Solidarity Playbook

Facing cybersecurity challenges: Lessons learned and opportunity areas

International Civil Society Centre

CyberPeace Institute

solidarityaction.network

1. Introduction

Digital infrastructure is core to the work of every civil society organisation – from staff email and internal communication platforms to storing and sharing documents, to the data collected on vulnerable populations and throughout a project's lifecycle, to name a few examples. However, with increased digitalisation comes the risk of digital threats such as cyberattacks.

In recognition of the growing challenge of digital threats and cyberattacks facing (international) civil society organisations ([I])CSOs), the International Civil Society Centre has partnered with the CyberPeace Institute to expand the Solidarity Playbook – a collection of case studies and best practices curated by the Solidarity Action Network (SANE). This expanded resource features four case studies on cybersecurity that share examples of how (I)CSOs have dealt with actual cyberattacks.

The aim of this case study collection is to make the (I)CSOs' experiences, strategies, and lessons learned available for other civil society actors who have faced or might face similar attacks and challenges in the future. The cases provide first-hand accounts of how (I)CSOs (case study partners) responded to cyberattacks and insights into how organisations can prevent and mitigate similar incidents.

Cyberattacks can take many forms. This collection of four case studies represents a snapshot of several different cybersecurity incidents: a phishing attack that hijacked an organisation's social media account; a spear phishing attack that targeted employees' email accounts over six weeks; a brute-force attack that featured a high volume of attempted logins; and a ransomware attack in which attackers exploited a server vulnerability to hold an organisation's data hostage.

The case studies provide relevant information for anyone working at an (I)CSO, regardless of their department as **cybersecurity needs to be a shared responsibility** – it requires attention across the whole organisation and cannot be borne only on the shoulders of IT staff. This overview captures key observations, challenges, and lessons learned across all four case studies and concludes with opportunity areas (I)CSOs can explore to better prepare for a cyberattack.

2. Key observations

While each case study was unique, some similarities have emerged:

1. Any organisation can face a cyberattack

No organisation is immune to cyberattacks, no matter how strong their cybersecurity is, and even purpose-driven not-for-profit organisations can become a target of cyberattackers. Moreover, any staff member within an organisation can be targeted and new staff members are particularly likely to be perceived as an easy target. Therefore, we need to normalise conversations about cybersecurity risks and incidents in the civil society sector and establish avenues for exchange of know-how and resources to strengthen organisations' ability to prevent and respond to cyberattacks.

2. Attacks are increasingly sophisticated

The case study partners noted that the cyberattacks they faced were more sophisticated than they had expected. For instance, phishing emails were well written, using sophisticated language or a writing style similar to that of someone within the organisation; or phishing links led to a webpage with the branding or appearance a user might expect. Oftentimes, a single character was omitted or changed in an email address or weblink, which made the discrepancy easy to miss.

3. Attacks are intense – and require attention even after they end

In the case studies, the length of time of an attack ranged from a few hours to six weeks. Sometimes, a response would prompt a change of direction – for instance, a team would block IP addresses only for attackers to create new ones. Those responding to the incidents described these attacks as like "firefighting" or "a game of cat and mouse," reflecting the sustained intensity of the attack and required response. Even after an attack ended, teams would spend several weeks working on forensic analysis to better understand the cyberattack and how their organisation's data and systems may have been compromised.

4. Attacks lead to increased staff awareness

The cyberattacks created greater awareness among staff and reinforced the notion that cybersecurity starts with each individual. The attacks underscored the importance of the measures staff members had been advised to take and made them more aware of the actions they should take – even after the incident. Additionally, the senior management gained a new understanding of the importance of cybersecurity. After experiencing an attack, they found that cybersecurity went from being an abstract notion to a concrete one.

3. What are the shared challenges?

Five shared challenges were faced by the case study partners, and solutions were implemented to tackle some of these challenges:

CHALLENGES

Resource constraints

Given the purpose-driven nature of their work, (I)CSOs tend to focus resources on programmatic impact rather than operational aspects like IT and cybersecurity. Therefore, IT teams at (I)CSOs are often relatively small for the size of the organisation. As many cybersecurity tools are designed for enterprises, they can be expensive and beyond the reach of many (I)CSOs (though there are affordable options, as the case studies demonstrate). Following the attacks, organisations allocated larger budget resources toward IT and cybersecurity or hired additional staff in recognition that greater protection against digital risks was needed to safely carry out their programmatic work.

