ARCUS

CYBERSECURE KOSOVO: STRENGTHENING CYBER RESILIENCE IN MEDIA & CIVIL SOCIETY

2025

eGA
e-governance academy

Funded by
the European Union

CYBERSECURE KOSOVO: STRENGTHENING CYBER RESILIENCE IN MEDIA AND CIVIL SOCIETY

AUTHOR:
BEHAR FAZLIU

May, 2025

ABOUT THE PUBLICATION

This publication was prepared within the framework of the KnowCyber Grants for the Western Balkans project, funded by the European Union and implemented by the e-Governance Academy (eGA), in cooperation with Open Data Kosovo and ARCUS. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the European Union, the e-Governance Academy, Open Data Kosovo, or ARCUS.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to the European Union for funding the KnowCyber Grants for the Western Balkans project, and to the e-Governance Academy (eGA) for their leadership in supporting its implementation.

We also extend our heartfelt thanks to our implementing partner ARCUS, whose collaboration and commitment were instrumental in strengthening the cybersecurity capacities of civil society organizations in Kosovo.

Special appreciation goes to the cybersecurity experts, trainers, and consultants who shared their knowledge and provided hands-on support throughout the assessments, workshops, and mentoring sessions. Their expertise and dedication played a vital role in building a more resilient digital environment for media and civil society actors.

We would also like to acknowledge the participating organizations for their openness, engagement, and willingness to improve their cybersecurity posture. Their cooperation made it possible to identify meaningful insights and develop tailored recommendations.

Lastly, we thank all individuals and stakeholders who contributed to the research and data collection phases, your input was essential in shaping the content and outcomes of this publication.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As digital threats grow more sophisticated, Kosovo's media and civil society organizations (CSOs), which are key defenders of democracy, face increasing cyber risks that threaten their independence and daily operations. To address this, **Open Data Kosovo (ODK)** and **Arcus**, with support from the **e-Governance Academy (eGA)** through the **KnowCyber Grants for the Western Balkans**, launched the CyberSecure Kosovo project.

The initiative aimed to assess, strengthen, and benchmark the cybersecurity posture of **10 media and CSO organizations** across the country. **Over six months**, the project team conducted detailed cybersecurity assessments based on a **11-domain framework** covering areas such as **data protection, email security, incident response, and disinformation defense**.

Each organization received customized support, ranging from penetration testing and policy development to technical configuration, awareness training, and investment planning. Reassessments were conducted to evaluate progress and identify remaining risks.

Key findings

- The average baseline cybersecurity score was low: 3.49 out of 10. Major gaps were found in incident response, legal compliance, endpoint security, and staff awareness.
- The strongest area was disinformation defense. Media organizations had strong editorial practices to detect and counter influence operations.
- After interventions, the average score improved to 4.07, with notable gains in data protection, compliance, employee training, and incident response.
- All 10 organizations received detailed domain-by-domain recommendations. High-impact services such as policy drafting, phishing awareness training, and email security improvements were commonly delivered.
- Systemic weaknesses persist:
  - Cybersecurity is still seen as a technical, not leadership, responsibility.
  - Most organizations lack dedicated staff or budgets for cybersecurity.
  - Few have incident response plans or supply chain security measures.
  - Readiness for advanced cyber threats remains low.

Policy and Investment Priorities

To build long-term cyber resilience in Kosovo's nonprofit sector, the report calls for:

- A national cybersecurity support fund for civil society and media;
- Security standards in donor-funded projects;
- A centralized cybersecurity policy toolkit for NGOs;
- Leadership-focused training and awareness initiatives;
- Support for peer learning and cybersecurity communities of practice;
- Localized training content in Albanian and Serbian;
- Emergency funding for real-time cyber incident response.

CyberSecure Kosovo shows that targeted, context-aware support can significantly improve cyber hygiene and awareness, even in resource-constrained environments. But the scale of the challenge is clear: **without sustained investment, policy support, and capacity building, civil society in Kosovo will remain vulnerable to evolving digital threats.** This report offers both a diagnosis and a path forward. **Now is the time to act,** by investing in the digital resilience of Kosovo's democratic institutions.

I. INTRODUCTION

Background:
Rising Cybersecurity Threats to Media & Civil Society in Kosovo

Cyber threats have become a serious concern for Kosovo's media and civil society organizations. As critical voices in a democratic society, these organizations rely heavily on digital tools to communicate, organize, and advocate. But this reliance has made them frequent targets for cyberattacks, disinformation campaigns, and digital surveillance.

