage, limiting democratic participation in the very spaces meant to expand it.

4.5. How the safety gap increases organisational risk

When protection does not grow alongside digital access, organisations face heightened exposure in several ways. Increased reliance on social media creates dependency on platforms whose moderation, security settings, and algorithms are opaque. Weak internal systems increase the probability of account compromise or data leaks. Staff unfamiliar with basic cyber hygiene often use the same passwords across personal and organisational accounts. Sensitive data stored locally becomes vulnerable to confiscation or tampering during raids or at border crossings. And when harassment escalates, organisations often lack documented protocols for response, leaving individuals to navigate digital attacks alone.

This situation directly affects organisational continuity. Digital disruptions can halt campaigns, compromise documentation, damage credibility, or create fear that discourages staff from engaging publicly. In extreme cases, it results in withdrawal from civic spaces, further weakening democratic processes.

4.6. Consequences for civic participation

The safety gap produces a chilling effect where CSOs hesitate to publish, document abuses, or speak openly due to fears of digital retaliation. It discourages field workers from capturing sensitive evidence. It reduces the willingness of communities to engage with organisations online, particularly when surveillance is a known threat. It pushes women, minorities, and at-risk groups into silence. The gap, therefore, reshapes the landscape of civic engagement, not by blocking access outright, but by making participation dangerous.

A digital democracy cannot function meaningfully when the people who most need protection are the least protected. The safety gap systematically narrows civic space by making risk a daily operational reality.

4.7. Practical implications for CSOs

Understanding the safety gap is critical because it forces organisations to recognise that digital safety is not a matter of technical upgrades but a shift in organisational culture. This means acknowledging that every campaign, every outreach effort, and every internal communication carries a digital footprint that must be protected deliberately. CSOs must begin integrating safety into the way they plan, strategise, and execute their digital engagement. This includes mapping vulnerabilities, investing in staff training, reducing unnecessary data collection, rethinking storage practices, and developing clear internal protocols for harm response.

The objective is not to eliminate digital risk, which is impossible, but to narrow the safety gap to a point where it no longer undermines the organisation's work or its ability to contribute to democratic processes.

4.8. Case study illustration based on patterns across uploads

One recurring pattern in South Asian CSO digital behaviour is the over-reliance on personal devices and accounts for organisational work. This creates a critical vulnerability. A single compromised device or personal account can expose entire organisational networks, internal communications, donor information, advocacy plans, and sensitive field data. Because digital access has expanded without accompanying structural protection, these risks are widespread across organisations, regardless of size or capacity.

Recommended external readings:

- Access Now – Internet shutdowns and their impact on civic rights https://www.accessnow.org/keepiton/
- Tactical Tech – The Data Detox Kit (organisational and individual protection guidance) https://datadetoxkit.org

- Citizen Lab – Analysis of targeted digital threats against civil society https://citizenlab.ca/research/
- CIVICUS Monitor – Documentation of shrinking civic spaces https://monitor.civicus.org
- EFF – Guidance on surveillance and digital security awareness https://www.eff.org/issues/surveillance

5. Session 3: Mapping Digital Risks and Vulnerabilities

[Presentations Attached: Session 3.1 - Mapping Digital Risks and Vulnerabilities & Session 3.2 - Key Digital Risks Facing Civil Society Organisations]

5.1. Introduction

Digital risks faced by civil society organisations are neither random nor evenly distributed. They are shaped by context, visibility, issue areas, organisational structure, and the identities of those involved. This session explores risk recognition, helping participants understand what kinds of digital threats exist, how they operate in practice, and why some organisations and individuals are systematically more exposed than others. The objective is not to create fear, but to build informed awareness that allows CSOs to anticipate threats and reduce harm.

5.2. Understanding digital risk in civil society work

Digital risk refers to the potential for harm arising from the use of digital technologies, platforms, and data in the course of organisational work. For CSOs, these risks are embedded in everyday activities such as communicating with partners, storing sensitive information, documenting abuses, running campaigns, or maintaining online visibility. Unlike traditional security threats, digital risks are often invisible until harm occurs. They operate through data trails, metadata, compromised credentials, platform governance failures, and hostile digital behaviours that exploit openness and trust.

5.3. Surveillance and monitoring

Surveillance is one of the most significant digital risks facing civil society in South Asia. It can take the form of state-led monitoring, commercial spyware, platform-level data collection, or informal surveillance by political actors and adversarial groups. Surveillance does not always involve sophisticated tools. It often relies on monitoring social media activity, metadata analysis, location tracking, and access to cloud-stored information. For CSOs working on sensitive issues, surveillance can expose networks, identify sources, and create chilling effects that discourage participation.

Documented research by Citizen Lab and Amnesty International has repeatedly shown that surveillance technologies are disproportionately deployed against activists, journalists, lawyers, and human rights defenders, making surveillance a structural risk rather than an exceptional one.

5.4. Harassment, intimidation, and coordinated attacks

Online harassment is a deliberate tactic used to silence, discredit, or exhaust civil society actors. It often appears as trolling, threats, smear campaigns, impersonation, or coordinated reporting designed to

trigger content takedowns or account suspensions. These attacks are rarely isolated; they are frequently organised and sustained over time. For organisations, harassment disrupts campaigns, damages credibility, and shifts resources away from substantive work toward crisis management.

Harassment becomes particularly effective when platforms fail to act quickly or consistently, leaving CSOs exposed to abuse with limited recourse. Over time, this creates an environment where withdrawal from public digital spaces feels safer than engagement.

5.5. Doxxing and exposure of personal information

Doxxing involves the malicious publication of private or identifying information such as home addresses, phone numbers, family details, or workplace data. For civil society actors, doxxing transforms online hostility into real-world risk. It enables offline intimidation, stalking, and threats, and often precedes physical harm or legal harassment.

Doxxing is especially dangerous in environments where law enforcement responses are weak or politicised. Once personal data circulates online, it is almost impossible to fully contain, making prevention and early mitigation critical components of digital safety planning.

5.6. Data seizure, loss, and compromise

Civil society organisations routinely handle sensitive data, including testimonies, contact lists, donor records, internal strategies, and documentation of abuses. When this data is inadequately protected, it becomes vulnerable to seizure, loss, or unauthorised access. Data risks arise from device confiscation, insecure local storage, weak access controls, malware infections, or account takeovers. In many South Asian contexts, reliance on personal laptops, shared devices, and locally stored files significantly increases exposure. Data compromise can endanger communities, undermine trust, and in some cases expose individuals to legal or physical retaliation.

