USAID FROM THE AMERICAN PEOPLE | PROgress PROTECTING GLOBAL RIGHTS | Freedom House | Internews Local voices. Global change.

DIGITAL SECURITY FRAMEWORK FOR HUMAN RIGHTS PROGRAMMING

HUMAN RIGHTS SUPPORT MECHANISM PROGRAM

This Digital Security Framework was developed by Freedom House and Internews as part of the USAID-funded Human Rights Support Mechanism (HRSM).

Report period: January 2022 – May 2023

Published: June 2023

Freedom House and Internews would like to thank USAID for its commitment to the HRSM learning agenda. Freedom House and Internews wish to extend their particular gratitude to HRSM program teams and partnering human rights organizations across the globe who contributed their invaluable time and input for the development of this learning product. Thanks are also owed to the many digital security and program experts who reviewed this document to ensure it was technically sound. Due to security considerations, not every contributor is listed by name.

Authors

Megan Guidrey | Director of Monitoring and Evaluation, Internews

Deanna Kolberg-Shah | Evidence & Learning Team Technical Lead, Freedom House

Leah Squires | Monitoring, Evaluation, and Learning Specialist, Freedom House

Expert Reviewers

Ashley Fowler | Senior Manager of Internet Freedom & Resilience Programs, Internews

Łukasz Król | Journalist Digital Security Specialist, Internews

Rafael G. Nunez | Senior Program Associate, Freedom House

Cover Image:
A group of men track presidential election results on their phones at the Gikomba market in Nairobi, Kenya, in August 2022. (*Credit: Alamy*)

Introduction

Digital security is crucial for human rights organizations (HROs) because they manage sensitive information and are often at risk of surveillance, cyberattacks, and censorship by governments and other malicious actors. HROs also face escalating harassment, intimidation, and repression because of this digital monitoring and interference.

By prioritizing digital security, HROs can protect their data and communications, safeguard the privacy and safety of their staff and partners, and ensure the continued effectiveness of their work. Strong digital security practices can also demonstrate a commitment to transparency and accountability, building trust with the communities they serve. (For the purposes of this report, HROs include civil society organizations that conduct human rights-focused work and media outlets that cover human rights issues.)

According to Freedom on the Net 2022, digital repression is on the rise, especially in authoritarian countries. Under increasing attack, these HROs need the support of international non-governmental organizations (INGOs) and donors to make the improvements necessary to increase their digital resiliency; however, INGOs and donors lack strong evidence or frameworks for providing this support.

The Digital Security Framework is a learning product that offers preliminary guidance intended for INGOs and other implementers who aid in HRO capacity building. Using this framework, democracy, human rights, and governance (DRG) stakeholders can better plan for, evaluate, and improve digital security support in programs, given the time and resources available.

Digital Security Framework for Human Rights Programming

What is the Digital Security Framework (DSF)?

This reference offers a logical framework for digital security support. It is intended for use by implementing partners to assist in the design, implementation, and monitoring and evaluation of digital security activities. As a learning product that draws on a limited evidence base, this report proposes a theoretical and programmatic approach for digital security efforts. Consequently, the DSF is a starting point for longer conversations about a theory of change for digital security support in DRG programming. The guidance herein should be subject to ongoing testing and refinement in different contexts; implementing partners can work closely with HROs to tailor the DSF based on an organization's specific needs, operating context, and available resources.

Digital security support is a common programmatic approach to enhance the security of organizations working on human rights in areas where they are at risk. It is distinct from incorporating a digital security protocol, which is designed to safeguard implementing partners and local beneficiaries during program implementation, including that of any digital security support activities. The DSF reflects digital security as a programmatic approach and does not address how to design digital security protocols.

This report was produced by monitoring, evaluation, and learning (MEL) experts from Freedom House and Internews, under the purview of the USAID-funded Human Rights Support Mechanism (HRSM). The logical framework emerged from an iterative learning process that drew on a diverse, albeit observational evidence base from HRSM programming between 2018–2023. It reflects the real-world experiences and needs of front-line HROs, and inputs from seasoned digital security specialists have added a measure of technical expertise to the framework. (See "Annex 3: Methods and Sources" for further detail.)

Many HRSM programs support HROs that work in challenging environments and have faced various digital security threats. The DSF thus applies an organizational rather than an individual lens to digital security support. While individual human rights defenders face similar digital threats—and work toward the same outcomes—they require different assessment and training interventions not addressed by this framework. Additional evaluation is required to build a digital security framework specific to the experience of individual human rights defenders.

Digital Security Interventions & Outcomes

There is no universal means to assess digital security needs, implement digital security supports, or measure digital security interventions since any approach is highly contextual. The DSF, which includes recommended outcomes and indicators, offers a means for designing, monitoring, and evaluating these diverse digital security programs.

This framework describes three main types of digital security interventions, reflecting digital security assistance that is likely achievable based on typical award timelines in human rights programming:

1. **Emergency Interventions** typically refer to an incident response around an immediate, specific threat or an attack that an organization has already experienced. While rapid data recovery or other emergency interventions last only days, programs that last less than eight months likely can only respond to a series of emergency requests. During this time, HROs may also receive targeted education and corresponding mitigation and/or prevention tools that help them survive the particular threat or attack. In an operating context where there is an immediate threat, i.e., ongoing surveillance, implementing partners should include incident response capabilities in the program design.
2. **Short-term Interventions** typically include ongoing support from the same digital security experts to HROs for a period of nine to twelve months. Activities can include emergency support, capacity assessments, and training and mentorship. While emergency interventions prioritize building an HRO's awareness or knowledge around a specific incident, short-term interventions can address both immediate needs and broader digital

security issues. These programs focus on preventing attacks and usually provide digital security support more broadly. The limited timeframe often still translates to limited assessment and training opportunities, so comprehensive, more sustainable support mechanisms likely remain out of reach.

3. **Long-term interventions** typically aim to improve holistic digital safety and security practices that better equip partners to respond to increasingly advanced digital threats. These year-plus programs incorporate activities typical of a short-term intervention, beginning with a focus on immediate needs and general digital security know-how. With a longer timeline, these interventions are distinguished by depth over breadth, progressing to implement more sophisticated assessments, as well as context-specific, mitigating and preventive solutions to address complex digital security threats.

This framework offers general guidance for implementation. Since programs vary in timing, budget, scope, and context, it's difficult to draw a firm line between different digital security support interventions. For each type of intervention, this guide provides a summary of the assessment methods to determine digital security needs; common digital security activities; financial and material support needed for effective implementation, monitoring, and evaluation; associated outcomes and indicators; and any known drawbacks related to specific interventions and associated measurement methods.

The DSF identifies three core digital security outcomes that can be measured as a result of digital security program assistance:

1. **Awareness** refers to changing participants' beliefs that digital threats pose a legitimate risk to organizational and personal safety.
2. **Knowledge** refers to changing participants' understanding of different digital security threats and the appropriate actions and tools to mitigate those risks. Knowledge development distinguishes itself from awareness raising because it requires a deeper understanding of threats and tactics, i.e., identifying which threats are most likely in a given context, and then prioritizing mitigation and preventative measures that are commensurate with the threat environment.
3. **Adoption** refers to changing participants' abilities and willingness to develop and implement digital security practices that address organizational and/or personal risks. Changes to awareness and knowledge must also be accompanied by a willingness to institute operational changes, so that organizations can build sustainable, resilient digitally secure systems and processes.

These three outcomes often have a cascading effect, building on each other and dependent upon the type of digital security intervention.