High-profile incidents, including cyberattacks on Koha.net, Gazeta Express, and Insajderi.org have exposed the vulnerabilities of independent media. Similarly, civil society organizations (CSOs) face growing risks, as they often handle sensitive data and challenge powerful interests, yet lack the resources or technical capacity to defend against advanced digital threats.

The rapid pace of digitalization in Kosovo has far outpaced the cybersecurity readiness of these groups, leaving them exposed to both criminal and politically motivated actors.

Project Objectives and Scope

To address this gap, **Open Data Kosovo (ODK)** and **Arcus**, with support from the **e-Governance Academy (eGA)**, launched **CyberSecure Kosovo: Strengthening Cyber Resilience in Media and Civil Society**.

This project, funded under the **KnowCyber Grants** for the **Western Balkans**, focused on assessing and improving the cybersecurity posture of ten selected media and CSO organizations.

The project's objectives were to:

1. Assess each organization across **11 key cybersecurity domains;**
2. Deliver **tailored technical and policy interventions**, including penetration testing, incident response planning, policy development, endpoint hardening, and training;
3. Conduct **follow-up reassessments** to track progress and identify remaining gaps;
4. Produce a final report with findings, lessons learned, and policy recommendations for national stakeholders and donors.

DESCRIPTION OF PARTNERS & ROLES

OPEN DATA KOSOVO

The project was led by **Open Data Kosovo (ODK)**, a respected civil society organization with a **decade of experience in digital governance and civic tech.** ODK managed stakeholder engagement, project coordination, stakeholder alignment, and communications. Its strong local reputation helped align the initiative with **national digital development efforts.**

ARCUS

Arcus, a Kosovo-based **offensive cybersecurity company** with international reach, provided the project's technical leadership.
Arcus led all cybersecurity assessments, interventions, and data analysis. Its team of certified experts **(OSCP, CRTO, & CREST)** conducted the technical work, identifying vulnerabilities, performing penetration tests, & developing security strategies.

Together, **ODK and Arcus** combined local trust with technical depth to deliver a high-impact initiative that addressed **both structural and operational cybersecurity challenges facing Kosovo's civil society and media organizations.**

II. METHODOLOGY

Cybersecurity Assessment Framework

The project was built around a comprehensive assessment framework that evaluated each organization's cybersecurity posture across 11 critical domains. Each domain included measurable subdomains to allow both granular and overall scoring. The framework reflected international best practices but was designed to be practical and relevant for local organizations with varying levels of digital maturity. For more details see the template: *Annex 1: Cybersecurity Assessment Scoresheet*.

01 **Data Protection**

02 **Content Security**

03 **Network Security**

04 **Endpoint Security**

05 **Email Security**

06 **Identity & Access Management (IAM)**

07 **Incident Response & Recovery**

08 **Compliance &Legal Requirements**

09 **Employee Training & Awareness**

10 **Disinformation Defense**

11 **Physical Security**

SELECTION OF BENEFICIARY ORGANIZATIONS

The project engaged **10 organizations:** five media outlets and five CSOs, selected to reflect diversity in:

- Mission and public visibility,
- Size and technical capacity,
- Willingness to engage in a full cybersecurity improvement cycle.

This diversity ensured that findings would be representative of broader sector challenges and useful for future policy and investment decisions.

ASSESSMENT TOOLS AND TECHNIQUES

The core assessment tool was a structured Cybersecurity Assessment Score Sheet, which scored each organization's status in the 11 domains.

The assessment process included:

- In-person interviews with leadership and IT staff,
- Structured reviews of policies, governance, and technical setups,
- Hands-on inspection of digital infrastructure and security settings,
- Validation of findings through documentation and technical evidence,
- Qualitative observations on awareness, behavior, and readiness.

This approach provided a thorough understanding of both technical vulnerabilities and organizational gaps.

TAILORED INTERVENTION APPROACH

Following the assessments, each organization received a customized support package based on its unique risks and operational needs. Most organizations received a detailed recommendations report aligned with the 11-domain framework.

In addition, interventions included:

- Penetration tests (for organizations with exposed services or suspected vulnerabilities),
- Policy development (for those lacking formal governance or response plans),
- Technical configuration support (email hardening, endpoint protection, router security, MFA setup),
- Security planning and investment roadmaps,
- Training sessions for staff and technical teams,
- Guides and templates for ongoing internal use,
- Support in procuring secure tools where needed.

