15 years

KCSS
Kosovar Centre for Security Studies

EMERGING
THREATS
PROGRAMME

CYBERSECURITY HANDBOOK FOR CIVIL SOCIETY ORGANIZATIONS

November 2023

Supported by: USAID

EMERGING
THREATS
PROGRAMME

Author: Donika Elshani, Jon Limaj, Vesa Kroci

About the Emerging Threats Programme

The Emerging Threats Programme has been designed as a response to evolving domestic, regional, and international security threats. Its primary aim is to consolidate and provide a better understanding of emerging threats that consistently move away from traditional conceptualizations of security challenges. Given the extent of evolving threats related to cybersecurity and disinformation, this programme seeks to build upon internal organizational capacities to provide evidence-based expertise to operationalize institutional responses to these challenges. Evidence-based research in relation to the Emerging Threats Programme focuses on: critical infrastructure, cybersecurity, disinformation and hybrid security challenges. While needs assessment(s), monitoring and research remain fundamental actions to be developed in the programme, KCSS aims to utilize expertise generated to directly enhance the capacities of executive institutions and agencies to respond effectively to cybersecurity challenges and disinformation. The programme will be developed through:

- State of the art evidence-based research related to emerging threats such as cybersecurity, critical infrastructure protection, hybrid threats and disinformation;
- Awareness-raising campaigns and targeted advocacy to improve the level of understanding of challenges related to cybersecurity, critical infrastructure protection, hybrid threats and disinformation in Kosovo;
- Awareness-raising campaigns and targeted advocacy to improve the level of understanding of challenges related to cybersecurity.

For more information, contact us at: EmergingThreats@qkss.org

The following report is published in the framework of the "Greater Internet Freedom" project, implemented by Internews and BIRN Hub, with the support of the United States Agency for International Development (USAID).

Supported By:

USAID

Table of contents

Introduction

The rapid development of technology worldwide has made the digital sphere an increasingly integral element of contemporary societies. These technological advancements have significantly changed the way people live, work, communicate and perform services via the global online network. Civil society organizations are no exception to this aspect. They are increasingly relying on various digital tools to carry out their daily operations in a more efficient and sustainable manner. Upon the development of various social and digital platforms and applications, civil society organizations have the opportunity to communicate quickly and efficiently with their citizens, donors and supporters locally and globally. The development of these technologies has introduced new opportunities for NGOs in the field of activism and political influence, enabling them to organize awareness campaigns and promote their causes to a wide audience of followers.

As the digital footprint of NGOs continues to grow, so does the risk to their privacy and security in the digital sphere. Cyber-attacks against this sector are on rise involving a range of tactics, including hacking official websites and communication systems of organizations, stealing sensitive data, misappropriating funds and spreading disinformation and fake news, among others. The consequences of such attacks are considerable and pose a serious risk to the regular functioning of NGOs. Some of the consequences that can be faced by the latter are damage to the reputation and image of the organization, which affects the loss of support and trust of donors, partners and groups with which the organization works; large financial losses; loss of information and other key resources of the organization, disruption of services and regular operations provided by the organization, and in extreme cases, permanent closure of the organization.

Adverse to these risks, it is crucial that NGOs take concrete measures to improve their cyber security and minimize the risk they face. By good fortune, NGOs do not need to have advanced knowledge in the field of information technology to protect themselves from threats in the digital sphere. It is enough for them to allocate a part of time, financial and human resources to cultivate a safety culture within the organization.

This manual was compiled with aim to serve NGOs in Kosovo, but not only, as a guide to develop and implement organizational security policies and strategies. The handbook presents good practices and concrete guidance as to how the organization, regardless of its scope, can minimize the risk it faces in the digital sphere. Some of the topics covered in this manual are the security plan and development of security culture in an organization, protecting electronic devices within the organization and securing access to them, protecting records, cyber security, physical security and what to do in case of incidents.