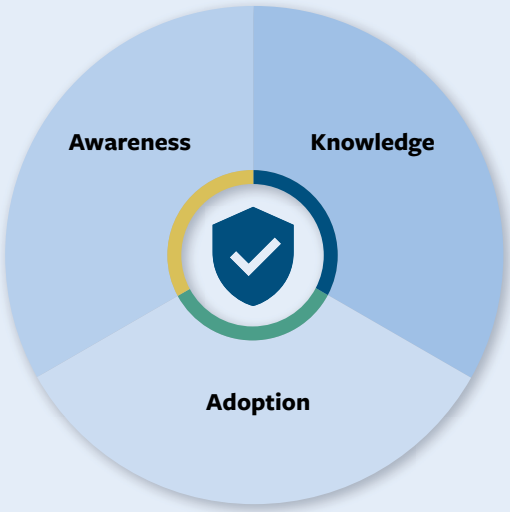
Emergency Intervention	Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms
Short-term Intervention	• Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms. • Staff have **increased knowledge** of actual digital security threats and mitigation and prevention tactics. • Staff **begin to adopt** digital security practices.
Long-term Intervention	• Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms. • Staff have **increased knowledge** of digital security threats and mitigation and prevention tactics. • Staff **implement** digital security policies/protocols. • Staff **adopt** digital security practices. • HROs have **increased capacity** in both preventative and responsive digital security approaches.

Digital Security Framework as a Cycle

Measuring these core outcomes—awareness, knowledge, and adoption—is a persistent challenge. The effectiveness of an intervention can be difficult to assess because digital security is not something that an organization achieves, but something that it must maintain. While the DSF implies an element of linearity, maintaining robust organizational digital security requires continued support and vigilance. Digital security is a dynamic, context-specific cycle that includes ongoing awareness raising, knowledge acquisition, and practice or policy adoption in response to emerging threats and organizational culture.

Measuring Digital Security Outcomes

Does your program aim to increase digital security awareness, knowledge, or adoption?



Awareness

Believes that digital threats pose a legitimate risk to organization and personal safety

Knowledge

Understands different digital security threats and appropriate interventions to mitigate those risks

Adoption

Develops and implements digital security practices that address organizational and/or personal risks

Achieving a digitally secure future is never the outcome because it is unattainable. The long-run outcome of digital security programming is instead digital security **resilience**, which refers to changes in organizational systems and culture that are contextually specific, adaptive, holistic, and sustainable. Demonstrating digital security resilience is a challenge because 1) it is difficult to document the process by which increased security know-how encourages more secure behaviors online, and 2) it is difficult to document and aggregate individual decision-making as a reflection of organizational change in digital security practices.

Digital security awareness, knowledge, and adoption effectively create a feedback loop, and when measured and assessed consistently over time, that data can promote learning and digital resiliency within an organization; however, the constant vigilance required is difficult to maintain. External and internal challenges can undermine an organization's digital health and resilience potential, reinforcing digital security as a cycle rather than a destination.

1. **Changing threat environments (external)**
   Digital threats or attacks are constantly evolving, so digital security cannot be pinned on a specific technology or tool. The response must always match the digital threat environment, as well as the broader operating environment, which can change suddenly or over time.

2. **Lack of high-quality IT support (external/internal)**
   In focus groups and case studies, implementing partners and HROs noted that sometimes there is an utter absence of digital security experts in the country, particularly in closed or restricted environments. This lack of localized support is critical because it often means that third-party experts or other resources may not function in the local language or be context specific. The language barrier can also make it hard to begin conversations about digital security. In countries where there is existing technical expertise, digital security experts may still lack skill because of the ever-changing

threat environment. Furthermore, HROs may be unable to pay for the support, losing out to other sectors who can pay a premium for such technical expertise.

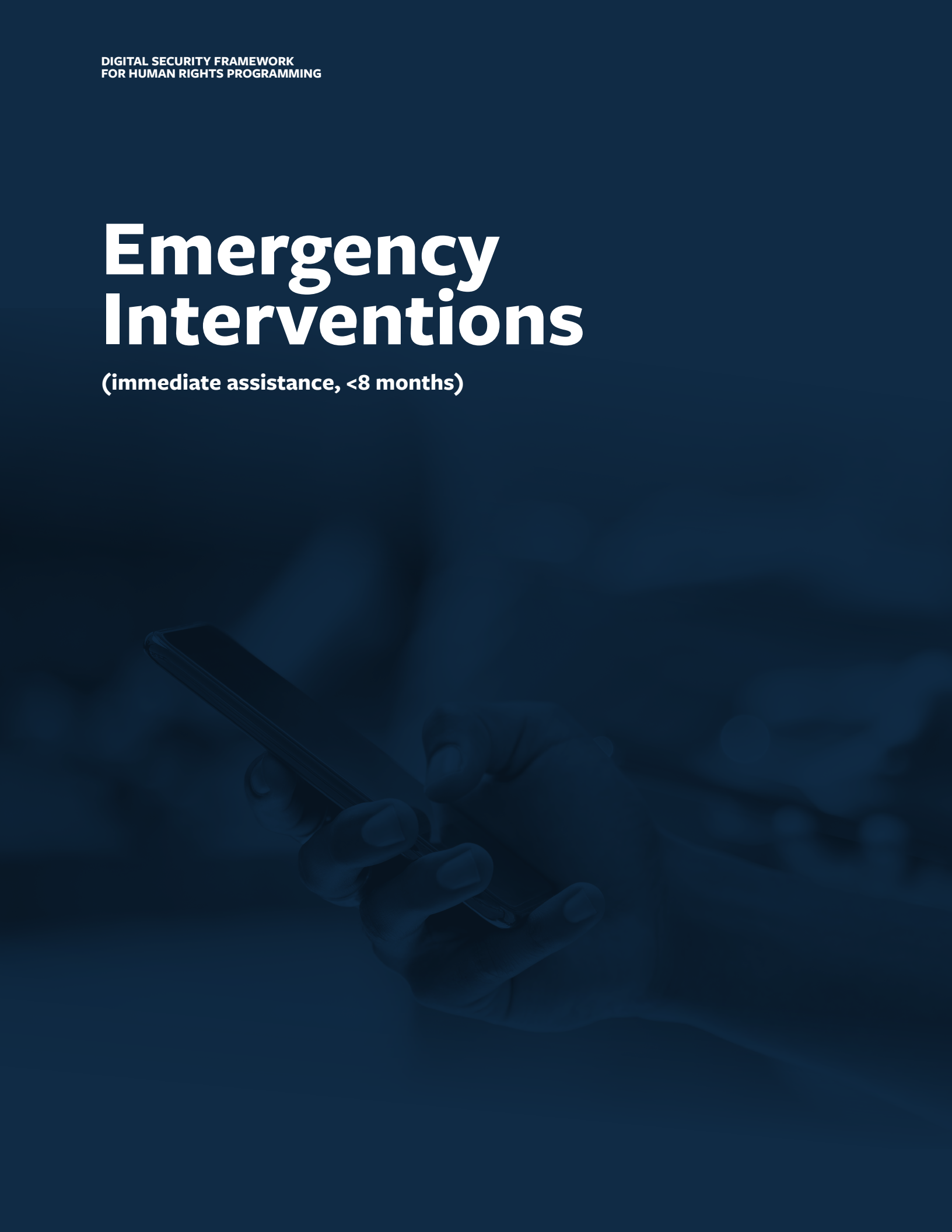
3. **Lack of trust (external/internal)**
   Addressing digital security inherently requires HROs to expose their organizational vulnerabilities, which is a difficult task even under optimal circumstances. Many HROs also already work in digitally and physically insecure environments, so they may be less trusting of implementing partners or outside experts. Likely, the more threats an HRO faces, the less trust there is at the outset. They are already vulnerable, and digital security support programming demands greater vulnerability. There is no explicit evidence or measure of overall trust to support this hypothesis; however, implementing and local partners repeatedly cited this factor as a limitation. Therefore, building trust must be an integral part of digital security.