Each intervention was designed to be actionable and sustainable within the organization's existing capacity.

POST-INTERVENTION REASSESSMENTS

After the interventions, each organization was reassessed using the same framework and scoring sheet, allowing for direct before-and-after comparisons. The reassessment included:

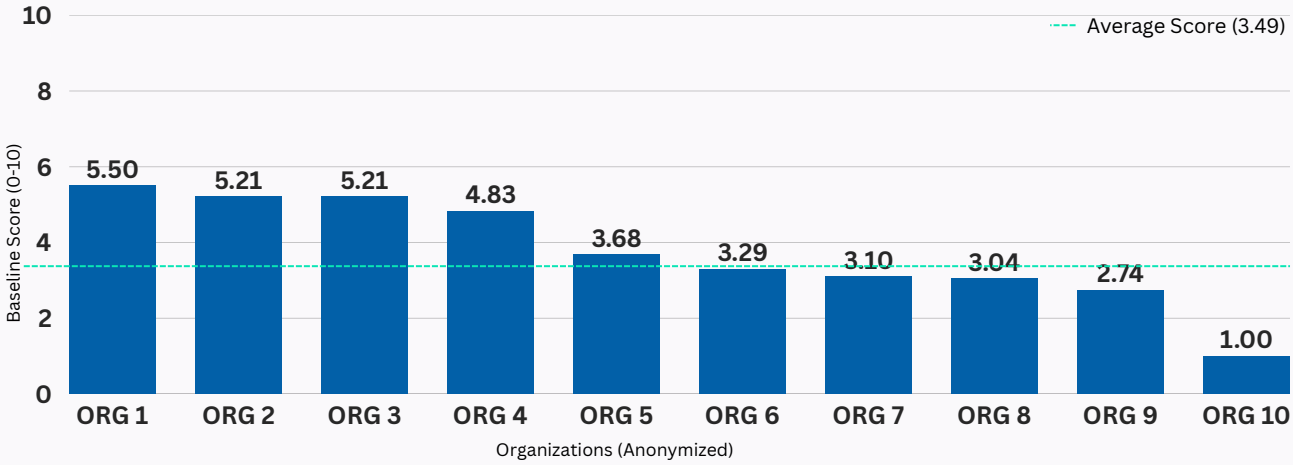
- Verifying implementation of recommendations,
- Reviewing updated practices and configurations,
- Gauging leadership engagement and staff awareness,
- Capturing qualitative signs of progress, like adoption of policies or budgeting for security improvements.

While not all changes could be implemented within the project timeline, the reassessment also looked for signs of sustained commitment, such as initiated procurement or policy adoption.

III. FINDINGS FROM INITIAL ASSESSMENTS

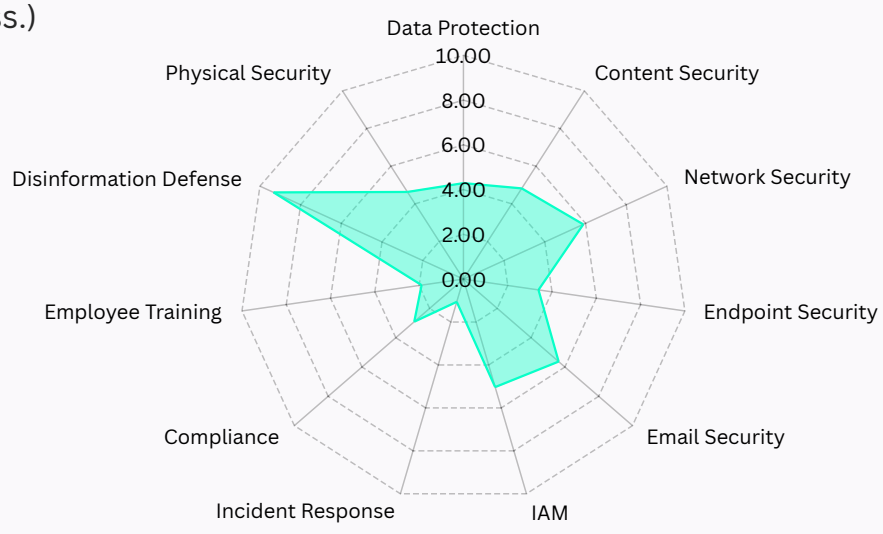
Overall Cyber Security Baseline

The initial assessments revealed a low average cybersecurity score of **3.49** out of **10** across the **10 organizations.** These scores confirmed an urgent need for tailored support, especially for grassroots or infrastructure-light CSOs.



