gisf

Section A: Policy and Planning

Module 4: Digital Security

Section A: Policy and Planning

Module 4: Digital Security

Introduction to the series

The pandemic continues to impact not only the security risks that NGOs may face but also the way risk treatment measures are developed, implemented, and communicated to staff. As we get used to new ways of working with COVID-19, and the focus is, rightly, on the pandemic and its impacts, we must ensure that we do not lose sight of ongoing and emerging security situations and issues.

Introduction to the module

As we move further into the 21st Century, life becomes increasingly complex and interconnected including as technology improvements impact every aspect of the way we work and live. Humanitarian, development, and advocacy organisations face new and increasingly diverse challenges that we must overcome if we intend to continue to serve the world's at-risk populations.

One way that organisations attempt to overcome these challenges, keep costs down and manage information better, is to turn to digital and technological tools. The advent of the COVID-19 pandemic has driven us to further embrace technology and that shift will remain a fixture in the future of the sector.

Yet few organisations really take the time to step back and examine their digital 'footprint' and the risks it may present to staff safety, programme integrity, donor confidence and reputational risk. This module is intended to encourage organisations to identify their key challenges going forward, develop a broader understanding of the risks and recommend cost-effective ways to improve an organisation's digital security.

Acknowledgements

This module was written by James Davis. James Davis is the Director of Safeguarding and Security at Women for Women International. A Canadian based in the UK, James has been involved in the international security sector for over 30 years including 11 years in the military and 15 years working with NGOs. James is the principle author of GISF's Security to Go tool and has also contributed guides on digital security. He has served on the UN Saving Lives Together Oversight Committee and presented to 2021's Humanitarian Networking and Partnerships Week (HNPW) on digital security issues.

Suggested citation

GISF (2021) Keeping up with COVID-19: essential guidance for security risk managers, Module A4: Digital Security. Global Interagency Security Forum (GISF). First Edition, January 2022.

Disclaimer

Why is digital security important during the COVID-19 pandemic?

What is digital security?

One of the first challenges for organisations and individuals to grasp is: what is digital security? For the most part it is assumed to be about passwords, computer security software, how to avoid the viruses contained in the fake/scam emails we all receive and how your IT department protects your organisation and confidential data. Certainly, these are the key components; much the same as door locks, alarms, security cameras or lights can be a part of a standard security system. But as we have seen in other modules, security, including digital security, is a much broader issue, encompassing duty of care, liability, acceptance, stress, reputation, terrorism and a host of other challenges.

To understand this, you need to consider your digital 'footprint.' Both for your organisation and as individual staff members. In 2022 our lives are so integrated with digital technology that we are rarely even aware of its existence anymore. It is like the air we breathe. Everything from your coffee maker, smartphone, laptop, car, online takeaways, navigating to a new restaurant, getting on a plane, gathering and analysing data for a new programme, completing a needs assessment or promoting a new campaign; all use digital technology.

Why is this important?

In the modern world the most valuable resource is not gold, diamonds or rubies, it is data. NGO's hold massive amounts of data related to funding, movement of people, community information, health trends, societal beliefs, even down to dates and locations that specific people will attend meetings.

This data is of immense value to governments suspicious of NGOs, minorities or marginalised groups.

Commercial entities looking to profit from identified needs want this data and criminal gangs looking for individuals, communities or agencies also want this data or to hold the data for ransom. LGBTQI+ staff and community members face a significantly elevated level of risk compared to other people. All organisations should be extremely careful in how any data related to those who identify in this group is used, stored or shared.

While many NGO's hold to the concept of neutrality and transparency as sacrosanct, any failure to protect such data from unauthorised access or abuse is a legal and moral failure of our duty of care and do no harm principles.

Scope of digital risk

Digital risk comes in many forms. It can reach us through the hardware, software and apps we use. These threats can target our confidential data, our communications and our programming. We can also suffer from non-targeted digital threats like misinformation or disinformation that undermines confidence in the sector, or programming or our motivations. The loss of data is often not considered when a phone is stolen or memory stick is mislaid and loss is calculated based on the value of the tech rather than the information contained therein.