4. **Common organizational barriers to implementation (internal)**
   - Prioritize their core function. HROs focus on delivering social change in alignment with their missions, sometimes at the expense of operational digital security. Personnel may view digital security training or practices as a mystery and a chore that interferes with completing their work.
   - Uneven understanding and appreciation for the importance of digital safety across an organization. Unmotivated and untrained staff is one of the greatest sources of risk that organizations face because they are only as safe as their weakest adherent to digital security protocols. Most staff are not interested in becoming digital safety experts, so mastering the concepts is not usually a goal, personally or professionally. Furthermore, high staff turnover, as well as the lack of an onboarding process that addresses digital security organizational norms, creates additional vulnerabilities and the need for ongoing training. Buy-in at every level of an HRO is crucial; management also needs to demonstrate commitment, leading by example and dedicating organizational resources to invest in digital security.

Despite these barriers, when HROs encounter a problem stemming from a digital security vulnerability, they become keenly aware of their risks and seek solutions. The three programmatic responses outlined in this reference—Emergency, Short-Term, and Long-Term Interventions—collectively offer a digital security framework for how implementing partners can respond to these risks and better support HROs.

Emergency Interventions

(immediate assistance, <8 months)



Emergency Interventions

(immediate assistance, <8 months)

Typically refer to an incident response around an immediate, specific threat or an attack that an organization has already experienced. While rapid data recovery or other emergency interventions last only days, programs that last less than eight months likely can only respond to a series of emergency requests. During this time, HROs may also receive targeted education and corresponding mitigation and/or prevention tools that help them survive the particular threat or attack. In an operating context where there is an immediate threat, i.e., ongoing surveillance, implementing partners should include incident response capabilities in the program design.

Assessments

Consultation & Diagnostic

Matching the urgency of the situation, a simple consultation between a digital security expert and the HRO is often sufficient to identify and address the most pressing digital safety issue(s). These consultations are usually pre-defined based on the threat facing an organization, such as setting up two-factor authentication for all staff after an account is compromised or retrieving data after a device is hacked. During the consultation, digital security experts and organizations can reference a list of no/low-cost digital security practices to identify additional mitigating or preventative response tactics. If time permits, an accompanying, simple diagnostic can cover key questions related to device security; software, hardware, and apps usage; online practices; personal and/or organizational digital security habits and practices; and threats.

Scope of Digital Safety Support

Support usually begins with addressing the immediate breach or problem identified during the consultation. The purpose of follow-on training during emergency interventions is to 1) increase awareness about certain digital security threats and 2) improve familiarity with specific tools and security practices relevant to the emergent threat or attack at hand. These targeted educational opportunities bolster immediate security needs, and such interventions can also build overall digital security awareness and inspire organizations to explore more extensive, long-term measures.

Examples:

1. *A digital security expert coordinates with necessary staff to recover lost files from a compromised device*
2. *A hands-on workshop where participants learn how to use tools such as password managers or two-factor authentication apps*

Scope of Financial & Material Support

Emergency interventions are difficult to plan for not only because they usually occur unexpectedly, but also because they require immediate attention and financial resources for hardware, software, or third-party services. Addressing a specific incident requires time to consult with digital safety experts, as well as a commitment to adopt new digital security measures. When the list of low/no-cost digital security solutions is exhausted, additional security measures likely require financial investment in hardware, software, or third-party services.

Monitoring & Evaluation

	Activities	Outputs	Outcomes
Emergency Intervention	1. Provide rapid response grant for digital security materials 2. Access to digital security emergency response hotline 3. Conduct diagnostic consultation to raise awareness 4. Conduct low-lift tool use workshops	• Immediate digital security incident is addressed. • Targeted digital security resources and tools are available to staff. • HROs/HRDs are trained on specific digital security threats and on adopting specific mitigation tools.	• Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms.

Indicators:

- *# emergency requests responded to*
- *#HROs/HRDs trained*
- *Reflections from HROs*

For emergency interventions, the immediate outcome should be increased awareness and understanding of a specific security threat or vulnerability. Participants should learn practical steps they can take to address the threat or vulnerability and mitigate any immediate risks to their security. These achievable steps in a short period of time can still have a meaningful impact on the HRO's overall security posture.

The monitoring burden should be light. Implementing partners can focus on output indicators and self-assessments or reflections related to the original consultation objectives.

Drawbacks

1. **Lack of customized training.** Even though targeted training is a best practice, a rapid intervention may lack the budget and timeline to create customized, context-specific activities for the HRO. Training participants may have to independently adapt the solutions conveyed in the training to their own work.
2. **Limited opportunities to build trust** between trainers and organizations.
3. **Digital security backsliding.** Since emergency responses are targeted and specific, the intervention lacks depth, and it is easy for the organization to feel like the issue has been fixed and no further action is required. Furthermore, as an individual threat recedes in prominence, individuals may stop using digital security practices—leaving their organizations at risk.
4. **The techniques may become outdated** in a rapidly changing digital security landscape, and a one-off emergency intervention rarely offers the opportunity to follow-up with HROs and provide updated guidance.
5. **Minimal ability to assess changes in digital security.** Emergency interventions work on a short timeline with a nominal baseline assessment, thus offering limited recourse assessing changes in digital security.
6. **Financial insecurity.** While there are many low/no-cost solutions available, some responses demand a continued financial commitment. Licensed software requires ongoing costs that are often prohibitive for HROs, particularly smaller or newer organizations.

Short-term Interventions

(9–12 months)

Short-term Interventions

(9–12 months)

Typically include ongoing support from the same digital security experts to HROs over a nine-to-twelve-month period. Activities can include emergency support, capacity assessments, and training and mentorship. While emergency interventions prioritize building an HRO's awareness or knowledge around a specific incident, short-term interventions can address both immediate needs and broader digital security issues. These projects focus on preventing attacks and usually provide digital security support more broadly. The limited timeframe often still translates to limited assessment and training opportunities, so comprehensive, more sustainable support mechanisms likely remain out of reach.

Assessments

Consultation & Diagnostic
A simple consultation and/or basic diagnostic form can be sufficient to identify an HRO's most pressing digital security concerns. Consultations may be pre-defined based on the threat facing an organization or reflect needs determined by a questionnaire. A simple diagnostic can incorporate key questions related to device security; software, hardware, and apps usage; online practices; personal and/or organizational digital security habits and practices; and threats. The more detailed the diagnostic, the more insight into a local partner's digital hygiene. This type of assessment can help establish a quasi-baseline, but usually lacks an endline that charts partner progress. During the consultation, digital security experts and organizations can also reference a list of no/low-cost digital security practices to identify additional mitigating or preventative response tactics.

Perceived Digital Risk
Conducting an assessment that captures partners' perceived risk can reveal awareness gaps; mismatches between beneficiary and implementing partner priorities; and show what digital security issues concern partners the most. Since HROs can misinterpret risk, collecting input on perceived risk is not a substitute for assessing an HRO's actual risk. This assessment can still help experts start a conversation about digital security that centers the experience of HROs and their goals. A perceived digital risk assessment is likely most effective when distributed widely across an organization, with data disaggregated by role, to accurately capture variation in people's understanding about digital security. Data should capture overarching assumptions about digital security, as well as targeted beliefs about specific threats and the organization's capacity to respond.

Organizational Capacity Assessment (OCA) or SAFETAG Audit
While conducting an OCA or SAFETAG may not be feasible during a short-term intervention, either may be worthwhile if it can be completed within the first three months of an intervention, as they can inform a strategic plan for improving the overall digital security of an organization. It may also be a good option for implementing partners who anticipate a cost extension will be appropriate for the short-term program. (See "Long-term Interventions" for more detail on OCAs and SAFETAG.)

Scope of Digital Safety Support

Support usually begins with any relevant emergency response and preparation required by the HRO, before focusing on expanded, generalized digital security training to promote proactive digital safety. The purpose of training during short-term interventions may include: 1) increasing awareness and/or knowledge; 2) tool-specific guidance; and 3) digital security mitigation and/or prevention strategies. Short-term interventions can provide training that focuses on helping partners understand the appropriate mitigation and/or prevention tactics for their situation and plan for future scenarios that could unfold given their operating environment. Using data from assessments and consultations, digital security experts can design targeted workshops that address actual risk and self-reported beneficiary priorities.