Average Scores Across Cybersecurity Domains

The following graph highlights the average cybersecurity scores across 11 key domains, clearly showcasing strengths (Disinformation Defense and Network Security) and revealing critical weaknesses (Incident Response and Employee Awareness.)



Strengths and Common Weaknesses

Key Strengths:

- Disinformation Defense scored highest **(avg. 9.33).** Media organizations had strong editorial standards to detect and counter misinformation. Disinformation defense was only applicable to media organizations.
- Email Security **(5.63)** and Network Security **(5.89)** showed decent performance due to use of managed services like Google Workspace and default router protections.
- Some organizations had implemented MFA and used identity platforms, contributing to an IAM average of **5.03.**

Common Weaknesses:

- Incident Response and Recovery was the weakest domain **(avg. 1.06).** No formal procedures, roles, or communication plans existed for handling incidents.
- Employee Training and Awareness **(1.89)** was critically low. While media staff had strong disinformation literacy, they lacked awareness on phishing, passwords, and social engineering.
- Compliance and Legal Requirements **(2.91)** revealed a general lack of understanding of data protection laws like GDPR. Few had written policies or formalized consent processes.
- Endpoint Security **(3.39)** was weak. Many devices were outdated, lacked antivirus or encryption, and were used without central management or admin restrictions.

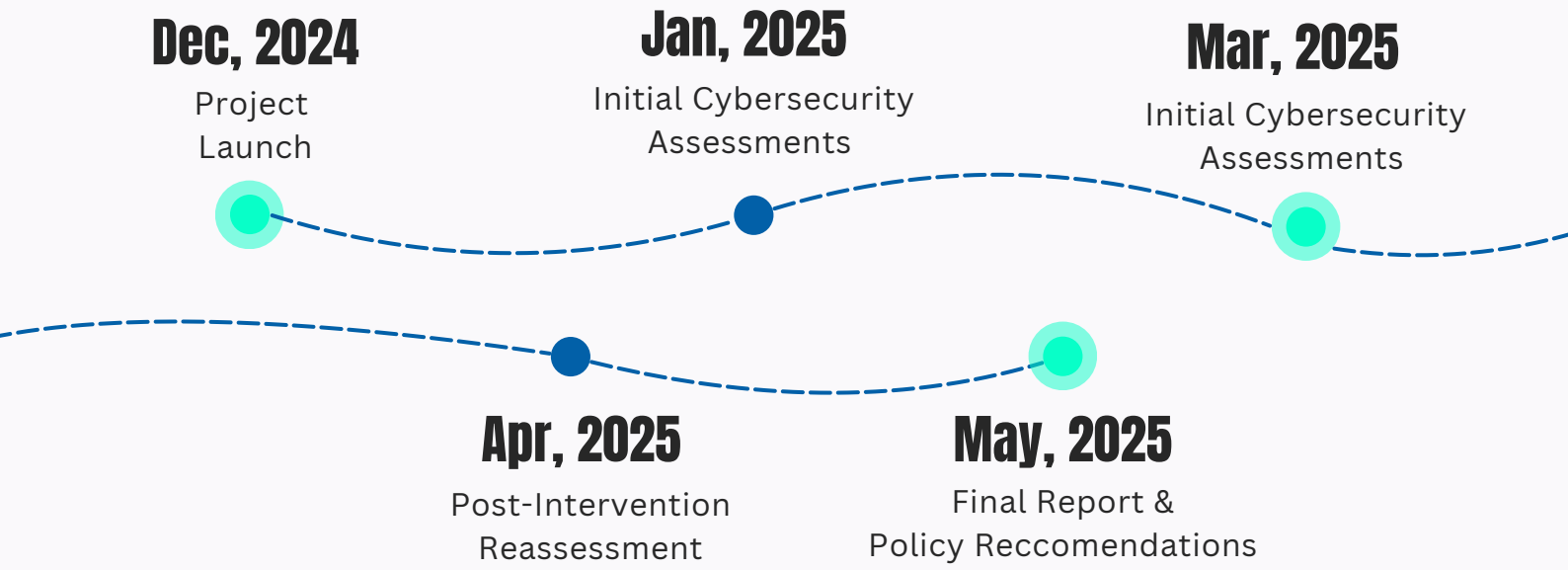
Real-World Examples (Anonymized)