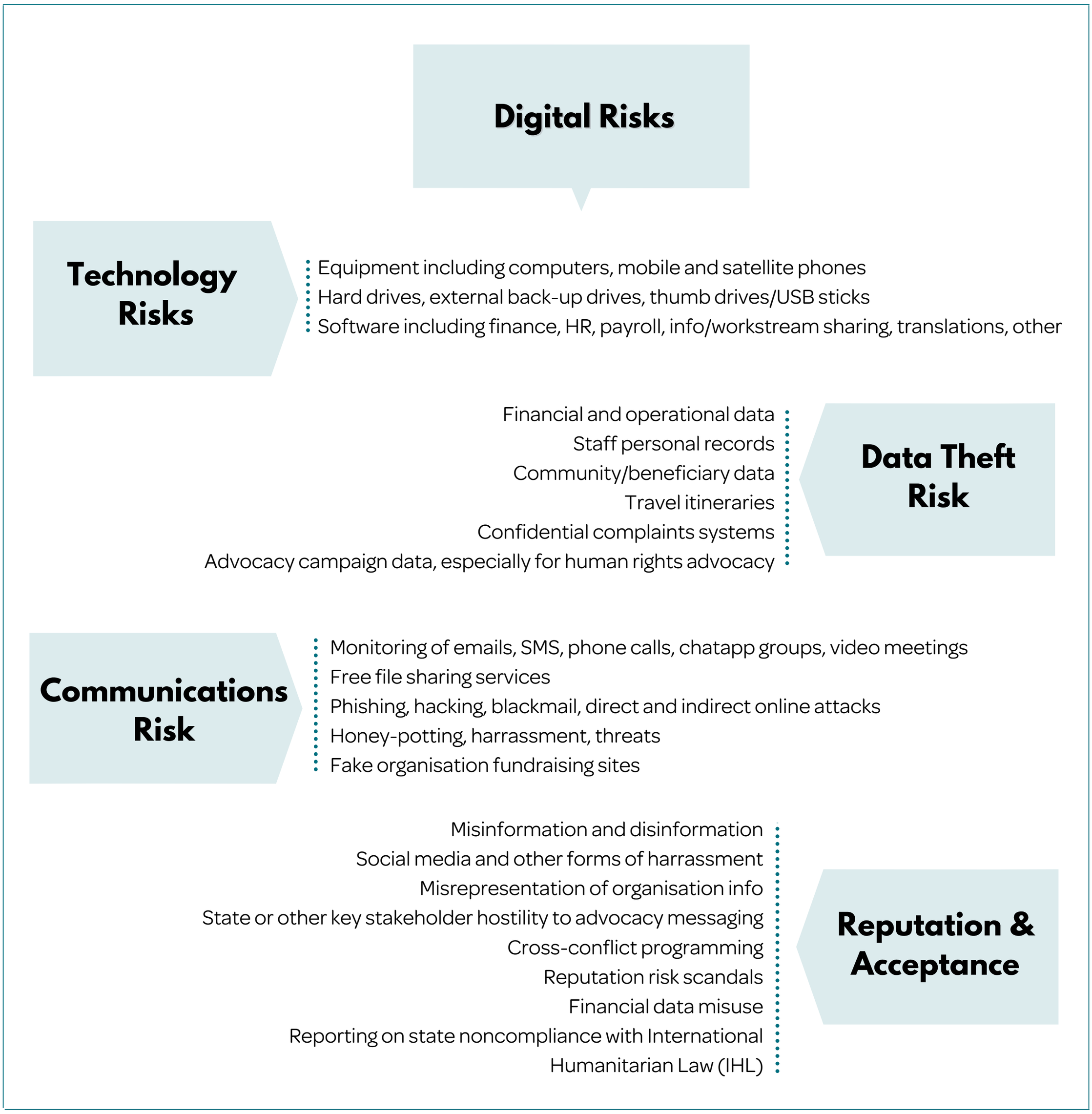

Figure 1: Digital Risks

COVID-19 and Digital Risk

During the COVID-19 pandemic, the aid sector was forced, like most global sectors, to shift to an increasingly digital way of working, including working from home rather than from designated office spaces. Videoconferencing became the norm for both day-to-day work interactions as well as delivering training, holding meetings and even large-scale conferences. Additionally, the pandemic drove more NGOs to adopt online work sharing platforms to ease collaborative work.

Even programme delivery moved further into the digital spectrum with an increase in cash-based programming and block chain for humanitarian relief and some development projects, while advocacy shifted significantly into the online media space. This shift brought an increased risk profile for the sector.

Good practice for security risk management: mitigating digital risk

Conducting an organisational digital risk assessment is a daunting task. The broad scope of all the possible threats that can target you via digital means would require a comprehensive analysis. To further complicate this challenge, many organisational IT departments are mostly focused on hardware security issues such as servers and equipment and not ideally suited to consider how misinformation or disinformation may affect acceptance in operational programming.