Examples:

New activities applicable at this scale are underlined.

1. *A digital security expert coordinates with necessary staff to recover lost files from a compromised device*
2. *A hands-on workshop where participants learn how to use tools such as password managers or two-factor authentication apps*
3. *An overview of common threats such as phishing attacks or malware, and teaching participants how to recognize and respond to them*
4. *Role-playing exercises where participants practice responding to simulated security incidents and learn how to escalate issues through the appropriate channels*
5. *Human resources-focused workshop to review staff onboarding processes to add basic digital security modules or practices*
6. *Mentorship opportunities, internally or externally, that expand staff understanding of day-to-day digital security practices*

Scope of Financial & Material Support

In addition to rapid response funding for material support (e.g., hardware, software, etc.), programs should budget for skilled digital security trainers to conduct activities with partner HROs throughout the program. While the short-term assessments are less technical, they are still best done by or in concert with a digital security professional—and should be budgeted for accordingly.

Monitoring & Evaluation

Short-term interventions can include any activities and associated data for emergency interventions.

	Activities	Outputs	Outcomes
Emergency Intervention	1. Provide rapid response grant for digital security materials 2. Access to digital security emergency response hotline 3. Conduct diagnostic consultation to raise awareness 4. Conduct low-lift tool use workshops	• Immediate digital security incident is addressed. • Targeted digital security resources and tools are available to staff. • HROs/HRDs are trained on specific digital security threats and on adopting specific mitigation tools.	• Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms.
Short-term intervention	5. Conduct targeted tool use and threat assessment workshops 6. Provide mentorship to address specific threats 7. Provide low-lift organizational policy tools, i.e., templates	• HROs/HRDs are broadly trained on basic digital security tools and practices. • HROs/HRDs are mentored on specific digital security threats.	• Staff have **increased knowledge** of actual digital security threats and mitigation and prevention tactics. • Staff **begin to adopt** digital security practices.

Indicators:

- *# emergency requests responded to*
- *#HROs/#HRDs trained*
- *Reflections from HROs*
- *Change in perceived digital risk (score may go down)*
- *Change in pre/post/ex-post scores for trainings*
- *Change in OCA score*
- *Digital security trainer reflections; trainee reflections*

For short-term interventions, the outcomes should be increased awareness and knowledge on a broad range of digital security concerns. Supplementing assessment inputs, MEL Specialists may use data from pre/post tests, as well as partner interviews and reporting, to monitor and evaluate the efficacy of digital security activities. Observation can also be a useful tool if the same digital security expert is engaged over the entire nine-to-twelve-month period. Various actions on the part of the organization, such as updating router passwords or implementing two-factor authentication on devices, can be verified by observation or quick tests.

Drawbacks

1. **Limited scope for customizable solutions.** A combination of a consultation/diagnostic and perceived risk assessment can offer some insight into a CSO's digital security ecosystem and hygiene, helping implementing partners to provide targeted training. These tools establish a preliminary risk baseline but do not incorporate robust monitoring tactics to track changes. Working on a short timeline and based on the available data, partners should work together to identify the intervention priorities.
2. **Minimal ability to assess changes in digital security.** The more accessible assessment options do not include comprehensive, ongoing checks of actual digital security capacity and risk. For example, reassessing perceived risk over time is less valuable because it cannot accurately measure change in digital security awareness, capacity, or threat reduction. The available indicators to monitor changes in digital security hygiene rely largely on activity-based indicators and qualitative methods. As a short-term program, minimizing the reporting burden is important to bear in mind, which shrinks the available evidence base.
3. **Lack of sustainable solutions.** Addressing immediate threats and increasing knowledge or awareness of staff does not necessarily lead to longer-term, systemic changes in the digital security infrastructure at an organization. Contexts and threat environments, as well as staff at an organization, can change quickly and an intervention that provides safety support for nine to twelve months does not mean that organizations are more digitally secure in the longer-term.

Long-term Interventions

(12 months or more)

Long-term Interventions

(9–12 months)

Typically aim to improve holistic digital safety and security practices that better equip partners to respond to increasingly advanced digital threats. These year-plus programs incorporate activities typical of a short-term intervention, beginning with a focus on immediate needs and general digital security know-how. With a longer timeline, these interventions are distinguished by depth over breadth, progressing to implement more sophisticated assessments, as well as context-specific, mitigating and preventive solutions to address complex digital security threats.

Assessments

For organizations seeking to improve their digital safety, there are two primary assessments that are recommended to diagnose vulnerabilities and develop a plan to mitigate threats: SAFETAG audits and Organizational Capacity Assessments. Both assessments are best suited to longer-term interventions due to the time required to conduct them and the resources required to implement any capacity and infrastructure improvements.

SAFETAG Audits

SAFETAG audits typically serve HROs by working with them to identify their digital risks and providing pragmatic next steps to address them. Trained SAFETAG auditors lead a risk modeling process that helps staff and leadership take an institutional look at their digital security infrastructure; expose software and/or hardware vulnerabilities that impact their critical processes and assets; and provide clear reporting and follow up to help the organization move strategically forward and identify the support they need to respond to or mitigate emergent threats. SAFETAG audits deploy a wide variety of methods to develop an audit report for an organization, including:

- organizational policy review,
- organizational device usage,
- user device assessment,
- vulnerability scanning and threat analysis (i.e., context monitoring), and
- responding to advanced threats, among others.

The final audit report also includes recommendations for the organization to consider when planning for the future. It is common for an audit report to form the basis for an organization's Risk Reduction Plan that clearly maps out the priority issues and how to address them to improve overall digital security.

Organizational Capacity Assessments

An Organizational Capacity Assessment (OCA) is a holistic and systematic approach that includes identifying digital security capacity gaps and developing a plan to address the gaps with a view of improving organizational safety. The OCA process is highly participatory and requires time and commitment from the recipient organization. It is designed to strengthen a partner organization's ownership of their digital security, while fostering a trusting and collaborative relationship between the OCA facilitator and the HRO being assessed. The following are examples of modules that are included in a digital security OCA:

- Technological capacity and equipment (assessment of hardware and software);
- technology support within the organization (dedicated staff with technology and digital security expertise);
- digital security planning and policies, including use of secure communications technology; and
- data security.

The assessment report is used to create an organizational development plan to address weaknesses and gaps, as well as establish a set of baseline data to use as a point of comparison for subsequent assessments.

Scope of Digital Safety Support

For long-term interventions, the support and purpose of training is similar to those of emergency and short-term interventions: 1) increasing awareness and/or knowledge; 2) tool-specific guidance; and 3) digital security mitigation and/or prevention strategies. These interventions are distinct, though, because there is greater opportunity to deepen their understanding of risk and increase their capacity for both preventative and responsive

digital security approaches. A key advantage of long-term interventions is that implementing partners/digital security experts have the chance to work with HROs over time as threats evolve. Guidance and support therefore evolve as HROs are forced to adapt over time.

Using assessment data, digital security experts can design targeted workshops that address these dynamic and difficult security challenges. Prioritizing contextually specific mitigation/prevention tactics helps partners respond to advanced threats, and over time, helps improve their digital security resilience and culture.

Examples:

New activities applicable at this scale are underlined.

1. *A digital security expert coordinates with necessary staff to recover lost files from a compromised device*
2. *A hands-on workshop where participants learn how to use tools such as password managers or two-factor authentication apps*
3. *An overview of common threats such as phishing attacks or malware, and teaching participants how to recognize and respond to them*
4. *Role-playing exercises where participants practice responding to simulated security incidents and learn how to escalate issues through the appropriate channels*
5. *Human resources-focused workshop to review staff onboarding processes to add basic digital security modules or practices*
6. *Mentorship opportunities, internally or externally, that expand staff understanding of day-to-day digital security practices*
7. *Workshops on becoming advocates for digital security within their organizations and communities—to pass on their knowledge and skills to others and promote a culture of digital security*
8. *Supporting HRO communities of practices and networks on digital security support*

Scope of Financial & Material Support

In addition to rapid response funding for material support (e.g., hardware, tools, etc.), programs should budget for skilled digital security trainers to conduct activities with partner HROs. Long-term interventions and the corresponding assessments are highly technical and require a skilled digital security professional. Also, SAFETAG audits and OCAs may reveal vulnerabilities with an organization's digital security infrastructure that might require big investments in servers and software to strengthen the organization's digital security. Financial support should be included specifically for Risk Reduction Plans so that organizations may receive the necessary support to make institutional changes that improve their security.