Security plan

The security plan is a strategic document that defines the objectives, policies, procedures and measures that an organization must follow to protect and secure its data, resources and infrastructure from external risks. The security plan can include various aspects of security in the organization, whether it is physical security, cyber security, operational security, as well as staff awareness of security risks and practices through training and awareness campaigns. The main purpose of the security plan is to provide that the organization has a structured and coordinated approach to minimize risks and to ensure that its activities are carried out in a safe and secure manner.

Each organization's security plan should be based on a detaile **risk assessmen** process. . The first step for the development of the security plan is the **identification of the main threat** that the organization may encounter and which would affect the security of the organization. In order to have a clearer picture of the risks that threaten the organization, it is important to **identify the actors**, whether they are individuals, groups or other entities, who may have motives and interest in targeting the organization through various attacks. These individuals or groups may be hackers, criminals, competitors of the organization, authorities of government agencies or insiders with access to key systems of the organization. Another important step is to **identify the assetse** that the organization possesses. These assets encompass important data, information systems, electronic equipment, physical infrastructure and any other resources that are important to the operation of the organization.

Each organization has its own security plan that is tailored to its specific needs and requirements. However, there are some universal rules and practices that can be taken as a basis when developing the organizational security plan, which are summarized below.

Protecting electronic devices, providing access to them and protecting records

Organizations rely on a broad set of electronic devices and digital tools to conduct their operations on a daily basis. Starting with computers, laptops, and smartphones up to servers, routers, and network devices, these devices serve NGOs to communicate, process data, develop projects, manage their resources, and perform many other activities related to their activity. The protection of electronic devices is extremely important because the latter contain all the vital information and data of the organization. Unauthorized access to these devices may result in compromising the integrity and confidentiality of this data.

Herein below are some simple steps that any organization can follow to protect and secure its electronic infrastructure

Password security

The organization and constituent staff have a large number of online accounts through which they carry out their activities related to the organization. For instance, this includes email accounts, accounts for social networks, accounts for e-banking services, accounts for using various applications, etc. An easy and efficient way to protect these accounts is to set a strong password that comprise these characteristics:

Length

A strong password must have at least 8 characters. In principle, the longer the password, the harder it is to find or crack it.

Complexity

n order to have a strong password, it must contain different combinations of letters, numbers and symbols, including the use of upper- and lower-case letters. The more complex the password, the more difficult it is to find or crack it

Parashikueshmëria

Predictable passwords are basically weak passwords. Employing the name, date of birth, phone number or other predictable data increases the risk of finding or cracking the password. Furthermore, setting passwords that consist of a predictable series of numeric digits, such as '12345678' or '11111111' should also be avoided.

Two-factor/multi-factor authenticatio

In addition to setting strong passwords, an additional method to protect accounts is to use two- or multi-factor authentication. This method requires that besides the password, the user provides additional information to verify his or her identity. This additional information can be a code that the user receives through the token, authentication applications or SMS message. Authentication prevents attackers penetrating different accounts, even if they have found or cracked the passwords of those accounts.

Some of methods that can be used for authentication are **tokens** or **security keys, codes received through phone messages and authentication applications.**

Tokens or security keys are physical devices used to secure accounts. These devices generate a simultaneous code or unique series of numbers which, once entered into the authentication platform, gives the user access to the account. The use of tokens is among the most secure methods of authentication and is the most recommended method by experts for protecting accounts.

Authentication applications are software that are installed on the user's electronic devices and serve as a secure way to generate and verify the authentication code for logging into various online accounts. Similar to tokens, this application generates a unique code that gives the user access to the account. This method is more convenient because it is integrated into electronic devices, such as smart phones or tablets.

Another way to secure accounts is through authentication via SMS code. Each time the user wants to log into an account, he or she receives a unique code via phone message, which, once entered on the authentication page, gives the user access to the account. This is among the most popular authentication methods, but at the same time it is also the least secure. This is because electronic devices, such as phones, can be tapped or hacked.