5.7. Gendered digital violence

Digital risks are not gender-neutral. Women and gender-diverse individuals face distinct forms of online abuse that are sexualised, identity-based, and explicitly designed to shame or silence. Gendered digital violence includes threats of sexual harm, circulation of manipulated images, character assassination, and attacks targeting family and personal morality.

Research by organisations such as Tactical Tech, UN Women, and APC shows that women journalists, activists, and organisers are more likely to self-censor or withdraw from digital spaces after sustained harassment. For women-led organisations, this risk extends beyond individuals to the organisation's public presence and sustainability.

5.8. Who is most at risk

Digital risk concentrates around certain characteristics rather than organisational size alone. Youth-led organisations often lack institutional protection, legal backing, or technical support. Informal or unregistered collectives operate without the safeguards that larger NGOs may have, making them easier targets. Women-led organisations face compounded risks due to gendered abuse. Groups working on

politically sensitive issues such as minority rights, enforced disappearances, corruption, or state accountability attract disproportionate attention from hostile actors.

Understanding who is most at risk helps organisations move away from one-size-fits-all security approaches and toward context-specific protection strategies.

5.9. Risk mapping as a practical tool

Risk mapping is the process of identifying what digital assets an organisation relies on, what threats it faces, who might target it, and what the potential consequences of compromise could be. Effective risk mapping connects organisational activities with likely threats rather than assuming generic danger. It encourages CSOs to ask practical questions about visibility, data sensitivity, communication channels, and dependency on platforms.

Risk mapping is not a one-time exercise. It must evolve as campaigns change, political contexts shift, and organisations grow or become more visible.

5.10. Why recognising vulnerability is empowering

Acknowledging vulnerability is often perceived as weakness, but in digital safety work it is a source of strength. Organisations that understand their exposure can take informed steps to reduce it.

Mapping risks allows CSOs to prioritise protections, allocate limited resources strategically, and design safer ways to engage digitally without retreating from civic participation altogether. The goal of risk mapping is not to eliminate risk, but to prevent avoidable harm and ensure that digital participation remains possible, sustainable, and aligned with organisational values.

5.11. Case studies from the South Asian region

Citizen Lab and Amnesty International have extensively documented targeted spyware attacks against South Asian civil society. One widely cited case is Amnesty International's "Targeted Surveillance in India" investigation, which uncovered Pegasus infections on the devices of Indian human rights defenders, lawyers, and Dalit activists in 2019, along with technical analysis by

Citizen Lab confirming links to known Pegasus operators. The full report is available at https://www.amnesty.org/en/latest/research/2019/10/india-targeted-surveillance-of-human-rights-defenders

A related Citizen Lab publication, examining the infrastructure used against Indian activists in the Bhima Koregaon case, provides further forensic evidence of sophisticated targeting: https://citizenlab.ca/2020/12/forensic-analysis-reveals-evidence-of-device-compromise-in-bhima-koregaon-case/

Bangladesh has seen systematic digital manipulation documented by Access Now and Amnesty International. During the 2018 elections, Access Now reported coordinated disruptions, network throttling, and targeted online harassment of journalists and activists.

Their findings remain archived and accessible here: https://www.accessnow.org/bangladesh-election-digital-rights

Amnesty International's investigation into the Digital Security Act (DSA) shows how digital surveillance, arrests, and intimidation have consistently targeted journalists and CSOs, creating a climate where online engagement becomes a source of danger: https://www.amnesty.org/en/latest/news/2021/02/bangladesh-digital-security-act-thrives-in-culture-of-fear/

Sri Lanka's 2022 Aragalaya movement provides a stark example of digital manipulation during political upheaval. The Sri Lanka Internet Shutdown Observatory and Access Now documented repeated disruptions to social media platforms and messaging services during protests, limiting the mobilisation capacity of civil society groups.

Access Now's detailed documentation of these shutdowns is available at: https://www.accessnow.org/sri-lanka-internet-shutdowns-2022/

Civil rights researchers have further recorded coordinated online disinformation and targeting of protest leaders, generating an atmosphere where civic actors were forced to restrict online participation.

Gendered digital violence is heavily documented across the region. The Association for Progressive Communications (APC) provides verified research showing the disproportionate targeting of women journalists across South Asia, including patterns of sexualised threats, doxxing, and smear campaigns that lead directly to self-censorship.

Their report can be accessed at: https://www.apc.org/en/pubs/weapons-of-control-human-rights-violations-gendered-online-violence

Similarly, Media Matters for Democracy's own research in Pakistan documents how online abuse pushes women journalists away from public digital spaces: https://mediamatters.pk/women-journalists-study/

5.12. Further reading and external resources

- Citizen Lab – Research on targeted digital surveillance and civil society https://citizenlab.ca/research/
- Tactical Tech – Digital risk, data exploitation, and activist safety https://tacticaltech.org/resources/
- Access Now – Digital security helpline and threat documentation https://www.accessnow.org/help/
- Association for Progressive Communications – Gendered digital violence research https://www.apc.org/en/work/online-gender-based-violence
- Electronic Frontier Foundation – Threat modelling and digital self-defence https://ssd.eff.org

6. Session 5: Cybersecurity for CSOs and Core Concepts

[Presentation Attached: Session 5 - Cybersecurity for CSOs and Core Concepts]

6.1. Introduction

Cybersecurity for civil society organisations is often misunderstood as a purely technical space reserved for specialists. In reality, it is the set of everyday organisational practices that protect staff, data, communities, and mission-critical work from disruption, manipulation, theft, or surveillance. For CSOs in South Asia, cybersecurity is not just an IT concern; it is an operational survival requirement. This session reframes cybersecurity as a practical, accessible, and essential organisational practice instead of a technical burden.

6.2. What cybersecurity means for CSOs in practice

Cybersecurity in civil society contexts refers to safeguarding people, information, devices, and workflows from threats that exploit digital systems. Unlike private companies, CSOs often work in politically charged environments, operate with limited resources, and manage sensitive data about vulnerable communities. This makes them attractive targets for adversarial actors who use digital means to undermine credibility, disrupt campaigns, access private communication, or intimidate staff.

In practical terms, cybersecurity for CSOs means ensuring that communications cannot be intercepted, sensitive data cannot be easily seized, accounts cannot be compromised, and campaigns cannot be derailed by malicious activity. It also means that staff feel confident using digital tools without exposing themselves or their communities to unnecessary risks. Cybersecurity becomes a protective layer that preserves the integrity of advocacy, field work, research, and community mobilisation.

