KCSS
Kosovar Centre for Security Studies

EMERGING THREATS PROGRAMME

DEVELOPING A SECURITY PLAN AND INCIDENT RESPONSE PLAN

USAID

2024

Internews
Local voices. Global change.

Author: Jon Limaj

EMERGING THREATS PROGRAMME

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, critical infrastructure protection, disinformation and hybrid threats, 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

© This handbook is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of Kosovar Centre for Security Studies and do not necessarily reflect the views of USAID or the United States Government"

DEVELOPING A SECURITY PLAN AND INCIDENT RESPONSE PLAN

2024

TABLE OF CONTENTS

INTRODUCTION

PURPOSE OF THE HANDBOOK

This handbook is created to assist non-governmental organizations (NGOs) in creating effective security and incident response plans. Recognizing that not everyone has a technical background, we've ensured that this guide is straightforward and easy to follow. Our main aim is to help you boost the safety and resilience of your organization.

Today we encounter a wide range of risks, from security threats to data breaches and natural disasters. Having a strong security plan and a well-prepared incident response strategy can make a crucial difference. This handbook simplifies the process into clear steps, providing practical advice and tools to your specific needs. Whether you are new to this type of planning or seeking to enhance your current strategies, this guide is designed to help you manage the difficulties of safeguarding your team and operations.

By implementing the suggestions and utilizing the templates provided, you will be better positioned to protect your staff, secure your resources, and maintain your essential work, even when faced with unexpected challenges.

IMPORTANCE OF SECURITY AND INCIDENT RESPONSE PLANNING FOR NGOS

NGO's often operate in challenging environments where they face a variety of risks. These can include security threats like violence or theft, accidents that could harm staff or disrupt operations, and data breaches that compromise sensitive information. Given these potential dangers, having a well-thought-out security plan and a detailed incident response plan is crucial.

A solid security plan helps identify and mitigate risks before they become serious problems. It lays out clear procedures for keeping your staff and assets safe, ensuring everyone knows what to do in case of an emergency. This proactive approach can prevent incidents from occurring in the first place, reducing the possibility of harm.

An incident response plan is equally important because it prepares your organization to react quickly and effectively if something does go wrong. Whether it's a natural disaster, a cyber-attack, or an on-site security breach, having a predefined set of actions can make all the difference in managing the situation and minimizing damage. This means the operations can continue with minimal disruption, and your team can focus on the important work they do.

These plans cover more than just handling emergencies—they're about creating a secure, resilient environment where your organization can succeed. They protect not just your physical and digital assets, but also the well-being of your staff, allowing you to fulfill your mission even under difficult circumstances.

HOW TO USE THIS HANDBOOK

It is designed to walk you through the process of creating your security and incident response plans in a clear, step-by-step methods. Each chapter builds on the one before it, providing you with definitions, practical steps, and templates to help you along the way.

CHAPTER 1:
UNDERSTANDING SECURITY RISKS

DEFINITION OF KEY TERMS

It is important to understand some key terms that will help navigate the process. A threat is anything that could potentially cause harm or loss to your organization, such as a security breach or natural disaster. Risk refers to both the possibility of this threat occurring and the potential impact it could have on your operations. Risk management is a systematic approach to identifying these threats, assessing how likely they are to happen, and preparing strategies to minimize their impact. By understanding these concepts, you'll be better equipped to develop effective plans to protect your organization.

TYPES OF RISKS NGOS FACE

Non-governmental organizations (NGOs) face a wide range of online risks that can significantly impact their operations. Cybersecurity risks include threats such as hacking, phishing attacks, and ransomware, which can lead to data breaches and the theft of sensitive information. These cyber threats might result in unauthorized access to donor information, financial records, or confidential personnel data.

Safety risks in the digital space can involve cyberbullying or online harassment of staff, which can lead to mental health issues or a hostile work environment. Administrator risks are related to financial fraud conducted online, such as phishing schemes that trick employees into revealing financial information or making unauthorized transactions.

