Measures for Mitigating Cyber-Security Risks

Rory Byrne

As this publication has explored, the current cyber-security environment – where even massively resourced and staffed organisations continue to be the subject of significant cyber-security breaches – poses an uphill challenge to NGOs with limited time, knowledge and resources. There is no one-size-fits-all strategy for hardening an organisation against hostile digital intelligence gathering, particularly since increased security often means decreased convenience. However, establishing a strong baseline and understanding when and how to introduce increased security measures has generally proven to be most effective. Humanitarian agencies also have the advantage of being able to learn mitigation lessons from the human rights world.

The tools and methodologies for information gathering by governments and hostile actors are openly acknowledged and increasingly directed against NGOs. As the experiences covered in this paper indicate, humanitarian organisations are not immune (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16). However, lessons can and should be drawn from other sectors who have already begun to address the issues of hardening their people and systems against the deleterious effects of unrestrained intelligence gathering. While the detailed discussion of such measures is beyond the scope of this paper, there are some basic strategic actions open to NGOs to help understand, identify and manage the risks.

Understand, model and constantly analyse

Humanitarian organisations are increasingly sophisticated in their analysis of physical security, and are gradually improving coordination efforts and information sharing through structures such as EISF and INSO. However, aid agencies should not forget that they must also understand and apply the same logic to digital threats (see Gilman, pp. 8-11).

Understanding the true nature of digital risks is vital to long-term viability. Organisations should map, audit and constantly update critical information they are mandated to preserve and protect. NGOs also need to understand the lengths and measures hostile actors operating in countries in which they have a presence are prepared to take in order to get access to sensitive information and core competencies (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).

Similarly, an internal review should also focus on information that leaves an organisation exposed, such as external emails, financial transactions or travel reservations – such information can be an invaluable source of insight into the comings and goings of an organisation and its people. Because outsiders must be relied upon to ensure the security of the entire organisation, this type of vulnerability represents another layer of risk that has to be accounted for.

Decisions should be driven by realistic risk modelling. For example, following the Snowden revelations, media scrutiny has focused our attention on the highest levels of intelligence gathering, while ignoring or glossing over some of the most common causes of data breaches – for instance, weak passwords, loss of laptops and social engineering. Similarly, many myths exist which hinder protection measures, such as those pertaining to the security of Skype, Blackberry and satellite phones – which depending on your threat model and potential adversary might be considered either highly insecure (versus a government level threat) or highly secure (versus a disorganised local militia).

Information security structures

Digital security is part of, but not the same as, information security. Information security is the wider context of how, why and when information is collected, shared and stored – both digitally and physically. The most sensitive information identified in a previous section should be tightly compartmentalised on a 'need to know basis', with the minimal access that is needed for the purposes of completing work.

Governments and other actors have exploited weaknesses in intelligence handling in a number of ways (see Byrne, a. pp. 12-16). For example, physical access to offices makes placing trojans much easier than remotely hacking into a machine, and failure to securely store or shred sensitive physical data and electronic media often bypasses any checks and balances put in place by the use of sophisticated encryption.

In comparison to human rights groups, humanitarian aid agencies generally have much better physical security management training, implementation and accountability structures. However, these need to be extended to deal with digital security (see Gilman, pp. 8-11). Information security breaches can create long-term damage to an organisation and its staff, and should be treated with the same due diligence as physical security breaches – with appropriate sanctions in place to ensure compliance as necessary. IT departments also need to be properly resourced with the capabilities and capacities to deal with the current threat environment. When outside contractors or suppliers are used for IT systems, they should be thoroughly vetted. Ideally 'red-teaming' or penetration testing of such systems should be conducted in order to identify potential weaknesses.

Select the right tools

Ensuring correct tool selection continues to be one of the most important parts of the success or failure in mitigating the impact of hostile digital intelligence gathering by governments and other actors. Investment in tools that reduce the ability of users to make mistakes (for example, encrypting all hardware automatically before distribution to staff) has proven to be one of the most effective measures for mitigating risk. Understanding the trade-offs between security, usability, functionality and cost are vital. This is particularly important, as many human rights and humanitarian agencies without the requisite skills or expertise in this area have often turned to expensive and off-the-shelf commercial solutions, which often do not meet the actual needs of the organisation (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).[118]

Similarly the choice of certain communications technology can also make an organisation a target. VPN connections, for example, are heavily restricted in certain countries and monitored. The Great Firewall of China has been documented to show signs of machine learning to pick up and block foreign VPN traffic and pinpoint where it is coming from.[119] The Tor network,[120] which anonymises and encrypts its traffic to protect user privacy, faces similar challenges. Russia recently came out as publicly targeting the service, offering a $110,000 bounty to crack the network, and recent leaks from other governments show similar efforts. Organisations should bear in mind where they are operating when making a technology choice, as choosing particular systems can make them the target of digital attacks or intrusions into their systems (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).

However, this process has become easier in the past few years with the emergence of the Liberation Technology (LibTech) movement.[121] Comprised of a number of technologists, NGOs and donors, it has contributed a significant number of free and open source tools and methods designed specifically with the humanitarian or human rights worker in mind. Organically developed training and management frameworks, based on years of experience in the field, are now available from a number of LibTech organisations.[122] New innovations have allowed humanitarian agencies to bypass some of the growing pains associated with other, less vulnerable, sectors.