6.3. Cybersecurity as organisational protection, not technical jargon

Cybersecurity must be embedded in the organisational culture, not treated as a set of confusing instructions or ad-hoc fixes. When organisations rely on multiple devices, shared accounts, varied communication channels, and public-facing platforms, every weak point can compromise the entire system. Many CSOs also operate with decentralised teams, volunteers, or part-time staff, making consistent security harder to enforce.

By viewing cybersecurity as organisational protection, the focus shifts from tools to behaviour. Instead of learning “technical concepts,” organisations build routines that lower risk: structured access control, safe file-sharing, strong authentication, updated devices, and secure communication norms. This shift empowers non-technical staff by allowing them to understand how their actions influence organisational risk and resilience.

6.4. Common misconceptions about cybersecurity in civil society

Many CSOs assume they are too small to be targeted or that they lack information worth stealing. In practice, civil society groups are often targeted exactly because they work on sensitive issues such as governance, accountability, minority rights, conflict documentation, or advocacy around state violence. Another misconception is that privacy tools alone are enough. In reality, effective cybersecurity requires

behavioural consistency, organisational processes, and a clear understanding of the threat environment. Technical tools cannot replace the need for organisational planning. A CSO with the most advanced encrypted tools can still be compromised if staff reuse passwords, store sensitive files on unencrypted laptops, or forward confidential documents over insecure channels.

6.5. The threat environment for CSOs

Civil society organisations face a wide range of adversarial actors. These can include government agencies conducting surveillance or intrusive data collection, political groups engaged in harassment or intimidation, and non-state actors such as troll farms, extremist networks, or private contractors deploying spyware or social engineering tactics. In some cases, threats come from within the organisation through weak protocols, shared credentials, or compromised personal devices. Across South Asia, digital threats against civil society are well documented. Amnesty International and Citizen Lab have exposed repeated incidents of spyware campaigns targeting human rights defenders, lawyers, and activists. Access Now's Digital Security Helpline has recorded hundreds of cases involving phishing, credential compromise, and social engineering targeting CSOs. These patterns demonstrate that digital threats are structural, not occasional.

6.6. Why cybersecurity must be proactive

Organisations often respond to digital threats only after harm has occurred. But cybersecurity is most effective when it focuses on preventing incidents before they escalate. Proactive measures reduce exposure, prevent data loss, and increase resilience during crises such as coordinated harassment or attempted account compromise.

Being proactive also protects communities. Many CSOs hold sensitive testimonies, personal details, or politically sensitive communication. A breach does not just affect the organisation; it affects people who may face real-world harm. Proactive cybersecurity, therefore becomes an ethical obligation for civil society groups.

6.7. Building a culture of cybersecurity

The most effective cybersecurity practice inside CSOs is building habits rather than purchasing tools. This means developing shared vocabulary around risks, maintaining updated devices, ensuring controlled access to sensitive data, and educating staff on avoiding phishing or manipulation. It also requires clear internal rules for how information is stored, shared, and archived.

A culture of cybersecurity makes safety part of everyday workflow. Staff know where to store files, how to communicate securely, who has access to what, and what to do if something suspicious happens. This reduces reliance on individual technical skills and turns safety into a collective organisational responsibility.

6.8. Practical implications for team workflows

Cybersecurity becomes practical when it is integrated into daily routines. Teams should know how to identify suspicious links, verify unknown emails, secure their accounts with strong authentication, and avoid mixing personal and organisational work on the same devices. Senior leadership must understand

that cybersecurity failures can result in operational shutdowns, legal exposure, and loss of credibility. Teams must adopt safer communication practices and maintain clear separation between public-facing work and sensitive internal coordination.

These behaviours ensure digital safety is not an afterthought but part of how the organisation functions.

6.9. Key foundational principles of cybersecurity for civil society organisations

Cybersecurity for CSOs rests on a small number of foundational principles that guide how organisations protect themselves in practice. These principles are not technical rules; they are ways of thinking about risk, responsibility, and protection in a digital environment that is often hostile to civic work. The first foundational principle is that cybersecurity is about people before technology. Most digital harm experienced by civil society organisations does not occur because systems are sophisticatedly hacked, but because people are manipulated, credentials are exposed, or unsafe behaviours are normalised. Phishing, social engineering, weak passwords, and shared accounts remain the most common entry points for attacks. This means that staff awareness, habits, and decision-making are the first and most important line of defence. Cybersecurity succeeds when people understand how their everyday actions shape organisational risk.

The second principle is that access should always be limited and intentional. Not everyone in an organisation needs access to everything. Sensitive data, administrative accounts, and decision-making systems should be accessible only to those whose roles genuinely require it. Over-broad access dramatically increases the impact of a single compromised account or device. This principle recognises that internal exposure can be as damaging as external attacks and that controlling access is a form of harm prevention. The third principle is that data should be treated as a liability as well as an asset. CSOs often focus on collecting information for advocacy, documentation, or reporting, but less attention is paid to the risks created by holding that data. The more sensitive data an organisation stores, the greater the consequences if it is seized, leaked, or misused. Foundational cybersecurity therefore involves minimising data collection, retaining information only as long as necessary, and understanding where data is stored and who can access it. Protecting data also means protecting the people behind it.

Another core principle is that cybersecurity must assume compromise is possible. No system is perfectly secure, and no organisation can guarantee that breaches will never occur. Planning for cybersecurity therefore includes planning for failure. Organisations must be able to detect suspicious activity, respond quickly to incidents, and recover without collapsing operations. This principle shifts the focus from fear of attacks to preparedness and resilience, reducing panic when something goes wrong.

Consistency is also a foundational principle. Cybersecurity measures are only effective when they are applied consistently across the organisation. Inconsistent practices, such as mixing secure and insecure communication channels or allowing exceptions for convenience, create weak points that adversaries exploit. Consistency turns security from an individual choice into an organisational standard. Finally, cybersecurity must be proportionate to risk. Not every CSO faces the same level of threat, and not every activity requires the same level of protection. Foundational cybersecurity involves aligning protection measures with the organisation's visibility, issue areas, political context, and the

sensitivity of its work. This prevents both under-protection, which increases harm, and over-protection, which can unnecessarily restrict participation and productivity.

Together, these principles frame cybersecurity as an organisational practice grounded in awareness, restraint, preparedness, and proportionality. They provide a shared logic that allows civil society organisations to make informed decisions about digital safety without needing deep technical expertise.