Securing the organization's equipment

In addition to securing accounts, it is also important to secure all the devices that the employees are charged with, such as computers, laptops, personal phones, USB drives, etc. The latter plays a very important role in the physical and cyber security of the organization, since they are the main doorway through which the organization's data and systems can be exposed. Therefore, the equipment must also be secured physically, either against theft or loss. Listed below are some general best practices for protecting the above-mentioned devices:

Acquisition of secured assets

As a first step, it is important that the equipment purchased by the organization is manufactured by reliable companies that operate in conformity with the global standards of the production of the equipment in question.

Data encryption

Encryption is one of the most effective security methods for protecting organization's devices. Encryption is the way of translating various data into a ciphertext form, whereas only those who have the encrypted 'key' are able to decrypt the data to its original form.

Create strong passwords

Securing the organization's devices with strong passwords is just as important as securing the online accounts through which the organization conducts its day-to-day activities. The recommendations listed above regarding securing passwords are as well applicable on the securing access to organizational devices, such as laptops, computers, phones, printers, etc.

Physical protection of equipment

Devices should also be physically protected, situating them in secure places within offices and monitoring them constantly. The latter can be implemented by deploying security cameras on the premises where the equipment in question is located. Another recommended practice is to maintain a logbook of the devices that the organization is in ownership and every log in/ log out of the device in question.

Protection of equipment from remote intrusion

One of the main risks to an organization's devices - apart from their loss, damage or theft - is remote intrusion, otherwise known as 'hacking' them. This enables unauthorized persons or entities outside the organization to gain access to the organization's equipment, data and systems, without having any physical contact with them.

"Malware" is the umbrella term that encompasses many subcategories of remote attacks. The latter can 'infect' the organization's devices and accounts through various channels, including through e-mail, various websites, USBs, etc. Such attacks constitute one of the greatest risks that can threaten an organization, because they can lead to the theft of important data, financial damage, to the vulnerability of the security of the organization's staff.

Herein below are listed some general good practices to protect against malware attacks:

Regular updates of all operational systems

Used by the organization, such as Windows, Mac, Linux and Android, is one of the easiest and most efficient methods to avoid the above-mentioned attacks. It is important to update operational systems on a regular basis, since malware attacks are constantly changing, each time bringing with them new and unknown risks. This applies not only to laptops and computers used by the organization's staff, but also to cell phones, which must also be updated

Installing anti-malware software

Is another way to get protection from remote attacks. There are similar programs which are free and reliable which can be easily utilized by the organization.

Staff awareness about security while surfing the Internet

Is another practice with which remote attacks can be prevented. The employees in the company should pay attention to what sites they browse on the Internet, not clicking on suspicious websites and not downloading or opening documents from untrusted sources.

Another very common risk when it comes to remote attacks are so-called ‘**phishing**-attacks’. With the latter, malicious persons, groups or other entities can take control over NGO accounts and equipment, steal sensitive information and cause significant damage. This attacking technique usually involves **sending fraudulent emails or creating scam websites** that look like the organization’s official website. By accepting messages or web pages that at first glance seem reliable, employees risk sharing confidential information, such as passwords, banking or personal data, etc., with malicious actors.

In order avoid phishing attacks, the organization and its employees can follow some simple and effective steps, as follows below:

Verifying the source’s messages/ websites

Any message received on the organization›s accounts and devices should be read carefully and with increased attention. Sites with suspicious or unsolicited backgrounds should be avoided at all times. Actually, messages from unknown persons seeking information about the organization should be subject of reporting as well. It is recommended that employees check the email addresses through which they receive messages, and it is recommended to avoid downloading suspicious documents sent via email.

Employee awareness about ‘phishing’ attack

The best way to avoid phishing attacks is knowing how to identify these attacks and how to respond in case of an attack. Employee training in the organization about the techniques and the first signs of phishing attacks is essential to protect the organization from attempted attacks in the future.