Monitoring & Evaluation

Long-term interventions can include any activities and associated data for emergency and short-term interventions.

	Activities	Outputs	Outcomes
Emergency Intervention	1. Provide rapid response grant for digital security materials 2. Access to digital security emergency response hotline 3. Conduct diagnostic consultation to raise awareness 4. Conduct low-lift tool use workshop	• Immediate digital security incident is addressed. • Targeted digital security resources and tools are available to staff. • HROs/HRDs are trained on specific digital security threats and on adopting specific mitigation tools.	• Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms.

	Activities	Outputs	Outcomes
Short-term Intervention	5. Conduct targeted tool use and threat assessment workshops 6. Provide mentorship to address specific threats 7. Provide low-lift organizational policy tools, i.e., templates	• HROs/HRDs are broadly trained on basic digital security tools and practices. • HROs/HRDs are mentored on specific digital security threats.	• Staff have **increased knowledge** of actual digital security threats and mitigation and prevention tactics. • Staff **begin to adopt** digital security practices.
Long-term Intervention	8. Provide repeat,updated trainings and workshops as needed 9. Draft organization-specific digital security policies and processes 10. Provide mentorship for building digital security organizational culture	• Targeted digital security policies and processes are created. • HROs/HRDs are mentored on how to sustain a digital security culture.	• Staff **implement** digital security policies/protocols. • Staff **adopt** digital security practices. • HROs have **increased capacity** in both preventative and responsive digital security approaches.

Indicators:

- *# emergency requests responded to*
- *#HROs/#HRDs trained*
- *Reflections from HROs*
- *Change in perceived digital risk (score may go down)*
- *Change in pre/post/ex-post scores for trainings*
- *Change in OCA score*
- *Digital security trainer reflections; trainee reflections*
- *Change in risk reduction plan and/or related policy*

For long-term interventions, the outcomes range from increased awareness and knowledge of broad digital security issues to implementing and sustaining adopted digital security approaches. Assessing long-term outcomes is multi-layered because adoption includes both the creation of needed digital security policies and processes, as well as its actual implementation; a policy that is fully adopted will be implemented across an organization with accountability mechanisms in place. The sum total of individual behavior change amounts to an organizational culture shift and increased digital security capacity. Monitoring and evaluation also becomes more advanced and nuanced, as implementing partners have the opportunity to observe changes in behavior among HROs that collaborate with digital security experts over time.

Drawbacks:

1. **Requires substantial investment.** SAFETAG audits and OCAs are best suited for projects that work with partner organizations for an extended period of time (ideally one year or longer) and offer substantial training, mentoring, grants, and other oversight to ensure that organizational development and changes take place. As a result, these methods can be expensive (in both time and money) and require specialized expertise from digital security professionals.
2. **Technical dependency can limit sustainability.** Long-term engagements by digital security professionals can lead to an unhealthy reliance on technical assistance. If organizations become accustomed to receiving continued support from outside professionals, the incentive to build that capacity within the organization is reduced and unsustainable.

Appendices

Appendix 1: Digital Security Resources

The digital security framework does not provide guidance on specific digital security tools or practices because the authors are not subject matter experts. There are also many such resources already available, including the following:

Front Line Defenders provides digital protection support to human rights defenders and maintains a list of Digital Protection Resources.

SaferJourno is a toolkit published by Internews that focuses on digital security resources for media trainers.

Security in-a-box offers digital security tools and tactics to address common concerns like device protection or secure internet connection.

Totem Project is an online platform that helps journalists and activists use digital security and privacy tools and tactics more effectively in their work.

Appendix 2: Digital Security Guidelines for Independent Media Partners (2022)

Under the USAID-funded Balkans Media Assistance Program (BMAP), Internews digital security experts developed the following guide to support independent media. Notably, these guidelines identify no- and low-cost digital security interventions. While untested with other types of organizations, this tool could likely be adapted to support an array of partners.

The Digital Security Guidelines were developed in 2022 and should be periodically reassessed by experts to match the current threat landscape. As a technical tool used to respond to dynamic threats, these guidelines should also be used by an organization with support from a digital security expert.

Introduction

These Digital Security Guidelines identify the recommendations and procedures for all individuals accessing and using an organization's IT assets and resources. The objectives of IT security guidelines are the preservation of confidentiality, integrity, and availability of systems and information used by an organization's members. The Digital Security Guidelines are a living document that needs to be continually reviewed and updated to adapt with evolving business and IT requirements.

This document consists of recommendations from the scope of digital security for independent media outlets. Since there is no general digital security rule that can be applied to every media outlet, this document tends to give preventative tactics and practices for the media outlets to customize according to their preferences, their assets, capacity, and awareness of the risks, as well as list all the important actors that influences the overall digital security within the outlet. These guidelines are built as a result of work in the field of digital security under BMAP project.

The document is divided into three general scopes of digital security - website, office and staff; digital security guidelines are approached in that manner, but also divided into seven subsections. This document has different presumptions about providing the hardware needs to organization's employees, maintenance and replacement of those needs, as well as software provision. Since there are a number of different approaches to digital security dependent on this set up, it's important to choose the right settings accordingly.

To get the sense of the overall security status in a particular media outlet follow the tables item by item and leave checks for the items that are true to the outlet in focus. Since different outlets have different assets of various priorities, any policy based on these guidelines should be set up accordingly and possibly after a thorough SAFETAG audit of the outlet.

Filled by:

Name:_____ Position:_____

Media outlet: _____

Items marked blue take no or low cost to implement within the outlet.

1. Website Infrastructure and Applications

1.1 Infrastructure

1.1.1 Domain management and access

Check	Recommendation
	The domain is registered to a company and not an individual
	Trusted individual(s) have access to the domain(s) management
	Access to the domain management is controlled via a password manager workflow
	Two factor Authentication required to access domain control panel
	Domains are registered for two years longer than the end of the project funding

1.1.2 Server/Hosting

Check	Recommendation
	Website backup is kept on a separate physical machine and a separate network
	Mail server is not kept on the same machine as web server
	Verified email services are used
	Failover Internet connection is provided
	Hosting is not shared among other websites; VPS is being used.

1.1.3 Website Network Protection and DDoS shields

Check	Recommendation
	Deflect or Cloudflare is connected as soon as the domain registered
	Website caching on the shield and on Wordpress/Joomla/Custom is on
	SSL/TLS encryption is enabled
	IP is changed after setting up the Cloudflare
	Shield security level set accordingly
	Shield pro plan is used (at least)
	WAF is used

1.1.4 Secure webserver and endpoint settings

Check	Recommendation
	Endpoint forwarding and testing
	File and path protection

1.2 CMS setup and access

1.2.1 Paid services, themes, plugins and modules

Check	Recommendation
	Only licensed software is used
	No inactive plugins exist
	Component monitoring software/plugins are being used

1.2.2 Website Backups and Failsafe

Check	Recommendation
	Website code, database and data is backed up on a regular basis
	More that one separate backup destinations is used

1.2.4 Website Maintenance

Check	Recommendation
	Auto-updates are enabled
	Website load and vulnerability tests are done on a regular basis
	Platform updated on a regular basis
	IP is changed after setting up the Cloudflare
	Website load and vulnerability tests are done on a regular basis

1.2.5 Dashboard Access and Permissions

Check	Recommendation
	No accounts called admin, administrator, user or root
	Separate accounts are created for everyone that access the website
	All unnecessary admin rights are removed
	2FA is used wherever possible