6.10. External Resources:

- Access Now's Digital Security Helpline offers detailed case studies and practical guidance on common CSO threats, available at https://www.accessnow.org/help/
- The Electronic Frontier Foundation's Surveillance Self-Defense platform provides accessible guidance on threat modelling, secure communication, and device protection, available at https://ssd.eff.org
- Tactical Tech's Data Detox Kit offers step-by-step digital hygiene practices tailored for activists and civil society, available at https://datadetoxkit.org
- Citizen Lab publishes forensic investigations documenting spyware, surveillance, and digital threats against civil society worldwide, available at https://citizenlab.ca/research/

7. Session 6: Common Weaknesses and Everyday Risks

[Presentation Attached: Session 6 - Common Weaknesses and Everyday Risks]

7.1. Introduction

Most cyber incidents affecting civil society organisations do not involve advanced hacking techniques or zero-day exploits. They rely on predictable weaknesses in everyday digital behaviour and organisational routines. This session focuses on how common practices such as weak passwords, shared accounts, lack of two-factor authentication, and unsafe network use become attack vectors.

By understanding how these threats are actually executed in real-world contexts, CSOs can recognise that most digital harm is preventable and that small behavioural changes can significantly reduce risk.

7.2. Why everyday risks are attractive to attackers

Threat actors targeting CSOs tend to prioritise efficiency rather than sophistication. Instead of attempting to break encrypted systems or bypass complex defences, they exploit known human and organisational weaknesses. These weaknesses are attractive because they require minimal resources, are difficult to detect in real time, and often provide broad access once exploited. Everyday risks persist not because organisations are careless, but because convenience, limited capacity, and lack of awareness normalise unsafe practices over time.

7.3. Credential-based attacks and weak passwords

Weak passwords are one of the most frequently exploited entry points in civil society organisations. These attacks rarely involve guessing passwords manually. Instead, attackers rely on credential stuffing,

phishing, or leaked password databases from unrelated services. When staff reuse passwords across personal and organisational accounts, a breach elsewhere can silently expose internal systems.

In practice, an attacker may obtain a staff member's email password from a previous data breach and then attempt to log into cloud storage, social media platforms, or collaboration tools using the same credentials. Once access is gained, attackers can read internal communications, reset other account passwords, impersonate staff, or quietly exfiltrate sensitive data. For CSOs, this can lead to exposure of sources, donor details, advocacy plans, and confidential field information.

7.4. Phishing and social engineering as primary attack methods

Phishing, combined with social engineering, remains the most common method used to exploit everyday weaknesses. These attacks are designed to manipulate trust rather than defeat technology. Phishing emails or messages often appear to come from known contacts, service providers, or colleagues, prompting recipients to click links, download files, or enter login details.

In civil society contexts, phishing is often tailored to organisational work. Messages may reference funding opportunities, event invitations, urgent document reviews, or security alerts. Once credentials are entered into fake login pages, attackers gain direct access to accounts. Social engineering can also occur through phone calls or messaging apps, where attackers pose as IT support, platform representatives, or senior staff members. The effectiveness of these attacks lies in their familiarity and urgency.

7.5. Shared accounts and the collapse of accountability

Shared accounts create structural weaknesses by breaking the link between identity and access. When multiple staff members use the same login credentials, it becomes impossible to know who accessed what, when, or from where. This eliminates accountability and makes incident response extremely difficult. In practice, shared email or social media accounts mean that a single compromised device or careless click can expose the entire organisation. When staff leave, access is often not properly revoked, increasing the risk of long-term exposure. Attackers who gain access to shared accounts can operate undetected for extended periods, monitoring communications or posting malicious content without raising immediate suspicion.

7.6. Absence of two-factor authentication and single-point failure

Without two-factor authentication, passwords become single points of failure. Once a password is compromised, attackers can access accounts without resistance. This makes phishing and credential theft far more damaging. Two-factor authentication disrupts many common attacks by requiring a second form of verification, such as a device-based prompt or code. In its absence, automated attacks and opportunistic intrusions become far more successful. Many CSOs delay enabling two-factor authentication due to concerns about usability, yet the lack of this protection significantly increases exposure across email, cloud services, and social media platforms.

7.7. Unsafe Wi-Fi and network interception

Network-based risks are often underestimated because they are less visible. When staff connect to public or unsecured Wi-Fi networks, attackers can intercept traffic, capture credentials, or manipulate connections through man-in-the-middle attacks. These attacks do not require malware installation and often leave no obvious signs of compromise.

In practice, a CSO staff member working from a café, hotel, or airport may log into organisational accounts over an unsecured network. An attacker monitoring the same network can capture login details or session tokens, later using them to access accounts remotely. For organisations working in high-risk environments or during travel, unsafe network use significantly increases vulnerability.

7.8. Why said weaknesses compound rather than exist in isolation

Everyday weaknesses rarely exist alone. Weak passwords combined with lack of two-factor authentication amplify the impact of phishing. Shared accounts combined with unsafe network use make breaches harder to detect and contain. When these risks overlap, a minor incident can escalate into full organisational compromise.

This compounding effect explains why relatively simple attacks can result in severe consequences for CSOs, including data loss, harassment escalation, reputational damage, and operational disruption.

7.9. The preventable nature of most digital harm

The critical insight from examining everyday risks is that most digital harm affecting CSOs is preventable. These incidents succeed not because defences are too complex to implement, but because basic protections are absent or inconsistently applied. Preventability shifts the conversation from fear to responsibility. It shows that organisations can meaningfully reduce risk through intentional practices rather than advanced technical solutions.

7.10. Organisational responsibility and risk reduction

Addressing everyday weaknesses requires organisational commitment, not individual heroics. CSOs must recognise that insecure practices often arise from unclear policies, informal workflows, and pressure to prioritise speed over safety. By setting clear expectations, providing guidance, and modelling safe behaviour from leadership, organisations can reduce reliance on individual judgement and create safer digital environments.

Everyday risks are the most practical starting point for cybersecurity because they offer the highest return on effort. When addressed systematically, they close the most commonly exploited pathways used against civil society.

7.11. External Resources:

- Electronic Frontier Foundation – Surveillance Self-Defense: Phishing, passwords, and account protection
  https://ssd.eff.org

- Access Now – Digital Security Helpline: Incident patterns affecting CSOs https://www.accessnow.org/help/
- Verizon Data Breach Investigations Report – Credential misuse and phishing trends https://www.verizon.com/business/resources/reports/dbir/
- CISA – Guidance on securing accounts and preventing credential abuse https://www.cisa.gov/secure-accounts

8. Session 7: Cyber Hygiene and Secure Communications

[Presentation: Section 7 - Cyber Hygiene and Secure Communications]

8.1. Introduction

Secure communication is not a single practice but a collection of habits applied differently across communication channels. Email, messaging apps, web calls, and video conferencing each introduce distinct risks, exposure patterns, and failure points. This session breaks cyber hygiene down by communication type, showing how everyday use of common tools can create vulnerabilities and how disciplined practices can significantly reduce harm. For civil society organisations, secure communication is not about secrecy for its own sake; it is about protecting people, relationships, data, and trust.