Information risks are a major concern, including data breaches where hackers gain access to sensitive data or incidents where staff mistakenly share confidential information. Legal and compliance risks involve not following data protection regulations like GDPR or breaking laws related to digital communications. Reputational risks arise from online activities or breaches that damage the organization's reputation, resulting in negative publicity and a loss of trust.

Operational risks in the cyber sphere involve disruptions caused by technical failures, such as server outages or software malfunctions, which can hinder the achievement of objectives due to reliance on digital tools and insufficient cybersecurity measures.

CHAPTER 2:
DEVELOPING A SECURITY PLAN

A strong security plan is essential for seeking to safeguard its digital assets and maintain the integrity of its operations. Such a plan must cover several key components to be effective. There needs to be a strong organizational commitment to online safety and security, with leadership and governance explicitly prioritizing these issues. This commitment should be reflected in the organization's culture, policies, and practices, ensuring that cybersecurity is considered a top priority at all levels.

Policies and procedures are fundamental to a solid security plan. These should be clearly written, regularly updated, and reflect the best practices in cybersecurity. Policies should cover a wide range of areas, including data protection, incident response, access control, and user behavior. Procedures should detail the specific steps to be taken in various scenarios, providing a clear roadmap for maintaining security and responding to threats.

Another critical component is a thorough risk assessment and analysis. This involves conducting detailed Security Risk Assessments (SRA) to identify and prioritize potential cyber threats. The assessment should consider all aspects of the organization's operations, from the technical infrastructure to the human element. It is important to understand the organization's vulnerabilities and the potential impact of different threats. Based on this analysis, mitigation strategies should be developed to minimize these risks. Strategies should include a combination of technical measures, such as firewalls and encryption; procedural measures, such as regular audits and compliance checks; and behavioral measures, such as training and awareness programs for staff.

Clearly defined roles and responsibilities within the organization are essential for maintaining cybersecurity. Every member of the organization, from the top executives to the newest employees, should understand their role in the security plan. This includes knowing how to recognize and report potential threats, following best practices for secure behavior, and understanding the protocols for responding to security incidents. Training programs should be implemented to ensure that all staff are equipped with the knowledge and skills they need to contribute to the organization's cybersecurity efforts.

STEPS TO CREATE A SECURITY PLAN

Creating a security plan involves several important steps. Start by performing a Security Risk Assessment (SRA) to identify potential cyber threats and vulnerabilities. Assess how likely each risk is to occur and the potential impact it could have, then prioritize them based on their severity. Next, create a risk register to record the identified risks and the steps you'll take to mitigate them. Make sure to keep this register updated regularly.

Creating mitigation measures is crucial. These should involve specific actions to reduce each identified cyber risk, such as updating security protocols, offering cybersecurity training, or improving IT infrastructure. Schedule regular reviews and updates of the cybersecurity plan to ensure it remains relevant and effective as new risks emerge or the digital landscape changes.

CHAPTER 3:
INCIDENT RESPONSE PLAN

IMPORTANCE OF AN INCIDENT RESPONSE PLAN

Having an incident response plan is crucial for organizations to handle cyber incidents quickly and effectively. It helps minimize damage and ensures a speedy recovery, keeping your operations running smoothly and protecting your organization's reputation. When a cyber-incident occurs, a well-prepared response plan allows your team to act promptly and decisively, reducing the impact on your systems and data.

An incident response plan outlines specific steps and protocols to follow during various types of cyber incidents, from data breaches to ransomware attacks. It includes clear guidelines on identifying and containing the threat, eradicating the source, recovering affected systems, and communicating with stakeholders. By having these procedures in place, your organization can mitigate the immediate threat and prevent similar incidents in the future.

Having a strong incident response plan demonstrates to clients, donors, and partners that your organization is proactive in managing and mitigating cyber threats. It reassures them that you are prepared to handle potential security breaches, thereby maintaining their trust and confidence in your ability to protect sensitive information. This trust is crucial for maintaining strong relationships and ensuring continued support from stakeholders.