2 Office/LAN

2.1 Data

Check	Recommendation
	Important data is encrypted
	Cloud-based encryption is used (i.e. Boxcryptor, cryptomator etc.)
	Important data is masked when shared in a communication

	Important data is sanitized when no longer needed
	Resiliency of important data is achieved
	Important information such as video materials, financial and legal documents have two backups, in addition to the original documents
	Automatic backup software is installed on users' computers
	A storage server at the office is used
	Backup of the storage servers is done on a regular basis to a hard drive/other storage outside of the office
	A BitLocker or similar software is used as disk encryption
	Admin user is locked
	Limited users are created for the staff

2.2 Network

Check	Recommendation
	Firewall is configured and running
	Firewall creates connections instead of an ISP modem
	Internet failover is configured
	Network Topology is documented and regularly updated
	IDS/IPS is configured and running
	NAT (Network Address Translations) and ACL (Access Control Lists) are configured
	No default logins exist on network devices
	Routers are set on a separate network range (VLANs).
	Remote access is enabled on the routers
	MAC filtering is set on the network
	Guest Wi-Fi is used, and password is changed regularly
	Wi-Fi is protected using contemporary protocols
	Departments use separate networks
	NAS server exists on the network
	Access to NAS/other local file servers is set and restricted
	Configuration backup of the firewall, router, NAS is done regularly
	UPS is set on network equipment
	Online configuration backup is available and secured

	Offline configuration backup is available and secured
	Portal/MDM (Mobile Devices Management) is configured
	Servers (All backed up, easily retrieved, ownership within the organization)
	• Sensitive data stored offsite; website securely hosted
	• Access - from within the organization
	• Ownership – different access to different platforms and servers
	Wired connections are used when/where possible
	Strong WIFI password for staff are used and changed regularly

2.3 Staff capacity

Check	Recommendation
	Staff get basic security trainings on a regular basis
	Security polic(ies) is being followed and applied by staff
	Recovery emails are used with security options on
	Admins use hardware security keys
	Biometric authentication
	Metrics on security practices are being measured: number of people trained, (successful) attacks experienced, 2FA accounts used, strong password used etc.

2.4 End devices

Check	Recommendation
	Updated and active antivirus on each computer (or centralized solution) is used
	Strong passwords are used
	Antimalware is used
	Secure browsing is enabled
	VPN is used
	TOR or similar browser is used
	Regularly updated, licensed OS is used, support on
	Updated, licensed software from verified published is used
	Work computers/phones used for work only, otherwise: • work software installed on devices and security procedures followed; • virtualization used and security procedures followed
	Tools for device security management are used (Google Endpoint Management, Apple MDM, Flock etc.)

3. Account security

Check	Recommendation
	2FA/MFA is used
	Strong passwords are used
	Trusted payment platforms are used where/when transactions are performed
	Password managers are used (Bitwarden etc.)
	Authenticator app is used
	Backup admin for used management is used
	Security features are enabled on social media too
	Updated, licensed software from verified published is used
	Privacy on social media adjusted

4 Accessibility

Check	Recommendation
	Electricity – full resilience to outages, no power issues
	Internet – no interruptions, comfortable bandwidth
	Service expiry/subscriptions - ideally: mapping of existing services and subscriptions and Preventative planification and budgeting for high sustainability is done

5 Communication security

Check	Recommendation
	Cloud services and collaboration tools capacity (Slack, Github, Google Docs, Mattermost) are used
	The organization has its own infrastructure where all the interactions are happening including emails
	A clear policy on how staff is interacting with each-other and with external parties and it is applied to high standards
	End to End Email Encryption is used
	Signal or similar for encrypted calls is used. Security options are enabled.
	Self destructing messages are used etc.
	Applications recommended: Jitsi, Signal.
	If using Whatsapp – security features are enabled

6 Other

Check	Recommendation
	Clean desk policy exists
	Lockable storage exists in the office
	Visitor protocols exist (guest Wi-Fi, pre-visit announcements)
	Policy of shutting down the computer before leaving exists
	Alarm system exists and is being used

7 Policies

Media outlets can review their policies; please note if some of the policies already exist:

1. Onboarding Policies
   - Information about staff, role, different level of access
   - List of accounts to be created
   - Devices to be delivered, software to be installed
   - Train the staff on how to use tools, and how to enable security measures
   - Setup security measures on accounts
2. Offboarding Policies
   - Map out accounts to be suspended, deleted, transitioned
   - Get devices, get the data
3. Travel Policies
   - Write a set of recommendations depending on the missions and the risk involved
4. Contingency Planning Policies
   - It is important to understand the risk environment in a specific country, update them regularly and be able to take necessary measures with the risk increase or decrease.
     i. Categorize level of threat (for example: Green to Red)
     ii. Map out possible risks (scenarios) in each threat level
     iii. What could be prepared in advance for each scenario?
     iv. What do we do if the scenario happens?

For these security guidelines to be successfully and fully implemented by a particular media outlet a risk assessment inside the outlet needs to be performed. The security of the assets directly depends on the level of the risk those assets are within the company.

This document serves as a general model of recommendations of security practices to be implemented in a media outlet and should not be taken as proof of outlet's overall security status.

Appendix 3: Perceived Digital Risk Self-Assessment (Sample)

This sample document is intended to be an online questionnaire and can be distributed at the beginning and end of a program.

1. Consider each of the following statements. Please indicate to what extent you agree with each statement.

   [Strongly disagree – Disagree – Neither agree nor disagree – Agree – Strongly Agree]

   - I believe that digital threats pose a risk to my organization.
   - I understand the different digital security threats that my organization faces.
   - I understand how to mitigate the digital security threats that my organization faces.
   - My organization has enforceable policies and practices to promote digital security.

2. From your perspective, what digital security threat poses the greatest risk to your organization? What digital security threat concerns you the most?

2A. Keeping in mind the greatest digital security threat to your organization, consider the following statements and select true or false, as appropriate.

   [True – False – I don't know]

   - At my organization, we know how to protect ourselves from our greatest digital security threat.
   - My organization has preventative measures already in place to protect ourselves from our greatest digital threat.

     If false, branch: Consider the following statement and select true or false, as appropriate.

     [True – False – I don't know]

     My organization has the capacity to implement the necessary preventative measures to protect ourselves from our greatest digital threat.

     - **If false, branch:** What support does your organization need to implement the necessary preventative measures?

     If true, branch: Consider the following statement and select true or false, as appropriate.

     [True – False – I don't know]

     Staff at my organization consistently follow the preventative measures in place.

     - **If false, branch:** What support does your organization and/or staff need to adopt the necessary preventative measures?

3. Consider each of the following digital security threats. For each threat, please indicate the extent of risk that you think that your organization faces.

   [Very low risk – Low risk – Moderate risk – High risk – Very high risk – I don't know]

- **Device seizures** *Organization electronic equipment is captured by a bad actor, thus compromising program data and contacts*
- **Doxxing** *Targeted attacks on individual staff members, in which their private content or identifying information is published online without their consent*
- **Malware** *Refers to malicious software viruses, e.g., ransomware, trojans, adware, keylogger, etc., that disrupt the organization's digital network and compromise organizational data*
- **Social engineering attacks** *Baited attacks in which the user is tricked into providing or exposing sensitive personal, programmatic, or organizational information to a bad actor; such attacks most commonly occur via email (phishing), but also via text, phone, and impersonation*
- **Surveillance** *Covert or overt surveillance of an organization's data, including social media accounts, with the intent to track, steal, damage, or disrupt the organization's digital network and information*
- **Website and server database attacks** *Targeted attacks to undermine or damage an organization's website or server database; commonly including Cross-Site Scripting (XXS), Structured Query Language (SQL), or Distributed Denial-of-Service (DDoS) attacks*

3A. Are there other specific digital security threats or types of attacks that are common for your organization? Please list them here.