8.2. Foundations of cyber hygiene across communication channels

Across all forms of digital communication, cyber hygiene rests on a few shared assumptions. Devices must be secure before communication can be secure. Accounts must be protected before messages can be trusted. Behaviour matters as much as technology. No communication channel is inherently safe if used carelessly, and no channel is inherently unsafe if used thoughtfully within clear organisational norms. With these principles in place, CSOs can approach each channel with realistic expectations rather than false confidence.

8.3. Email communication: risks and realities

Email remains one of the most widely used and most exploited communication channels in civil society work. It is particularly vulnerable to phishing, account compromise, forwarding without consent, and metadata exposure. Even when content is encrypted in transit, email headers reveal sender, recipient, timing, and sometimes location, which can be used to map organisational networks and activity patterns.

Attacks via email are usually not technical exploits but deception. Phishing emails impersonate donors, partners, platform providers, or internal staff, prompting recipients to click malicious links or enter credentials. Once an email account is compromised, attackers often use it to reset passwords for other services, quietly monitor conversations, or send further phishing messages from a trusted address. For CSOs, email should be treated as a medium suitable for low to medium sensitivity communication, with heightened caution when sharing documents, personal data, or operational details.

8.4. Messaging apps: encryption does not equal safety

Messaging apps are often assumed to be safe because many advertise end-to-end encryption. In practice, messaging security depends on much more than encryption alone. Risks emerge from insecure device backups, weak account protection, SIM swapping, compromised devices, and unsafe group practices. Common attacks involve account takeover through SIM-based verification, phishing links sent via trusted contacts, or access to unencrypted backups stored in cloud accounts. Group chats also introduce risks, as sensitive information can be forwarded, screenshotted, or accessed by unintended participants. Messaging apps are best suited for real-time coordination, but only when paired with strong account protection, secure devices, and disciplined group management.

8.5. Web calls and voice communication

Web-based voice calls are frequently used for coordination, interviews, and internal discussions, yet they are often treated as inherently private without sufficient scrutiny. Risks include call interception on insecure networks, unauthorised recording, identity exposure, and metadata leakage. In practice, web calls can be compromised when participants join from public Wi-Fi networks, use outdated applications, or rely on accounts with weak authentication. Even when call content is encrypted, participants 'identities, IP addresses, and call timings may still be exposed. For civil society organisations, voice calls should be treated as potentially observable spaces, particularly when discussing sensitive topics. Awareness of who is on the call, how the call is accessed, and whether recordings are enabled is critical.

8.6. Video conferencing: visibility as a risk factor

Video conferencing introduces additional layers of exposure because it combines voice, visuals, metadata, chat logs, and sometimes recordings. Risks include unauthorised access to meetings, accidental disclosure through screen sharing, insecure storage of recordings, and exposure of participants 'identities and locations. Common failures include publicly shared meeting links, lack of waiting rooms or access controls, automatic recording without clear consent, and participants joining from shared or compromised devices. In politically sensitive contexts, video calls can inadvertently reveal organisational hierarchies, participant networks, or physical environments. For CSOs, video conferencing should be approached as a semi-public space unless deliberately secured, with clear norms around participation, recording, and information sharing.

8.7. Cross-cutting risk: backups and device security

Across all communication channels, one of the most underestimated risks is insecure backups. Messages may be encrypted in transit but stored unencrypted in cloud backups tied to weak accounts. Device compromise can expose email, messages, call logs, and stored media regardless of how secure the communication platform itself claims to be. This is why cyber hygiene cannot focus on tools alone. Device updates, strong account protection, and controlled backups are essential for maintaining secure communication across channels. Building organisational norms for secure communication

Secure communication only works when organisations agree on shared practices. This includes clarity on which channels are appropriate for which types of information, how identities are verified, how

access is managed, and what to do when something goes wrong. Without shared norms, individuals make ad-hoc decisions that create uneven risk across the organisation. Organisations that normalise secure communication reduce confusion, limit exposure, and protect staff from having to make high-stakes decisions under pressure.

8.8. External Resources:

- Electronic Frontier Foundation – Surveillance Self-Defense guides on email, messaging, and secure calls
  https://ssd.eff.org
- Access Now – Digital Security Helpline resources on secure communication failures and incident response
  https://www.accessnow.org/help/
- Tactical Tech – Data Detox Kit sections on communication hygiene and metadata awareness
  https://datadetoxkit.org
- Citizen Lab – Research on communication interception, spyware, and targeted surveillance
  https://citizenlab.ca/research/

9. Session 8: Safe Social Media and Online Exposure

[Presentation Attached: Session 8 - Safe Social Media and Online Exposure]

9.1. Introduction

Social media has become the primary public interface through which civil society organisations communicate, advocate, mobilise support, and challenge dominant narratives. It is also the space where these organisations face their greatest exposure to risk. The same visibility that enables reach and influence also attracts harassment, surveillance, impersonation, and coordinated attempts to silence or discredit civic actors. Navigating this environment requires an understanding of how social media platforms function, how exposure is created, and how organisations can balance public engagement with safety.

9.2. Understanding exposure in social media environments

Exposure on social media is structural rather than accidental. Platforms are designed to maximise engagement, often amplifying emotionally charged content and pushing posts beyond their intended audiences. Public profiles, open comment sections, hashtags, and algorithmic recommendations allow content to circulate widely and unpredictably. This circulation creates digital trails that can be analysed by adversarial actors to identify routines, relationships, and vulnerabilities. Every post contributes to an organisation's digital footprint. Timing, interaction patterns, visual content, and engagement behaviour all reveal information. Over time, these fragments can be assembled to map organisational networks, identify individuals behind accounts, and anticipate moments of vulnerability.

9.3. Patterns of harassment, trolling, and intimidation

Online harassment is rarely spontaneous. It often follows recognisable patterns designed to exhaust, intimidate, or silence. These include sustained verbal abuse, identity-based attacks, threats of violence, coordinated swarming of posts, impersonation, and organised mass-reporting aimed at triggering automated platform penalties. Such attacks frequently escalate during politically sensitive moments, major campaigns, or periods of heightened visibility. They are effective because they exploit platform dynamics and human emotional responses. Recognising these patterns allows organisations to respond strategically rather than reactively.