Training

Training remains one of the best methods for mitigating the ability of hostile governments and other actors to abuse digital intelligence. A strong foundation must exist within an organisation as the weakest link can often compromise an organisation's entire network. Particularly in places with lower levels of digital literacy, experience shows that training tends to be hit-and-miss, not fit for the purpose, outdated, at too high/low level for the job description, or it does not represent a good fit for the current range of information systems and processes already in place.

118 A good example is the choice of using encryption. Although it is tempting to use it as a blanket across an organisation, if the intention is to use it in places that require licences, like China, Burma, Iran, or Israel, bringing encrypted devices across borders could draw unwanted attention and potentially cause legal issues. Also, even if a licence is not required, the use of encryption can affect relationships with governments, who may see that organisations that claim to be in the country to help, have something to hide. For further information see: Koops, B.-J. (2013). Crypto Law Survey. Available from: http://www.cryptolaw.org. [Accessed 2 Sept. 2014]. JISC Legal Information. (2013). What's the legal position of transporting encrypted equipment abroad? 13 May. Available from: http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2947/Whats-the-legal-position-of-transporting-encrypted-equipment-abroad-13-May-2013.aspx. [Accessed 2 Sept. 2014].

119 Arthur, C. (2012). China tightens 'Great Firewall' internet control with new technology. *The Guardian*. 14 Dec. Available from: http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control. [Accessed 2 Sept. 2014].

120 See https://www.torproject.org. [Accessed 2 Sept. 2014].

121 For more information, see Stanford University Center on Democracy, Development, and the Rule of Law. Program on Liberation Technology. http://cddrl.fsi.stanford.edu/libtech. [Accessed 2 Sept. 2014].

122 For example, Tactical Technology Collective and Front Line Defenders. Security in a Box. https://securityinabox.org. [Accessed 2 Sept. 2014].

For example, participants at HQ might be trained in how to use encrypted email software, while their field offices are not; the implication is that security is weakened and hostile elements, if given the chance, will exploit obvious weak spots.

Implementation continues to be a recurring problem for mitigation strategies. With digital training and tools the pace of change is extremely rapid, and the rate at which skills fade, become obsolete, or are forgotten is extremely high. Following up with additional training, online learning, auditing and other methods of reinforcement is necessary to guarantee that proper protocols are being adhered to (see Kaiser and Fielding, pp. 37-41). New employees should be given information security training as part of any induction process. When this is not possible, information access should be limited to only those functions that are necessary to conduct their job.

While training staff in specifics of security is a vital part of the process of mitigating cyber-security risks, it important to involve staff in the non-technical aspects of security – for example not opening email from unknown senders, not responding to phishing emails, not answering social engineering enquiries, not sharing company information with others, or taking care talking about company business outside the company – to explain how protecting an organisation's information and assets is not solely the job of the security professional. Raising awareness in all aspects will be an important part of protecting the organisation.

Prepare for failure

With so much information stored digitally, from mobile phones to servers housed at HQ, it is inevitable that failures will occur. As with any security mitigation effort, preparing for failure is the *sine qua non* of best practices.

Building in resilience, with regular secure offsite backups, is crucial for minimising any damage caused by accident or disruption operations launched by hostile governments and actors – such as the seizure, theft or destruction of computer equipment. In some environments, the additional benefit of doing this outside the country of operation (in countries such as the Netherlands, Finland and Iceland with strong NGO protection laws) is strongly recommended.[123]

Last, but not least, digital security breaches and adverse reputational issues should be integrated into business continuity planning and crisis management practices and procedures. For example, simulations should occur of dealing with potential risks such as a finding a hostile network penetration, critical system failure or dealing with a large leak of sensitive data.

123 When selecting information security tools, another thing that should be noted is local regulation and compliance in regard to information security. Data protection laws are the obvious example. European data protection regulations restrict the transfer of any personal data outside the EU and failure to take that into account can lead to significant fines. Organisations should think about what data they are holding and the implications when moving it between countries. Organisations using cloud services should also carry out a strong audit of where that data is hosted.

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 66 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Editors

Raquel Vazquez Llorente and Imogen Wall.

The editors welcome comments and further submissions for future publications or the web-based project. If you are interested in contributing, please email eisf-research@eisf.eu. Imogen Wall can be contacted at imogenwall@hotmail.com.

Acknowledgments

The editors would like to thank Lisa Reilly, EISF Coordinator, for her input and advice, and especially for her comments on the initial drafts. We would also like to extend our gratitude to Tess Dury, for her research support at the initial stages of the project, Brian Shorten for sharing his expertise with us, and Crofton Black for his early guidance and, as always, his continuous support.

Suggested citation

Vazquez Llorente R. and Wall, I. (eds.) (2014) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management*. European Interagency Security Forum (EISF).

Cover photo: Mary Kiperus, community health worker, uses a mobile phone for reporting to the local nurse. Leparua village, Isiolo County, Kenya. February, 2014. © Christian Aid/Elizabeth Dalziel.

Disclaimer

Other EISF Publications

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

Briefing Papers

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Reports

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez, R. (Sp. and Fr.) – EISF Secretariat

Managing The Message: Communication and Media Management in a Crisis
September 2013
Davidson, S., and French, E., EISF Secretariat (eds.)

Family First: Liaison and Support During a Crisis
February 2013 *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L. – EISF Secretariat

Forthcoming publications

Office Opening Guide