Data security: Storage, sharing and communication

The maintenance of cyber security in an NGO largely depends on vital components such as communication and data storage or exchange. NGOs regularly handle confidential information about their beneficiaries, donors and missions, as well as other confidential data such as passwords, bank accounts and staff personal data, which may fell prey to external attacks.

Encryption is the most commonly recommended method to ensure secure communication within the organization. Encryption is the process of securely encoding data in such a way that makes it difficult for others to understand or read it without authorization. Encryption involves a mathematical algorithm or a special key to encrypt data, which can only be read by people who have the decryption key.

One of the most common types of encryptions is the so-called **'end-to-end encryption'**. This type of encryption ensures that only the person sending the message and the person intended to receive the message can read its contents. No other person, including the service provider or any third party, can access or read the message. Organizations should promote communication practices utilizing tools that have built-in encryption, such as Signal or WhatsApp. The organization should also have regulations on how long messages sent to the organization's accounts can be retained. When it comes to communication via e-mail, it is preferable to use an organization-wide system, in which case the risk of using private e-mail addresses by employees is eradicated.

Another important aspect when it comes to securing the organization's data is storage. Storing data in the **"cloud"** ose **"cloud computing", nowadays"** is the most recommended option by digital security experts. This method allows organizations to store their data on remote servers that are managed by companies specializing in data storage services, such as, for example, Google and Microsoft.

Some of the benefits of storing data in the 'cloud' storage include:

Access data from anywhere:

Storing data in the 'cloud' allows the organization's employees access to it regardless of where they are, they just need to have internet connection. This makes this method ideal, especially for organizations that have geographically distributed workforce or that need easy access to data on the go.

Increased security in case of incidents:

Most 'cloud' services offer automatic backup services, ensuring that data is safe even in the event of device loss or other untoward events.

However, it is essential that organizations take several security considerations into account when using "cloud" storage services. This includes ensuring data encryption, whether by password or two-factor authentication, choosing a reliable enterprise that provides "cloud" services, as well as drafting a clear corresponding security policy that defines how data should be handled and stored in this environment.

Safe Internet Browsing

It is important that when surfing the Internet, NGO employees ensure that their sensitive data is not exposed to security risks. This can be achieved by following some simple and effective practices as follows:

Using secure sites and connections (HTTPS/VPN)

It is recommended that whenever the organization's employees visit a website, they must use the **'https'**, protocol, which provides a secure connection that prevents third party intrusions and the disclosure of browser data. Similarly, the use of a **'VPN (Virtual Private Network)'** is also recommended to increase the level of security and conceal the identity and location of users.

'Phishing 'attacks prevention

The organization employees should avoid any unsafe web sites by which the organization's data could be compromised. Further, they must exercise special vigilance when browsing the Internet to prevent the compromise of confidential information such as bank data, passwords, or employee's personal data. NGOs should impose strong email security measures in place to maintain the integrity of their work. This involves implementing advanced spam filters and anti-malware software, training employees on a regular basis on how to identify and address email threats and ensuring the secure transmission of important data through encryption.

Updating browsers regularly

Updating web browsers such as Google Chrome, Safari and Mozilla Firefox, constitutes a good and easy way to ensure that web browsing is safe and without consequences for the organization. Regular updates ensure security improvements and make the organization's devices safer from potential attacks.

Physical security in NGOs

Although cyber security is of particular importance for the regular functioning of an NGO, physical security measures should not be ignored, including the security of the organization's equipment, inventory and employees. Physical intrusion such as theft or loss of equipment/inventory often have significant consequences for both physical security and information security. By following the steps below, NGOs can prevent the physical intrusion they are threatened with:

Control of entrances and exits to the office premises

The organization must maintain a regular record of every person visiting the office premises. This register must contain identification data of the persons in question, respectively the name and family name, the date and time of the visit as well as the reason for the visit. In this way, the organization prevents unauthorized access that could lead to physical and information security vulnerabilities.