Regularly updating and testing the incident response plan is also essential. Conducting simulated cyber-attack exercises can help identify weaknesses in the plan and provide valuable training for your response team. This preparation ensures that when an actual incident occurs, your team can respond efficiently and effectively, minimizing downtime and financial losses.

KEY COMPONENTS OF AN INCIDENT RESPONSE PLAN

SEVERAL KEY COMPONENTS ARE CRITICAL TO THE EFFECTIVENESS OF SUCH A PLAN:

1. It should clearly outline procedures for identifying and reporting cyber incidents. This involves establishing protocols for recognizing signs of a potential breach or attack and ensuring that staff know how to quickly communicate these issues to the appropriate personnel. A well-defined reporting mechanism allows for the immediate detection and escalation of incidents, reducing the time it takes to respond.
2. The plan should define immediate actions to protect staff and secure assets following an incident. This includes isolating affected systems to prevent the spread of the attack, safeguarding sensitive data, and ensuring the safety of personnel.

3. The strategy must detail the roles and responsibilities of the incident response team. Each team member should have specific tasks and authority, ensuring a coordinated and effective response. This includes designating an incident commander to oversee the response efforts and communicate with senior management. Clear explanation of responsibilities helps avoid confusion and ensures that all aspects of the response are covered.

4. Clear communication protocols are essential for maintaining both internal and external communication during an incident. Internally, staff should be kept informed about the status of the incident and any necessary actions they need to take. Externally, it is crucial to manage communication with clients, partners, regulators, and the media to maintain transparency and manage the organization's reputation. Effective communication helps build trust and ensures that stakeholders are aware of the situation and the steps being taken to resolve it.

5. The incident response plan should incorporate a post-incident review. After an incident has been resolved, conducting a thorough review to analyze what occurred is vital. This involves identifying the root cause of the incident, assessing the effectiveness of the response, and documenting lessons learned. Implementing these lessons helps improve future responses and enhances the organization's overall cybersecurity position.

STEPS TO DEVELOP AN INCIDENT RESPONSE PLAN

* **IDENTIFY AND DEFINE INCIDENT TYPES AND SEVERITY LEVELS**
    - Categorize potential cyber incidents by type and severity
    - Establish clear criteria for each severity level
* **ESTABLISH RESPONSE PROCEDURES**
    - Develop step-by-step actions for responding to incidents
    - Create checklists and flowcharts to ensure clarity and ease of use
* **CONDUCT TRAINING AND REGULAR DRILLS**
    - Train staff on the incident response plan
    - Conduct regular drills to ensure everyone is familiar with the procedures and knows how to act quickly
* **MAINTAIN DOCUMENTATION AND REPORTING**
    - Keep detailed records of incidents and responses
    - Use these records to review incidents, analyze effectiveness, and improve the plan

* **POST-INCIDENT REVIEW AND LEARNING**
    - Perform a post-incident review to understand what happened
    - Implement lessons learned to enhance future responses

CHAPTER 4:
PRACTICAL TOOLS AND TEMPLATES

SAMPLE RISK REGISTER TEMPLATE

A risk register is a valuable tool for documenting identified risks and their corresponding mitigation measures. Here's an example of how you might structure it:

RISK	LIKELIHOOD	IMPACT	MITIGATION MEASURES	RESPONSIBLE PERSON	REVIEW DATE
Data Breach	Medium	High	Implement two-factor authentication, conduct regular security audits	IT Manager	Quarterly

SAMPLE SECURITY PLAN OUTLINE

Creating a complete security plan involves several key sections. Here's a typical outline to guide you:

1. **INTRODUCTION**
   Overview of the security plan's purpose and scope
2. **ORGANIZATIONAL COMMITMENT**
   Statement of commitment to security from leadership
3. **POLICIES AND PROCEDURES**
   Detailed security policies and procedures
4. **RISK ASSESSMENT AND ANALYSIS**
   Methods for identifying and analyzing security risks
5. **MITIGATION STRATEGIES**
   Specific strategies to mitigate identified risks
6. **ROLES AND RESPONSIBILITIES**
   Clear definition of roles and responsibilities within the organization
7. **REVIEW AND UPDATES**
   Procedures for regularly reviewing and updating the security plan

SAMPLE INCIDENT RESPONSE PLAN OUTLINE

An effective incident response plan includes several crucial components. Here's a sample outline:

1. **INTRODUCTION**

   Purpose and scope of the incident response plan.