- A CSO publicly exposed sensitive beneficiary data through an unprotected Google Drive folder.
- A media outlet's WordPress admin panel was accessible via a simple URL with no access restrictions.
- Protest volunteers coordinated via a shared Gmail account without MFA, risking exposure of operations.
- Several organizations had suffered breaches (spam campaigns, data loss) but had no response or documentation processes in place.
- These findings showed that while some strengths existed, mainly in media organizations, there were widespread and severe cybersecurity gaps across nearly all domains. These findings directly informed the next phase of the project: delivering targeted interventions.

Domain-by-Domain Summary (Pre-Assessment)

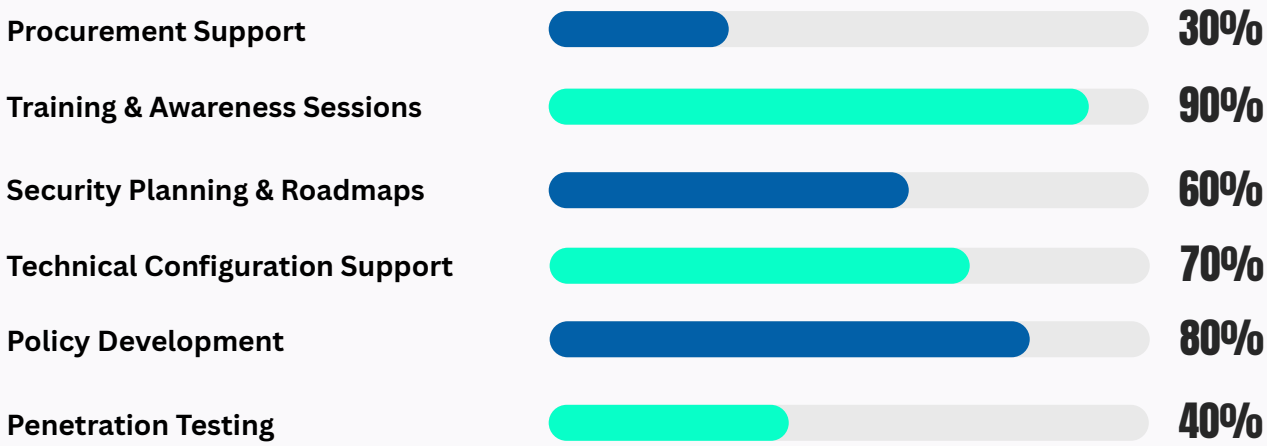
#	Domain	Score	Key Observations
1	**Data Protection**	**4.29**	No structured data classification or encryption policies. Backups were inconsistent and rarely tested.
2	**Content Security**	**4.82**	Many websites used outdated plugins, lacked access controls, and shared publishing credentials.
3	**Network Security**	**5.89**	Basic router protections in place, but lacked monitoring, segmentation, and secure Wi-Fi configurations.
4	**Endpoint Security**	**3.39**	Mixed device usage, outdated software, and poor patch management. No centralized policies.
5	**Email Security**	**5.63**	Managed platforms helped, but SPF/DKIM/DMARC were often missing. Password reuse was common.
6	**IAM**	**5.03**	Some MFA use, but shared accounts and lack of role-based access were
7	**Incident Response**	**1.06**	No playbooks, designated roles, or reporting procedures. Incident handling
8	**Compliance**	**2.91**	Few organizations understood legal requirements. No DPO roles, unclear consent practices.
9	**Employee Awareness**	**1.89**	Minimal technical training. No phishing simulations or awareness programs.
10	**Disinformation Defense**	**9.33**	Media outlets excelled here. CSOs lagged slightly in structured defense practices.
11	**Physical Security**	**4.63**	Mixed setups. Some had CCTV and badge access, but others lacked basic access controls.

IV. TAILORED INTERVENTIONS DELIVERED



Scale of Tailored Cybersecurity Interventions Delivered

Following the initial assessments, the project team implemented targeted interventions to address the specific cybersecurity gaps of each organization. Interventions were prioritized based on risk severity, organizational capacity, and relevance to core operations.



TYPES OF INTERVENTIONS

1. Penetration Testing

Several media outlets and larger CSOs received penetration tests to simulate real-world attacks. These tests focused on websites, public-facing infrastructure, and internal networks.