Appendix 4: Methods and Sources

The intervention types and relevant outcomes were identified from a desk review of Human Rights Support Mechanism (HRSM) programming; a questionnaire distributed to HRSM implementing partners; and interviews and focus groups with participating HRO members and digital security professionals.

The intervention types, relevant outcomes, and MEL framework were developed inductively from observations gathered across all sources of data (case studies, learning events, interviews, focus groups, and implementers survey). Therefore, the framework described within this document was not *tested* through HRSM programming, but instead *developed* through HRSM programming. As a next step, the authors intend to refine the framework by deductively testing implications in future projects, and they encourage other users of the framework to do the same.

Cases Considered

The authors looked at all instances of digital security support offered through the Human Rights Support Mechanism, a seven-year Leader with Associate Award mechanism funded by USAID to protect and promote universally recognized human rights. At the time of writing, HRSM consisted of thirty-eight associate awards, which range in length from two to five years, and fifty-five rapid response grants, which are generally smaller in size and respond to an action-forcing event. HRSM programs cover all continents, representing a variety of operational contexts.

After analyzing all reporting from these awards, the authors identified nineteen programs where digital security support was mentioned as an activity. After a desk review of these projects, the authors identified four case studies to conduct follow-up interviews and other data collection events. The cases were selected to represent a variety of operating contexts and intervention timelines. The authors also considered the centrality of digital security support to programmatic activities and the level of interest from program staff. Programs that had already closed by the time the report was being produced were excluded from follow-up data collection due to feasibility issues.

For three of the case studies, the authors interviewed program staff and conducted a desk review of programmatic materials. For one of the case studies, the authors conducted a three-day, in-person learning event to learn directly from project stakeholders about how and why digital security support was helpful to their work.

In addition to the case studies and learning event, the authors conducted focus groups with digital security professionals, and they distributed a survey to HRSM implementing partners (Freedom House and Internews) to identify pain points in implementing digital security support programs.

Sources

Authors utilized the following sources:

- Document review of program reports and budgets from the selected HRSM case studies
- Interviews with program teams implementing the selected HRSM case study projects

- Digital Security Programming survey of staff at implementing organizations (Freedom House and Internews)
- Focus group with digital security experts
- Learning Event on digital security practices with journalists and digital security experts in a difficult operating environment
- Reviews and comments on the Digital Security Framework by digital security experts and implementers

Limitations

The framework has not been tested independently, so therefore it should be considered a launchpad for generating program design that should be reflected on and tested. All recommendations are based on observations and reflections by stakeholders in the digital security space; recommendations should be considered anecdotal because they have not been rigorously tested. The framework is also based on the experience of implementing organizations within the PROGRESS consortium, and not representative of all implementing organizations in the human rights field.

Funding and Conflicts of Interest

This project was funded by USAID through the Human Rights Support Mechanism under Objective 4: Identification of effective approaches for protecting human rights. The authors work on monitoring and evaluation teams at Internews and Freedom House, two members of the PROGRESS consortium that operates the Human Rights Support Mechanism. Freedom House is the prime recipient of the mechanism, and case studies were implemented by Pact, Internews, and Freedom House.

Feedback

For more information or feedback about this product, please reach out to info@freedomhouse.org.

Appendix 5: BMAP Forward Learning Event Key Takeaways

Under the purview of the Human Rights Support Mechanism, Freedom House and Internews organized a learning event on digital security with the Balkans Media Assistance Program Forward (BMAPF) in Podgorica, Montenegro from December 6–8, 2022. The two-day program was an interactive, mutual learning opportunity for funders (HRSM, Internews Balkans) and grantees (BMAPF media partners) to increase their understanding of digital security. The event addressed the following questions and objectives:

Learning Questions
1. How can we encourage people to be both aware of and proactively respond to the digital security risks that they face? Is awareness enough to promote proactive digital security mitigation and/or prevention?
2. What barriers exist to lowering digital risks? How can we break down those barriers?
Learning Objectives
1. Reflect on the efficacy of existing digital security assessment tools and interventions, based on partner experience
2. Promote recommended standards for digital security, with the intention of cocreating shared understanding of these standards
3. Recognize that digital security is an ongoing process, requiring vigilance and recurring assessments of and updates to procedures/policies to mitigate digital threats (organizationally and personally)

Based on data gathered at the learning event, there emerged four clear trends—ideas or beliefs reiterated across sessions and participants—across both learning question areas. The four clear trends are outlined first, followed by additional takeaways related to each learning question.

Partners articulated that they:

- Need ongoing awareness raising about digital security
- Generally lack high-quality IT support
- Believe digital security attacks are inevitable
- Prioritize their core function (reporting the news) over digital security

1. Ongoing awareness raising

Across all four focus groups and in additional sessions and all-group discussions, participants repeatedly emphasized uneven awareness of and knowledge about digital security risks among media outlet staff, e.g., journalists, editors, managers, and IT specialists. Participants called for ongoing digital security awareness training, recognizing both the existing awareness/knowledge gap and the ever-evolving nature of digital security threats. Current training typically targets management and/or IT specialists,

which remains a critical approach since manager buy-in was identified as an important enabler for adopting digital security practices. Participants also highlighted, though, that journalists need rigorous awareness training, as they have not historically benefited from training and they were represented as not taking digital security seriously.

2. Lack of high-quality IT support

Across all four focus groups and in additional sessions and all-group discussions, participants noted a general lack of high-quality IT support; however, focus group data show that managers and IT specialists offered nuanced views on the scope of IT support. True to their expertise, IT specialists focused on the need for software or hardware interventions, noting specific problems that their media outlets faced. In comparison, managers tended to speak to a lack of capacity or expertise: in-house IT staff do not have the capacity to manage all of an outlet's IT challenges and digital security threats; outlets do not pay enough to consistently attract top IT talent; smaller outlets rarely can afford in-house IT expertise at all; outsourced digital security consultants remain expensive with varying quality; and neither in-house nor external IT support are 24/7. IT specialists also affirmed these points during the course of the learning event.

Participants repeatedly mentioned the idea of a "flying team," with one digital security expert serving multiple outlets in the region. In at least one focus group, participants mentioned that journalists are concerned about privacy with IT specialists, so building trust over time is important.

3. Digital security attacks are inevitable

Participants in every focus group shared that their media outlet had suffered a digital security attack, if not multiple attacks. In after action reviews, HRSM and Internews Balkans staff emphasized the sense of hopelessness they heard from partners—outlets cannot keep pace with evolving digital security threats, and even the best prevention and/or mitigation interventions are not a full-proof defense. Notably, a closer look at focus group data indicates that only managers expressed that digital security breaches were an inevitability.

4. Prioritize their core function

Managers also clearly articulated their media outlets' priorities: report the news first, tackle digital security later. Fulfilling their core function to deliver the news drives both high-level decision making and on-the-ground reporting, which often undermines digital security interventions. During the partner panel session, an IT specialist acknowledged this tension, saying, "Sometimes we have to loosen digital security practices in order to get the job done.... There is a need to balance minimum security with freedom and space to work."

Learning Question 1: How can we encourage people to be both aware of and proactively respond to the digital security risks that they face? Is awareness enough to promote proactive digital security mitigation and/or prevention?

Risk Perceptions

Most organizations believe that experiencing attacks heightens perception of risks. In the aftermath of major attacks on an organization, staff are more willing to comply with digital security efforts, but that renewed interest in digital security can be short-lived. While many of the individuals in attendance had experienced an attack, one of the facilitators commented that "[o]rganizations that haven't gone through attacks by now talk about threats and risks as if they are happening to someone somewhere far away and not going to happen to them."

Participants highlighted untrained or unmotivated staff as one of the greatest sources of risk that their organization faces

because organizations are only as safe as their weakest adherent to digital security protocols. In light of this "human factor," staff believe that more training and support is warranted, but some participants believe that training alone is not enough to encourage digital security vigilance. Staff mentioned that "consulting" or having an external force hold them accountable would help.