9.4. Coordinated online attacks and manipulation

Coordinated attacks involve deliberate organisation by groups seeking to disrupt civil society work. These operations may include the activation of large numbers of accounts simultaneously, repetition of identical talking points, amplification of misleading narratives, and deliberate flooding of comment sections. The goal of coordination is not debate but overwhelm. By creating the impression of mass hostility, attackers aim to delegitimise organisations, discourage supporters, and pressure platforms into action. Preparedness reduces the effectiveness of these tactics by allowing organisations to identify coordination early and limit its impact.

9.5. Platform vulnerabilities and systemic limitations

Social media platforms were not designed to protect civil society actors operating in high-risk environments. Moderation systems are inconsistent, slow, and often fail to account for local political contexts or targeted abuse. Coordinated actors can exploit reporting mechanisms, while algorithmic amplification can unintentionally prioritise harmful engagement. Public follower lists, open profiles, and visible interaction histories make it easier for adversaries to monitor organisations and their networks. These systemic weaknesses mean that organisations must assume responsibility for their own safety rather than relying on platform protections.

9.6. Content-level risks and unintended disclosure

Social media content can reveal far more than intended. Images may expose locations, faces, or surroundings. Videos can capture identifying details, emotional states, or organisational dynamics. Live broadcasts present particular risks by revealing real-time location and activity. Even text-based posts can expose patterns when viewed collectively. Deleted content often persists through screenshots and archives, making restraint and foresight critical components of safe engagement. Understanding how content can be misused helps organisations make more deliberate decisions about what to share publicly.

9.7. Managing harassment without escalation

Responding to harassment requires discipline. Direct engagement with abusive actors often increases visibility and intensifies attacks. Emotional responses can amplify harmful content and attract further attention.

Effective management involves documenting abuse, using platform tools to limit exposure, and escalating severe cases through appropriate channels. Organisations benefit from predefined response protocols that remove the burden of decision-making from individuals under pressure. Treating harassment as an operational risk rather than a personal conflict reduces its disruptive impact.

9.8. Organisational exposure and internal practices

Social media risk is amplified when organisational roles and boundaries are unclear. When multiple individuals manage accounts without defined responsibilities, or when personal and organisational identities overlap, exposure increases. Staff may be targeted through their personal histories, families, or past statements. Clear separation between personal and organisational accounts, controlled access to official platforms, and shared norms around posting reduce vulnerability. Social media management should be treated as a responsibility that carries both communicative and security implications.

9.9. Reducing exposure while sustaining advocacy

Safety does not require withdrawal from public discourse. It requires intentional engagement. Organisations can reduce exposure by avoiding real-time posting from sensitive locations, limiting personal identifiers, controlling account access, and planning content strategically. Deliberate pacing, careful framing, and internal review processes help maintain influence without inviting unnecessary risk. Advocacy remains effective when it is informed by awareness of platform dynamics and threat patterns.

9.10. Supporting staff facing online abuse

Online harassment has psychological and emotional consequences that can affect wellbeing and professional capacity. Women and marginalised groups often experience intensified, identity-based abuse that extends beyond the digital space. Organisations have a responsibility to support staff through clear reporting channels, internal solidarity, and access to appropriate support resources. Protecting individuals strengthens organisational resilience and preserves long-term capacity for civic engagement.

9.11. External Resources:

- Access Now provides guidance and incident support for civil society organisations experiencing online harassment and digital attacks at https://www.accessnow.org/help/
- The Association for Progressive Communications documents patterns of gendered online violence and protective strategies at https://www.apc.org/en/work/online-gender-based-violence
  Tactical Tech offers research and tools on digital footprints, exposure, and influence at https://tacticaltech.org/projects/the-influence-industry/
- PEN America maintains a field manual for responding to online abuse against journalists and activists at https://pen.org/online-harassment-field-manual/
- Citizen Lab publishes research on coordinated online attacks, surveillance, and digital threats at https://citizenlab.ca/research/

10. Session 9: Data as Power and Risk

[Presentation Attached: Session 9 - Data as Power and Risk]

10.1. Introduction

Data is one of the most powerful assets held by civil society organisations, and at the same time one of the greatest sources of risk. CSOs collect, process, and store information that enables advocacy, documentation, service delivery, and accountability. That same information, if exposed, seized, or misused, can cause serious harm to organisations, staff, partners, and communities. This session examines data not as an abstract technical concept, but as a form of power that creates responsibility and risk. It explores the kinds of sensitive data CSOs hold, how data vulnerability emerges in practice, and why reliance on local storage remains one of the most persistent weaknesses.

10.2. Understanding data as power

Data gives CSOs the ability to document abuses, substantiate claims, mobilise support, influence policy, and protect communities through evidence-based work. Testimonies, reports, databases, contact lists, and internal communications all enable civil society to operate effectively in contested environments.

At the same time, data concentrates power. Whoever controls access to information controls narratives, exposure, and outcomes. When data falls into hostile hands, it can be weaponised to intimidate, discredit, surveil, or silence. Understanding data as power means recognising that data protection is inseparable from human protection.

10.3. Types of sensitive data held by civil society organisations

CSOs routinely handle multiple categories of sensitive data, often without fully recognising their risk profile. This includes personal data such as names, phone numbers, addresses, identity documents, and demographic details of staff, beneficiaries, sources, and partners. It also includes sensitive contextual data such as testimonies, witness statements, case files, medical or legal information, photographs, videos, and field notes documenting rights violations or abuse.

Operational data is equally sensitive. Internal strategies, donor communications, funding records, internal assessments, staff lists, travel plans, and organisational communications can expose networks, priorities, and vulnerabilities if accessed by adversarial actors. Even seemingly low-risk data, when combined or analysed over time, can reveal patterns that put individuals or organisations at risk.

10.4. Data vulnerability in practice

Data vulnerability does not arise only from hacking. It emerges from how data is collected, stored, accessed, shared, and retained. CSOs often accumulate data over long periods without clear retention policies, creating large repositories of sensitive information that are rarely reviewed or minimised. Access controls are frequently informal, with multiple staff members able to view or edit files without clear justification.

Sharing practices also create vulnerability. Files may be exchanged through unsecured channels, forwarded without consent, or stored on personal devices. Each transfer increases the risk of exposure. Over time, data vulnerability becomes embedded in routine organisational behaviour rather than exceptional incidents.