Key outcomes included:

- Discovery of exposed admin panels and weak authentication;
- Identification of outdated and vulnerable software;
- Detailed reports showing exploitation paths and mitigation steps.

2. Security Plans & Policy Drafting

Many organizations lacked formal cybersecurity documentation.
The project delivered customized policies and plans, such as:

- Cybersecurity governance frameworks (roles, responsibilities, escalation paths);
- Data classification, retention, and disposal policies;
- Basic incident response recommendations & guidance and email threat handling guides;
- Acceptable use and password policies.
- Templates and relevant materials supported adoption and implementation.

3. Security Configurations

Where feasible, technical changes were implemented directly.

These included:

- Setting up SPF, DKIM, and DMARC for secure email;
- Assistance with rolling out antivirus and patching schedules for endpoints;
- Assistance with reconfiguring firewalls and routers for stronger protections;
- Enabling MFA and applying access control best practices.

Where hands-on changes weren't possible, organizations received step-by-step guides and follow-up support.

4. Awareness and Training Sessions

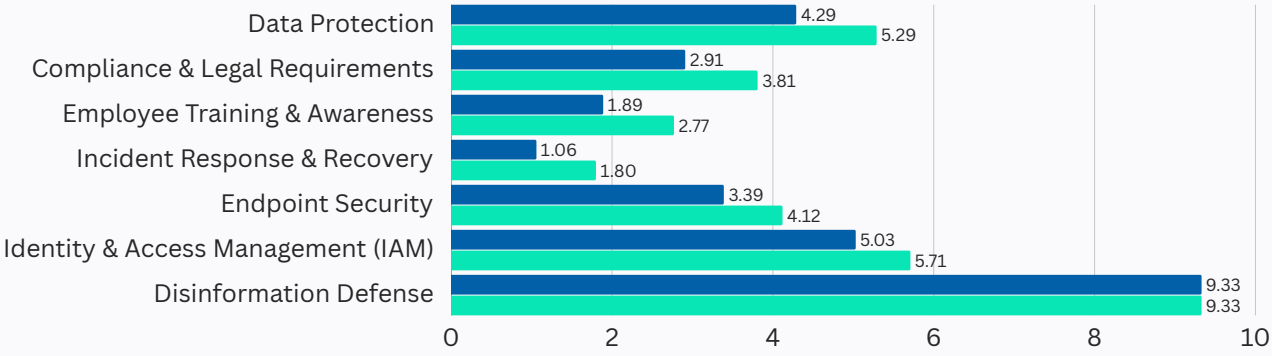
Cybersecurity awareness was a major gap, so tailored training was delivered to staff and leadership. Topics included:

- Phishing detection, password hygiene, and general security practices;
- Cyber threat briefings tailored for journalists and media staff;
- Basics of incident response and day-to-day security practices.

Training included presentations, guidebooks, and long-term resources, delivered online or in person based on each organization's needs. These practical, scalable steps set the stage for stronger cybersecurity and post-intervention reassessment.

V. POST-INTERVENTION REASSESSMENT FINDINGS

After tailored interventions were completed, each organization was reassessed using the same 11-domain framework to measure progress and identify remaining gaps.



Before vs After: Score Comparison: Average score increased from 3.49 to 4.07 out of 10. Most domains showed measurable improvement, confirming the value of targeted support. *Disinformation Defense remained at 9.33, with no room for numerical improvement.*

Domain-by-Domain Summary (After-Assessment)		
#	**Domain**	**Average Score Increase**
1	**Data Protection**	**(+ 1.00)**
2	**Compliance & Legal Requirements**	**(+ 0.90)**
3	**Employee Training & Awareness**	**(+ 0.88)**
4	**Incident Response & Recovery**	**(+ 0.74)**
5	**Endpoint Security**	**(+ 0.73)**
6	**Identity & Access Management (IAM)**	**(+ 0.68)**
7	**Disinformation Defense**	**(+ 1.00)**

LESSONS LEARNED

Establish cybersecurity standards and policies

Invest in leadership focused training

Raise cybersecurity awareness

Build in-house technical capabilities

Bridge the cybersecurity gap

- **Tailored support works:** The most improvement came from hands-on guidance and organization-specific resources.
- **Policy adoption is achievable:** Even without prior documentation, many groups successfully implemented key cybersecurity policies.
- **Training delivers quick wins:** Awareness efforts led to immediate improvements in digital hygiene and behavior.
- **Capacity remains a limiting factor:** Technical improvements that require infrastructure or dedicated staff progressed more slowly.
- **Editorial vs technical divide:** Media organizations excelled at countering disinformation but struggled with broader IT security—a gap worth bridging.