Maintaining equipment in safe and constantly monitored spaces

Electronic apparatus and any other equipment of importance to the organization must be kept on secure and locked premises. Access to these devices should be limited to organization staff only. It is also recommended to install security cameras and alarm systems so that the devices are under constant surveillance.

Storage of documents and other physical materials

Although much of the day-to-day activities of NGOs have already moved into the virtual realm, organizations continue to produce hard copies of documents and other materials. It is important that copies of documents containing any kind of confidential information about the organization are kept in confined and secure premises. It is recommended that these are kept in locked cabinets that are accessible only to authorized persons in the organization. Further, organizations are recommended to have a paper shredder, thus ensuring that data in documents that are no longer needed by the organization do not fall into the wrong hands.

Responding to security incidents

Although the aforementioned practices help prevent security incidents within the organization, they do not eliminate the possibility of incidents occurring. It is important that when incidents occur, the organization's employees know how to respond quickly and effectively.

Every organization should have an **incident response plan** in place as an integrated part of the organization's overall security plan. Among other things, the incident response plan must have the following elements specified:

Specific steps to be followed in the event of an incident, including identification and confirmation of the incident, intervention to prevent its spread, investigation and assessment of damages, and regular communication with necessary personnel and authorities.

Assessment of damage caused, including financial damage to reputation and other damage related to the daily activities of the organization. Once the damage assessment has been done, the organization should have a regular procedure for reporting the incident to senior management, as well as for communicating with security authorities and internal personnel. Communication is a very important aspect of the rehabilitation process from the incident caused. What information is shared with the public regarding the incident, how this information is shared and by whom, determine the way this event will be perceived by actors outside the organization, therefore the people responsible for managing the incident must take these factors into account.

Any information, pictures or movements related to the incident should be preserved as evidence. In this case it is very important to prevent further damage and take immediate steps to address the problems, weaknesses and vulnerabilities that caused the incident.

Regular training and sensitization of staff regarding incident response procedures.

Another aspect of rehabilitation following a security incident that is often not given due importance is emotional support for staff affected by the incident. Security incidents, especially large or serious ones, can cause anxiety, fear, stress and other negative feelings among the staff. Creating an open environment where employees feel free to talk about their feelings and fears helps release stress and improve their emotional well-being. In certain cases, the organization is recommended to offer counseling services of a psychologist or other mental health specialists.

Katalogimi në botim – **(CIP)**

Biblioteka Kombëtare e Kosovës “Pjetër Bogdani”

519.718(047)

Elshani, Donika

Cybersecurity Handbook for Civil Society Organizations / Donika Elshani, Jon Limaj, Vesa Kroci. - Prishtinë : QKSS, 2023. - 8 f. ; 28 cm.

1. Limaj, Jon

2. Kroci, Vesa

ISBN 978-9951-842-09-9

About KCSS

Established in April 2008, the Kosovar Center for Security Studies (KCSS) is a specialized, independent, and non-governmental organization. The primary goal of KCSS is to promote the democratization of the security sector in Kosovo and to improve research and advocacy work related to security, the rule of law, and regional and international cooperation in the field of security.

KCSS aims to enhance the effectiveness of the Security Sector Reform (SSR) by supporting SSR programs through its research, events, training, advocacy, and direct policy advice.

Advancing new ideas and social science methods are also core values of the centre. Every year, KCSS publishes numerous reports, policy analysis and policy briefs on security-related issues. It also runs more than 200 public events including conferences, roundtables, and debates, lectures – in Kosovo, also in collaboration with regional and international partners.

A wide-range of activities includes research, capacity-building, awareness raising and advocacy. KCSS's work covers a wide range of topics, including but not limited to security sector reform and development, identifying and analyzing security risks related to extremism, radicalism, and organized crime, foreign policy and regional cooperation, and evaluating the rule of law in Kosovo.

This year, KCSS celebrated its 15th Anniversary. For more details about KCSS, you can check on the following official platforms:

qkss.org
securitybarometer.qkss.org

@KCSSQKSS
#KCSSQKSS

ISBN 978-9951-842-09-9