10.5. Reliance on local storage and its risks

One of the most consistent findings across civil society contexts is the heavy reliance on local storage. Sensitive files are often kept on personal laptops, external hard drives, USBs, or office computers. While local storage feels familiar and controllable, it creates serious risks. Devices can be lost, stolen, confiscated, or damaged. Files may not be encrypted. Backups are often irregular or non-existent.

In environments where CSOs face raids, device seizures, or border searches, local storage poses an acute threat. Data stored locally can be accessed, copied, or destroyed, potentially exposing entire networks of contacts or years of documentation. The risk is compounded when devices are shared, outdated, or used for both personal and organisational work.

10.6. Survey findings and patterns of exposure

Across multiple studies and digital safety assessments conducted globally, including those referenced in your presentation, CSOs consistently report limited confidence in their data protection practices. Surveys show high levels of reliance on local storage, low adoption of encryption, unclear data ownership, and limited understanding of who has access to what data.

These findings point to a structural issue rather than individual negligence. Many CSOs lack the resources, guidance, or organisational frameworks needed to manage data safely. As a result, data risk becomes normalised, even when organisations work on highly sensitive issues.

10.7. Data access and internal risk

Not all data risk comes from external actors. Internal access practices can create significant exposure. When access is not role-based or reviewed regularly, staff may retain access long after it is necessary. Departing staff may still have copies of files or access to shared folders.

This internal exposure does not imply bad intent. It reflects informal organisational cultures where data governance has not kept pace with digital dependence. Addressing this requires clear norms around access, responsibility, and accountability.

10.8. The cumulative nature of data harm

Data-related harm often unfolds gradually. A single document leak may seem manageable, but repeated exposure, partial access, or long-term surveillance can create comprehensive risk. Adversaries may collect fragments of information over time, assembling profiles of organisations, staff, or communities.

This cumulative nature makes data protection especially important. Preventing small leaks and reducing data footprints limits what can be exploited later.

Balancing data utility and protection

CSOs cannot stop collecting data. Their work depends on it. The challenge is to balance usefulness with protection. This involves asking deliberate questions about what data is truly necessary, how long it needs to be kept, and who needs access. Data minimisation reduces risk without undermining impact.

Key takeaway: Treating data as both an asset and a liability encourages more thoughtful practices and reduces unnecessary exposure.

10.9. Organisational responsibility and readiness

Protecting data is an organisational responsibility, not an individual one. It requires leadership recognition that data risk can disrupt operations, endanger people, and undermine trust. Clear policies, shared understanding, and basic safeguards reduce dependence on individual judgement and create collective resilience.

Data readiness also includes preparing for incidents. Organisations should be able to respond to device loss, seizure, or breach without panic, knowing what data is at risk and what steps to take.

10.10. External Resources:

- Access Now's Digital Security Helpline provides guidance on protecting sensitive data and responding to incidents at https://www.accessnow.org/help/
- The Electronic Frontier Foundation offers practical resources on data protection and encryption at https://ssd.eff.org
- Tactical Tech provides research and tools on data exploitation and civil society risk at https://tacticaltech.org
- Citizen Lab publishes investigations into data seizure, surveillance, and digital targeting of civil society at https://citizenlab.ca/research/

11. Session 10: Principles of Data Protection

[Presentation Attached: Session 10 - Principles of Data Protection]

11.1. Introduction

Data protection within civil society work is not merely a technical discipline but a framework for reducing harm, preserving trust, and safeguarding the people whose information CSOs hold. Principles like data minimisation, access control, and encryption exist to ensure that sensitive information—particularly data belonging to vulnerable communities—is handled in a way that prevents misuse, limits exposure, and preserves organisational continuity. This session builds a grounded understanding of these principles and explains how CSOs can apply risk-appropriate protections in practice.

11.2. Data minimisation: collecting only what is necessary

Data minimisation is one of the most effective ways to reduce organisational risk. Every unit of data collected becomes a potential point of vulnerability. Civil society organisations often gather far more information than is required—full names, IDs, phone numbers, photographs, internal notes, and

contextual details that may not be essential to the work. This accumulation increases exposure without necessarily increasing usefulness.

Data minimisation means asking deliberate questions before collecting or storing information: is this data essential to the purpose, and is there a safer alternative? It also means reviewing old data to assess whether it should still be retained. Reducing the volume of data reduces the surface area of risk, ensures better control, and prevents long-term accumulation of unnecessary sensitive information. Minimisation is especially critical for organisations working with communities at risk of surveillance, discrimination, or harassment.

11.3. Access control: limiting who can see what

Access control ensures that only individuals with a legitimate need have access to specific information. In many CSOs, access grows organically: staff accumulate permissions over time, shared folders expand without review, and volunteers or interns sometimes retain access long after projects end. These patterns create internal exposure that adversaries can exploit through compromised devices, phishing, shared accounts, or unauthorised downloads.

Effective access control is role-based. Access is granted intentionally, reviewed regularly, and revoked as soon as a role changes. Sensitive information should be accessible only to those directly working with it. Separating access reduces the impact of breaches and prevents a single compromised device or account from exposing the entire organisation. Access control is a structural safety mechanism that protects both data and people.

11.4. Encryption: protecting data in transit and at rest

Encryption protects data by making it unreadable without the correct key. It is essential for civil society work because it limits exposure even when networks are unsafe, devices are compromised, or files are intercepted. Encryption in transit protects data moving between devices, while encryption at rest protects stored data on laptops, phones, drives, or cloud systems. Both forms are necessary.

Encryption becomes particularly important when staff travel, operate remotely, or work in restrictive environments where device seizure is a real possibility. Without encryption, a single confiscated device can expose contacts, testimonies, internal communication, and years of organisational work. Encryption is not about secrecy but about ensuring that information cannot be weaponised against vulnerable people.

11.5. Understanding risk-appropriate protections

Risk-appropriate protections recognise that not all data carries the same level of sensitivity and not all organisations face the same threat environment. Protecting an event sign-up sheet requires a different approach than protecting testimonies from conflict zones or case files from rights-based litigation. Risk-appropriate protection begins by assessing the threat landscape: the political context, the organisation's visibility, the issues it works on, the likelihood of surveillance or harassment, and the sensitivity of the data held. From there, protections are matched to risk—stronger for high-risk data, lighter for routine operational information. This approach prevents over-securing low-risk data while

ensuring that high-risk information is handled with the necessary safeguards. It also helps CSOs prioritise resources, especially when capacity is limited.

11.6. The link between data protection and trust

Civil society organisations rely on trust: trust from communities, partners, donors, and the public. When data is mishandled or exposed, trust is damaged, sometimes irreversibly. Protecting data is therefore not only a legal or operational requirement; it is an ethical obligation. Communities share information with CSOs because they expect responsible stewardship. A strong culture of data protection strengthens credibility and reinforces accountability.