The reassessment confirmed that structured, personalized interventions can lead to tangible improvements in cybersecurity posture, especially when supported by practical tools, leadership buy-in, and contextual awareness.

VI. KEY INSIGHTS AND ANALYSIS

Overall Cyber Resilience

The project provided a clear snapshot of cybersecurity readiness among Kosovo's media and civil society organizations. While some had strengths, especially in disinformation defense and email security, most were in the early stages of cybersecurity maturity.

Pre-intervention average:	Post-intervention average:
3.49	4.07

The increase confirms that targeted support is effective, but also shows that most organizations are still far from meeting basic cybersecurity standards.
Most organizations remained reactive, only addressing risks when identified, rather than proactively managing them.

Systemic Weaknesses

The following issues were common across nearly all organizations:

1. Lack of Cybersecurity Governance

- Few had formal policies before the project.
- Cybersecurity responsibilities were unclear or assigned informally to IT staff or external providers.

2. Underinvestment in Security Tools

- Many lacked basic protections like firewalls, endpoint detection, or secure backups.
- Even when low-cost tools were available, staff capacity to use them was limited.

3. Cultural and Organizational Gaps

- Cybersecurity was seen as an IT issue, not a leadership responsibility.
- Security was not integrated into daily operations, HR, procurement, or communications.

4. Minimal Incident Preparedness

- No incident playbooks or predefined response roles.
- Few organizations had ever handled or documented a cyber incident properly.

5. Ignored Third-Party Risks

- No formal reviews of vendor security.
- Outsourced services lacked basic security clauses or oversight.

Positive Developments in Cyber Hygiene

Despite the low baseline, progress was made in core areas:

- **Policy Adoption:** Most organizations received or committed to using essential policies on access, data protection, and incident response.
- **Behavioral Change:** Staff reported stronger passwords, enabled MFA, and more careful handling of email.
- **Awareness and Visibility:** Leadership teams developed a clearer understanding of their cybersecurity risks and exposure.

Proactive Engagement: Some began budgeting for cybersecurity and seeking continued external support.

Readiness for Advanced Threats

While the foundations have been laid, most organizations are not yet ready to face sophisticated cyber threats such as:

- **Spear phishing**
- **Credential theft**
- **Infrastructure compromise**

Critical gaps include:

- **No threat monitoring or log management**
- **No threat intelligence integration**
- **Limited network segmentation or breach containment strategies**

07

However, the shift in mindset and the adoption of basic controls suggest that these organizations are ready to progress, if supported with ongoing investment and technical capacity building.

VII. FUTURE INVESTMENT AND CAPACITY BUILDING NEEDS

The project proved that quick wins are possible with targeted support. But lasting cybersecurity resilience requires long-term investment, institutional support, and local capacity building. The following areas should guide future donor funding, technical assistance, and national planning.

#	Investment Area	What	Why	Who Benefits
1	**In-House Technical Capabilities**	Train focal points, certify staff, provide secure tools	Build internal resilience and reduce external reliance	Technical teams, leadership
2	**Regular Pen Testing & Assessments**	Conduct simulations and red team exercises	Boost real-world preparedness	All staff, IT teams
3	**Long-Term Cybersecurity Roadmaps**	Develop 3–5 year security plans	Ensure sustained improvements and accountability	Org management, funders
4	**Peer Communities & Networks**	Enable knowledge exchange and support circles	Foster collective learning and resilience	All participating orgs
5	**Localized Training Resources**	Tailored multilingual educational content	Improve access, relevance, and adoption	CSOs and media in remote areas
6	**Emergency Response Support**	Hotline, emergency grants, incident responders	Help small orgs recover from attacks quickly	Smaller, under-resourced orgs
7	**Integrated Capacity Building**	Cybersecurity integrated in core donor support	Embed security into daily operations and planning	Whole sector and donor community

1. Strengthen In-House Technical Capabilities: Most organizations depend on outside help for cybersecurity. Future efforts should build internal capacity by:

- Training dedicated cybersecurity focal points
- Supporting certifications (e.g., CompTIA Security+, ISO 27001)
- Providing affordable or donated tools (endpoint detection, encrypted storage, access management)

Why it matters: Resilience requires internal know-how, not just external support.