First-time experience

The cyberattacks faced by the organisations in the case studies were a new experience that they had not had before. They might have had some experience in handling other incidents, but staff (both IT and management) had not faced cyberattacks of this intensity before. This lack of prior experience led to uncertainty as to how to respond, which organisations successfully navigated by seeking help, whether from external cybersecurity experts or the organisation's wider network. Having existing crisis response mechanisms for responding to non-digital incidents was helpful in coordinating and responding to a cyberattack.

Unknowns are unsettling

The case study partners reported having more questions than answers during and in the aftermath of the cyberattack. For instance: Why were they attacked? Why did the attack stop? What were the attackers' intentions? And did the organisation uncover the full extent of the attack? It can be difficult to get answers to these questions even with a post-mortem analysis, and this uncertainty remains a challenge.

Balancing incident response and day-to-day tasks

In most cases, two or three staff members were the organisation's frontline responders to the cyberattack. At the same time, these staff members also had to carry out their normal duties, particularly if the incident took place over a long period of time. It was exhausting for the IT staff to keep up with day-to-day demands while responding to the attack.

Deciding what to communicate

When, how, and to whom organisations communicate about a cyberattack can vary depending on the type of cyberattack, its severity, and the organisation's decisions. For instance, an organisation may decide to communicate externally about an incident if the attack affects a public-facing channel and they wish to prevent their audience from possible scam attempts. Internally, it can be challenging for IT teams to communicate with colleagues regularly about a situation when they are "firefighting" and in the midst of responding to an attack. However, internal communication – such as to senior management and staff – can be vital in creating a strong response by facilitating coordination, ensuring colleagues stay alert, managing possible work disruptions, and enabling a quick recovery. Deciding exactly what information to communicate was perhaps the biggest challenge facing the case study partners. Those responding to cybersecurity incidents sought to strike a balance between providing sufficient information to keep people (whether staff or members of the public) safe and informed and not oversharing (which might increase the organisation's vulnerability).

4. What are the main lessons learned?

Reflecting on their responses, what they would do differently next time, and changes they have made since facing a cyberattack, the case study partners shared four key lessons learned:

LESSONS LEARNED

Plan for incident response

Different organisations went about this in different ways, but all took steps to ensure a better response next time. Their strategies included: developing a disaster recovery plan or adding cybersecurity risks to an existing plan; improving the threat model by exploring cybersecurity threats in greater detail; and leveraging existing crisis mechanisms for cybersecurity incidents. If working with external providers (such as outsourcing data storage), know how they would respond to a cyberattack. Additionally, learn about your legal obligations, such as whether and how a breach must be reported to data protection authorities.

Make use of available cybersecurity measures

In the aftermath of the cybersecurity incidents, the organisations reviewed their security measures and took steps to increase cybersecurity. A common measure was to implement multi-factor authentication (MFA), which requires staff to prove their identity in two or more ways to access their accounts. Another common step was to perform regular system maintenance and check for available updates. While no cybersecurity measure is bulletproof, taking these steps may help to prevent or delay an attack.

Avoid blaming others and stay calm

A cyberattack is a vulnerable time for any organisation, and staff on the frontline of incident response can feel frustrated, angry, deceived, or worried. Staff members who succumb to phishing emails may blame themselves for falling for the trick (although phishing emails are increasingly sophisticated and convincing). Remember that a cybersecurity incident is no-one's fault. All staff should know that any organisation – and anyone within an organisation – can face a cyberattack. Further, those responding to incidents often feel pressure during the stressful period of responding to a cyberattack. This pressure may be compounded by worrying about their colleagues' reaction to learning about the cybersecurity incident. For staff responding to a cybersecurity incident, remember that staying calm will help you to respond better and that colleagues will likely be more appreciative and understanding than you might expect.