11.7. Data protection as an organisational practice

Effective data protection is not achieved through tools alone. It depends on organisational policies, shared norms, and consistent behaviour. This includes establishing clear data lifecycle practices, training staff on secure handling, avoiding informal sharing channels, ensuring safe disposal, and embedding safety into routine workflows. When data protection becomes part of everyday operations, organisations reduce exposure and increase resilience. Policies and tools support the work, but the behaviour of staff, how they store, share, and handle data, determines whether protections succeed.

11.8. External Resources:

- Access Now provides guidance on data protection practices and civil society risk mitigation at https://www.accessnow.org/help/
- Electronic Frontier Foundation offers practical instruction on encryption and safe data handling at https://ssd.eff.org
- Tactical Tech produces resources on responsible data stewardship and minimising data exposure at https://tacticaltech.org
- Citizen Lab publishes research on threats to civil society, including data seizure and targeted digital attacks, at https://citizenlab.ca/research/

12. Session 11: Secure Storage, Backup, and Recovery

[Attached Presentation: Session 11 - Secure Storage, Backup, and Recovery]

12.1. Why secure storage and recovery matter for civil society

For civil society organisations, data loss or exposure is not a technical inconvenience but an operational and human risk. Files stored by CSOs often contain personal details, testimonies, internal assessments, and sensitive communications that, if accessed by hostile actors, can endanger individuals and disrupt entire programmes. Secure storage and reliable recovery planning are therefore not optional safeguards; they are core elements of organisational resilience. This session focuses on how storage choices, encryption practices, and backup planning directly shape an organisation's ability to withstand disruption, including scenarios involving device loss, theft, or seizure.

12.2. Understanding cloud storage in practice

Cloud storage offers significant advantages for civil society organisations, particularly in terms of redundancy, accessibility, and continuity. Files stored in the cloud are protected against physical loss of devices and can usually be restored even if hardware is damaged or destroyed. Cloud systems also allow teams to collaborate across locations and provide version histories that reduce the risk of accidental deletion.

At the same time, cloud storage introduces specific risks. Security depends almost entirely on account protection. Weak passwords, shared logins, or the absence of two-factor authentication can allow attackers to access large volumes of data remotely. Cloud services also operate within legal jurisdictions that may compel data access under certain conditions. For CSOs working on sensitive issues, it is essential to understand where data is hosted, who controls access, and how account security is enforced. Cloud storage is most effective when combined with strong authentication, clearly defined access roles, and careful control over sharing permissions.

12.3. Local storage and its vulnerabilities

Local storage remains widely used by CSOs because it feels tangible and under direct control. Files stored on laptops, desktops, USB drives, and external hard disks are often easy to access and manage. However, local storage is highly vulnerable to loss, theft, damage, malware, and seizure. In environments where civil society actors face travel checks, raids, or harassment, local devices are often the first targets.

Without full-disk encryption, data stored locally can be accessed immediately by anyone who obtains the device. Even when devices are password-protected, many systems allow data extraction if encryption is not enabled. Local storage also tends to accumulate sensitive data over time, especially when devices are used for both personal and organisational work. Understanding these vulnerabilities is critical for deciding what data, if any, should be stored locally and under what protections.

12.4. Comparing cloud and local storage through a risk lens

Choosing between cloud and local storage is not about identifying a universally safer option. It is about matching storage methods to the organisation's threat environment and the sensitivity of the data. Cloud storage reduces physical risks but increases dependence on account security and external providers. Local storage offers offline control but exposes organisations to physical compromise and loss.

Risk-aware organisations often use a hybrid approach, storing the most sensitive data in encrypted local or offline environments while using cloud storage for collaboration and less sensitive materials. The key principle is intentionality. Storage decisions should be deliberate, documented, and reviewed rather than driven by habit or convenience.

12.5. Low-cost encrypted solutions

Encryption is one of the most effective safeguards available to civil society organisations, particularly those with limited resources. Low-cost encrypted external drives, encrypted folders on laptops, and secure mobile storage applications can dramatically reduce exposure if devices are lost or seized.

Encryption ensures that data remains unreadable without the correct credentials, even when hardware is compromised.

For CSOs handling testimonies, case files, or sensitive contact lists, encryption should be considered a baseline requirement. It protects data at rest and limits the damage caused by physical access to devices. When combined with strong passwords and safe key management, even simple encrypted solutions provide meaningful protection against both opportunistic and targeted threats.

12.6. Backup planning as organisational insurance

Backups are the safety net that allows organisations to recover from incidents without losing critical information. Effective backup planning begins with identifying which data is essential to operations and ensuring it is copied regularly to secure locations. Backups should be protected with the same care as primary data, including encryption and access controls.

Reliance on a single backup location creates new vulnerabilities. A resilient backup strategy includes redundancy across different storage environments so that no single failure can erase important data. Regular testing of backups is equally important, as untested backups often fail when they are needed most.

12.7. Preparing for device loss and seizure scenarios

Device loss and seizure are realistic risks for many civil society organisations, particularly those operating in restrictive or politically sensitive contexts. When a device is confiscated, all data stored on it becomes potentially accessible unless strong protections are in place. This can include emails, documents, photos, messaging histories, and location data.

Preparing for these scenarios requires designing workflows that assume devices may be taken. Sensitive data should be minimised on physical devices, encrypted wherever possible, and backed up securely elsewhere. Organisations should be able to revoke access, secure accounts, and continue work without relying on compromised hardware. Planning for loss or seizure transforms a potentially catastrophic event into a manageable disruption.

12.8. Recovery and continuity after disruption

Recovery is the final and most often overlooked element of secure storage planning. It involves restoring data, securing accounts, replacing devices, and resuming operations without compounding risk. A clear recovery plan ensures that staff know what steps to take after an incident, who is responsible for which actions, and how to prioritise safety during restoration. Recovery planning reinforces organisational confidence and continuity. It allows CSOs to respond calmly and effectively to disruption, protecting both their mission and the people they work with.

12.9. External Resources:

- Access Now provides guidance on secure storage, encrypted solutions, and incident response at https://www.accessnow.org/help/

- Electronic Frontier Foundation offers practical resources on encryption, backups, and device security at https://ssd.eff.org
- Tactical Tech publishes research and tools on responsible data handling and storage practices at https://tacticaltech.org
- Citizen Lab conducts research on device seizure, surveillance, and digital threats facing civil society at https://citizenlab.ca/research/