2. Support Regular Penetration Testing and Vulnerability Assessments: Few organizations have experience with offensive security testing. Strengthen readiness by:

- Funding regular penetration tests, especially for public-facing platforms
- Conducting red team exercises that simulate attacks and test staff response
- Including CSOs and media in national cyber drills and tabletop exercises

Why it matters: Simulated attacks build practical preparedness for real-world threats.

3. Fund Long-Term Cybersecurity Roadmaps: Every organization should develop and follow a 3–5 year plan that includes:

- A timeline for tech upgrades and policy implementation
- Training schedules and awareness activities
- Incident response testing and improvement

Small grants can support key milestones like equipment upgrades or staff training.

Why it matters: One-time interventions fade without a structured, funded roadmap.

4. Build Peer Communities and Networks: Encourage collaboration by creating communities of practice through:

- Local and regional workshops and events
- Online platforms for sharing tools, templates, and lessons
- Partnerships between CSOs and cybersecurity experts or universities

Why it matters: Peer learning is often more effective and sustainable than top-down training.

5. Localize and Maintain Training Resources: Develop and regularly update cybersecurity content tailored to nonprofits, including:

- On-demand video modules
- Interactive quizzes and practical guides
- Offline-friendly materials (printable toolkits)
- Gender- and privacy-sensitive content
- Language availability in Albanian and Serbian

Why it matters: Accessibility, relevance, and cultural fit are key to adoption.

6. Create Emergency Response Support for Cyber Incidents: Smaller organizations need help when attacks happen. Establish support such as:

- A hotline or rapid-response team for urgent cases
- Emergency grants to recover from incidents (e.g., ransomware)
- Retainers for trusted cybersecurity service providers

Why it matters: Most CSOs have no one to call during a crisis.

7. Integrate Cybersecurity into Core Capacity Building: Make cybersecurity a standard part of how civil society organizations are supported. This includes:

- Adding cybersecurity into donor-funded development frameworks
- Requiring basic cybersecurity planning in core operational grants
- Training boards and directors on their responsibility to manage cyber risks

Why it matters: Cybersecurity should be treated as a core organizational function, not a side issue.

In short: Kosovo's civil society is willing to strengthen its cybersecurity, but cannot do it alone. Long-term, locally grounded investment is essential to build a secure and resilient civic ecosystem.

IMMEDIATE	SHORT-TERM	LONG-TERM
Establish a dedicated mechanism to provide civil society and media with access to assessments, tools, emergency response, and policy development assistance.	Integrate clear requirements like MFA, data protection, and basic training into all donor contracts to raise the baseline across the sector.	Develop a centralized cybersecurity policy toolkit for NGOs. Invest in leadership and awareness training. Include civil society in the national cybersecurity strategy.

VIII. CONCLUSION

The **CyberSecure Kosovo project** served as both a diagnosis and a catalyst for improving cybersecurity in Kosovo's media and civil society organizations. Through detailed assessments, tailored interventions, and structured follow-ups, the project uncovered not only technical vulnerabilities but also deeper organizational and systemic gaps.

The results show that even modest, well-targeted support can lead to real progress. **Organizations that previously had no cybersecurity practices in place began adopting basic policies, training staff, and implementing essential protections.** Awareness increased, leadership engagement improved, and some organizations began planning future investments.

However, the project also revealed a clear warning: **most civil society organizations remain unprepared for advanced cyber threats.** They continue to face serious challenges due to limited technical capacity, lack of funding, and minimal incident response readiness. Without continued support, the improvements made during this project may not be sustained.

Cybersecurity is no longer a purely technical issue, it is a democratic necessity. Media and civil society groups play a vital role in defending rights, exposing corruption, and informing the public. Their digital safety is directly tied to the strength of Kosovo's democracy.

This report is not the end of the journey, it is the beginning of a roadmap. A roadmap that **calls on policymakers, donors, and stakeholders to act now:**

- **To make cybersecurity support a permanent feature of civil society funding**
- **To embed resilience into policy and governance frameworks**
- **To ensure that no organization is left vulnerable in the digital age**

The threats are growing, but so is the readiness to respond. With the right support, Kosovo's civil society can build a secure digital foundation for years to come.

Funded by
the European Union

CONTACTS

www.opendatakosovo.org

info@opendatakosovo.org