Identify and seek support

External help played a significant role for the case study partners in managing and/or resolving incidents. This help can come in different forms, such as hiring external cybersecurity consultants who have expertise in responding to similar incidents, managing negotiations with cyberattackers, or conducting forensic analysis in the aftermath. Organisations that had existing relationships or connections to cybersecurity experts (such as having worked with them before or knowing them from an assessment conducted for cyber insurance) were able to quickly engage their support and respond. IT staff also noted the importance of identifying internal helpers – such as colleagues in communications or legal functions – who may be able to support certain aspects of the response. Meanwhile, organisations which focus on providing cybersecurity support to (I)CSOs, such as the CyberPeace Institute, can provide staff trainings and further assistance.

5. Opportunity areas

The collected case studies highlight the sense of vulnerability felt by staff when their organisation experienced a cybersecurity incident and the challenges of anticipating an attack. After facing a cyberattack, all organisations took action to improve their cybersecurity. Our overall advice for (I)CSOs is to **take action now** rather than waiting for an attack to happen first, to empower your organisation to prevent and respond to cybersecurity incidents.

What might (I)CSOs do right now to better prepare for and respond to future cyberattacks?

Recognising possible limitations faced by (I)CSOs (including organisational structures, processes, infrastructures, teams, or budget constraints), the following action steps may offer opportunities for improved preparedness:

1. Assess your cybersecurity readiness

a. Audit current resources to determine what could be useful in the face of an attack. For instance, assess staff capacities and knowledge as well as measures currently in place to protect IT systems.

b. Remember to take into account existing processes and procedures that you may use for other types of crises, which could potentially be applied to cybersecurity incidents. Consider existing risk management, crisis mitigation, or disaster response plans. You may find that your organisation has several tools and resources already in place which can be adapted or updated to help prepare for cybersecurity threats.

2. Share the responsibility of cybersecurity

a. Everyone in the organisation needs to be aware of cybersecurity. Consider how you might encourage staff to think proactively about cybersecurity. This mindset could be encouraged through gamifying exercises and trainings, such as periodically sending out fake phishing emails and sharing the click-through score with all staff across the organisation. Embed cybersecurity in organisational processes such as IT onboarding and data protection, as well as communication trainings and resources.

b. Increase management's awareness of cybersecurity challenges, potential tools, and ways to help protect your organisation. Raising awareness of the severity of cyber threats and the importance of preventative measures may ensure that cybersecurity is given adequate attention and resources as a potential risk.

c. Advocate with donors for more resources to improve your organisation's cybersecurity.

3. Identify cybersecurity support and invest in relationships

a. Establish peer networks and engage with similar organisations to share resources, seek advice, and support each other on cybersecurity issues. A cyberattack may target multiple organisations, so information sharing can improve each organisation's capacity for prevention and response.

b. Identify organisations that provide support and develop tailored resources on cybersecurity for (I)CSOs. They can provide advice and connect your organisation to technical support and peer support, such as events on cybersecurity topics where you can meet and learn from people in other organisations facing similar challenges.

c. Identify specialist cybersecurity firms that could support you in the event of an attack. Explore potential relationships and arrangements with them – for example, they may offer pro bono or reduced-price services to (I)CSOs or be included as part of cyber insurance.

d. Explore cyber insurance options that can help to protect your organisation in case of cyberattacks.

6. Conclusion

Every (I)CSO should prepare for, and expect to face, a cybersecurity incident. When a cyberattack happens, how an organisation approaches the response and its aftermath is critical. While it is undoubtedly difficult and challenging to withstand a cybersecurity incident in the moment, a cyberattack can also provide a valuable trigger to instigate genuine behavioural change within the organisation. Rather than implementing changes as a reactive response, organisations can use the post-incident phase to carefully consider how actions taken will fit into their larger strategy and operations. This intentional approach should then convert into meaningful actions. For instance, organisations should not only include cybersecurity considerations in risk management plans but ensure that the organisation is able to use and implement the devised mitigation strategies when needed. The organisation should also strike a balance between moving on from a cybersecurity incident and keeping the institutional memory of the incident alive. Finally, (I)CSOs should find a way to continually evolve and improve their cybersecurity as threats evolve and change over time.

Discover Solidarity Playbook case studies on cybersecurity
solidarityaction.network/cybersecurity

Solidarity Playbook

Facing cybersecurity challenges: Lessons learned and opportunity areas

Sacha Robehmed and Nonso Jideofor

March 2023

International Civil Society Centre

CyberPeace Institute

In partnership with