Executive-level participants largely believed that risks are unavoidable. One participant commented, "We are very often made to believe that whatever we do will not be good enough because someone who wants to do harm will find a way....The ministry of defense reacted to an article that we hadn't even published. The Ministry of Defense has 10X better tools than we could ever have." Because risks are unavoidable, some executives suggested minimizing the impact of an attack, rather than its likelihood, by making frequent website backups.

Both executive and IT specialists agreed that digital security practices should not stand in the way of journalists producing content, but media executives emphasized the importance of combating risks that would prevent the outlet from functioning. When listing digital security "nightmare" scenarios, both IT specialists and executives listed personal online safety, social media hacking, DDOS attacks, Data Archive Vulnerability and "the Human Factor" as their greatest fears, all of which affect the ability of a newsroom to function and the safety of their colleagues. Media executives placed a high value on keeping journalists safe. One mentioned that "Digital security is not only about data—if your data is taken then you face physical risks or other risks. Also when your data is not secure you endanger other people besides yourself, you also endanger your colleagues." Others justified digital security practices because they helped prevent attacks that cause major newsroom disruptions, like access to emails or websites. While many executives claimed they were too busy to prioritize digital security, reframing digital security as vital to the smooth functioning of a newsroom may make digital security incentive compatible with content production.

Assessments

Digital security assessments are useful because they help organizations identify and evaluate potential security risks and vulnerabilities in their systems, networks, and infrastructure. By conducting regular assessments, organizations can proactively identify areas that need improvement and implement measures to mitigate those risks. Among the participants that received the SAFETAG audit, there was consensus that the audit helped them realistically assess their risk. They particularly appreciated that the audit was accompanied by recommendations, and the ability to apply for risk reduction grants from the BMAPF team. SAFETAG audit recommendations are often very expensive, including servers, cameras, licensed products, separate internet lines, etc. Participants agreed that it would be helpful to have the consultant who conducts the SAFETAG audit work with them to oversee the implementation of the more advanced recommendations.

Participants similarly agreed that the Organizational Capacity Assessment (OCA) was helpful for understanding challenges and gaps in digital security, but thought that the OCA should accompany resources and templates for crafting solutions rather than just highlighting deficiencies. Participants also mentioned that the OCA toolkit focused on internal policies and practices, but because they host content and backups on external sites like WordPress they lacked the ability to evaluate those external third-party sites' security practices. Participants also agreed that the OCA assessment tool's language was often vague (i.e. what does "regularly" actually mean?).

Learning Question 2: What barriers exist to lowering digital risks? How can we break down those barriers?

Both managers and executives stated that costs are a barrier to implementing many digital security practices. Although low and no-cost digital security solutions were acknowledged as useful, participants mentioned high costs related to training, hiring a technology specialist to help maintain strong systems internally, procuring necessary equipment, and software subscriptions that require ongoing investments on a regular basis. Media outlets prioritize content production, and it is difficult to find resources to invest in these types of solutions to lower digital risks. Also, some digital security solutions cost time to implement and can interfere with the pace at which newsrooms work. For example, outlets with high daily output have a harder time being vigilant

and consistently applying solutions that are low cost financially, but high cost or impractical in implementation, such as using two-factor authentication to log into an account as many as 30 times a day during content production.

Similarly, manager buy-in was listed by all participants as a barrier as well as an enabler of implementing digital security practices at outlets. Managers determine budgets, including investments in digital security, which can lead to either a high or low financial and operational commitment to digital security. For example, if a technology expert provides recommendations to an outlet and introduces digital security practices and/or policies, management must be receptive and demonstrate a commitment to the advice provided by both investing in solutions for risk reduction and enforcing new policies. As a result, managers can be either a barrier or an enabler to lowering digital risk depending on the degree to which they prioritize digital hygiene and create a culture of digital security awareness at an outlet. Similarly, participants mentioned that a barrier to adopting digital security practices at outlets is the lack of onboarding processes that would allow managers to set the tone for how digital security should be incorporated into daily operations.

Other barriers to lowering digital risks at outlets that were mentioned in focus group discussions include lack of awareness of risks among both outlet managers and journalists and lack of trustworthy, knowledgeable trainers that can prepare media professionals to mitigate threats; difficulty in consistently implementing policies once they are introduced because they might interrupt daily operations or there is no way to enforce the policies; and the speed with which threats shift and advance leave people feeling like there is no way for trainings and financial investments in security to keep pace with changing risks.

Practices

When discussing the no and low cost solutions developed by Internews' Marija Herceg, participants agreed that most practices were both easy to implement and high impact; however, the technical knowledge required was a barrier to some participants. The low and no-cost practices tool itself requires "tech translation" for non-technical experts to increase take up. Executive staff were significantly more likely to indicate that they did not know enough about the practice to rate it on ease and impact.

Both managers and executives agreed that encrypting data is the most important practice their organizations can use to increase digital security. When participants placed the practices on a matrix of ease of implementation compared with degree of impact, a handful of practices were deemed both difficult to implement and low impact, meaning that participants perceived that they are likely not worth the effort for media outlets. Eighteen percent of participants indicated that using TOR or other similar browsers was both low impact and difficult to implement, with agreement between executive and IT participants. Similarly, eighteen percent of participants felt the same about implementing a clean desk policy; however, while both media executives and IT participants both agreed it was difficult to implement, IT participants were more likely to view this as low impact. Perceptions that practices are easy and high impact can enable greater adoption.

Policies

Many of the outlets present lacked clear and formalized digital security procedures or policies. Without written policies, participants lacked easy means of communicating digital security practices to new staff, who they believed present a greater digital security threat than long-term staff. Digital security policies are important for training staff because they provide a clear set of guidelines and expectations for how employees should handle sensitive information and interact with company systems. Some participants noted that they tend to have poor long-term implementation of digital security policies due to vigilance fatigue.

Standard policies alone, however, are not enough to improve security. Participants emphasized that policies should be crafted through consultations with digital security trainers that can both recommend customized solutions for their organization and keep them accountable to these solutions over time. By providing customized support, employees are better equipped to identify and prevent security threats. Additionally, employees are more likely to follow best practices and adhere to security protocols if they understand the reasoning behind them and if the practices fit with their existing routines.

When asked how they hold staff accountable for digital security practices, media executives in one focus group noted that executives have little ability to threaten negative consequences if policies are not followed because they rely on journalists to produce content. One executive described that the most serious consequence he could implement would be taking a staff member who had poor digital security hygiene out for drinks to encourage him or her to comply with security protocols. Instead, participants emphasized the need for digital security practices that fit with journalists existing practices. Positive incentives rather than negative incentives may be a more effective management tactic to encourage accountability.

Because policies themselves do not equate to behavior change, policies should build in opportunities to hear back from journalists about how the policies fit within their work flow. Creating feedback structures between management, digital security experts, and staff can promote policy adaptation that will ultimately increase adherence.

Finally, creating a community of norms around digitally secure journalism may be an important way to generate buy-in among staff. Because journalists across the sector have significant autonomy in their work, and many are freelance, raising the bar for security may be better set at the sector level than with individual outlets. One option is to target training and standards-setting practices at umbrella organizations for media like regional or local press clubs.

Freedom House

Freedom House is a nonprofit, nonpartisan organization that works to create a world where all are free. We inform the world about threats to freedom, mobilize global action, and support democracy's defenders.

1850 M Street NW, 11th Floor
Washington, DC 20036

freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouse
info@freedomhouse.org
202.296.5101

Internews
Local voices. Global change.

Internews is an international media support nonprofit that believes everyone deserves trustworthy news and information to make informed decisions about their lives and hold power to account. We train journalists and digital rights activists, tackle disinformation, and offer business expertise to help media outlets become financially sustainable. We do all this in partnership with local communities — who are the people best placed to know what works.

2000 M Street NW, Suite 850
Washington, DC 20036

www.internews.org
facebook.com/internews
@internews
202.833.5740