2. **INCIDENT IDENTIFICATION AND REPORTING**

   Procedures for identifying and reporting cyber incidents.

3. **IMMEDIATE ACTIONS**

   Immediate steps to take to secure assets and protect staff after an incident.

4. **INCIDENT RESPONSE TEAM**

   Roles and responsibilities of the incident response team.

5. **COMMUNICATION PROTOCOLS**

   Internal and external communication procedures during an incident.

6. **POST-INCIDENT REVIEW**

   Steps for conducting a post-incident review to analyze what happened.

7. **DOCUMENTATION AND REPORTING**

   Maintaining detailed records of incidents and responses for future reference and improvement.

By following these templates, NGOs can create strong cybersecurity strategies created to their specific needs, ensuring they are prepared to handle potential cyber threats effectively.

CHAPTER 5:
BEST PRACTICES AND LESSONS LEARNED

REAL-LIFE CASE STUDIES

Case studies provide invaluable insights by showcasing how incident response plans work in real-world situations. One case study might describe how an NGO successfully implemented a cybersecurity incident response plan. This study could highlight best practices like regular security training for staff, using advanced encryption methods, and setting up clear protocols for identifying and responding to cyber threats. Key takeaways might include the importance of leadership commitment to cybersecurity, the benefits of regular security audits, and the positive effects of the development of a security-aware culture among staff.

Another case study could focus on an organization that faced a significant cyber breach. It would outline the steps the organization took to manage the breach, from immediate containment measures to long-term improvements in their security posture. Lessons learned might include the critical role of having a strong incident response plan, the value of clear communication protocols during a crisis, and the need for thorough post-incident reviews to understand what went wrong and how to prevent similar incidents in the future. This case could also highlight the position of investing in advanced cybersecurity technologies and continuous training programs to enhance staff readiness and resilience.

COMMON DANGERS AND HOW TO AVOID THEM

When it comes to incident response planning, common dangers include overlooking non-physical threats, not updating plans regularly, and inadequate training. To address these issues, it's crucial to adopt a practical approach to risk assessment, ensuring that plans are reviewed and updated regularly to reflect the latest threats and best practices. Establishing comprehensive training programs keeps staff informed and prepared. Regular training help ensure that everyone knows their role and can act quickly and effectively in the event of an incident.

PROMISING PRACTICES FROM LEADING NGOS

Building a culture of security within the organization is essential, ensuring that every staff member understands the importance of cybersecurity and their role in maintaining it. Leveraging technology for security management, such as implementing advanced cybersecurity tools and software, can greatly enhance an organization's ability to detect and respond to threats. Collaborating with other organizations is also beneficial, as sharing security insights and experiences can help nonprofits stay ahead of potential threats and adopt innovative solutions. By embracing these practices, these organizations can ensure a strong security posture and effectively protect their operations and assets.

Katalogimi në botim – **(CIP)**

Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

343.296:681.3(036)

Limaj, Jon Developing a Security Plan and Incident Response Plan : handbook for NGOs / Jon Limaj. - Prishtinë : Qendra Kosovare për Studime të Sigurisë, 2024. - 10 f. ; 28 cm.

ISBN 978-9951-842-33-4

KCSS
Kosovar Centre for Security Studies

ABOUT KCSS

Established in April 2008, the Kosovar Centre 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 16th Anniversary. For more about KCSS, please visit and follow our social media accounts:

www.qkss.org
www.securitybarometer.qkss.org

@KCSSQKSS

ISBN 978-9951-842-33-4