This challenge of conducting digital security risk assessments requires a broad range of skills:

- IT teams to assess the hardware, software and system threats.
- All department managers to analyse what software their staff are using and where vulnerabilities might lie.
- Communications staff to conduct a 'digital context analysis' to assess who the stakeholders are and how they use digital media to influence or manipulate acceptance.
- Security staff to identify safety vulnerabilities such as travel risk, communication reliability, physical security of data storage and transport as well as linking other physical risks such as GBV, kidnapping, robbery or sexual harassment and bullying from digital exposure.
- Programming staff to consider how people involved in projects may be exposed to abuse, criminal targeting or other manipulation linked to a digital component of the programme such as cash-based programming, advocacy messaging, community mobilisation or even access to programmes.

Examples of digital risk mitigation measures

Threat:

Digital viruses, phishing attacks, direct and indirect attempts to break into systems.

Mitigation Measures:

- Staff training in good digital practices including recognising digital attacks.
- Complex passwords that are changed regularly
- Caution in accessing 'free' internet in cafe's, airports or elsewhere as these provide relatively easy access into your computer/phone.
- Using Virtual Private Networks (VPNs) whenever possible
- Ensuring staff do not use pirated software on any device that links to your organisational networks
- Set firm rules for uses of thumb drives (USB Sticks), external hard drives and other storage devices and how they are accessed.

Threat:

Hacking or Interference in Communications

Mitigation Measures:

- Set firm rules for videoconferencing including firmly identifying who is attending any calls. This can include making video mandatory at least during introductions, using waiting rooms before access to confirm invite and muting all participants unless permission given to speak by organiser.
- Be aware that any 'free' service for communications like chatapps or videoconferencing earns income by making the user the product. While the content of your call may be 'end-to-end' encrypted, who you are talking to, locations of participants, how long the call lasts, what functions you use is all available for sale to those interested, such as state agencies or commercial actors.
- For advocacy work on 'sensitive' subjects, develop lists of who the known disruptors are and what level of risk they present.
- Be aware of 'honey-potting' where agencies interesting in monitoring the work of NGO staff and their programming pose as similar organisations or networks and invite staff to join and share information with like-minded individuals.

In answer to everyone's question: Is your phone listening to you? The answer is yes. Smartphones and other devices do passively monitor conversations for keywords. It is also possible for some state agencies to access some digital devices to listen for keywords.

This does not mean a person is listening to your conversations. That level of hacking would only occur if you were actively targeted by a state actor.

Advice: For any sensitive conversations, do not have any digital devices present within the room.

Threat:

Challenges to acceptance or reputation through digital means.

- The prevalence of social media as a principal method of spreading information across populations in the modern, digital world presents challenges for NGOs. Aid organisations and their programming are prime targets for manipulation for political, religious or other agenda-driven purposes.
- Misinformation will seek to mislead populations about your work, donors or motivations.
- Disinformation will seek to create counter-narratives of situations to confuse or splinter communities into sometimes dangerous opposing camps.

Mitigation Measures:

- Develop a communication strategy as part of any programme and for each context. As part of your 'digital' context analysis identify what misinformation and disinformation messages are likely to be seen and develop counter messaging.
- Train staff in online safety and the policies around social media messaging.
- Prepare contingency plans for times when especially dangerous misinformation/disinformation appears and what actions will be taken and at what level.
- Be clear in your planning on how and when to actively counter acceptance/reputation attacks. By engaging you may escalate the situation

Threat:

Loss of data

- Temporary confiscation of computers at borders can result in data theft, loss or tampering
- Hacking into computers left accessible, in hotel rooms and elsewhere
- Theft of kit (phones / computers) for resale value
- Loss of computers/ phones / thumb drives

Mitigation Measures:

- Ensure staff maintain good password management and change these regularly
- Ensure data can be wiped remotely by an Administrator
- Establish and disseminate clear Standard Operating Procedures for data management and storage, and device management

Inclusivity consideration for digital security

It is critically important as part of your digital risk assessment and mitigation measures to remember that like physical threats, digital threats do not target everyone equally.

- In locations where people are only beginning to get online and are new to the digital world, their awareness of the threats present may be lower. If programming has any digital component, from how registrations are received through to M&E feedback or especially cash-based programming, ensure you have online safety awareness training as a component of programme delivery.
- Women and girls are at a higher risk of targeting for harassment or online abuse. Ensure that safeguarding, protection and Code of Conduct policies are clearly reflected in your digital security strategies.

- LGBTQI+ staff and community members face a significantly elevated level of risk compared to other people. Ensure that security concerns are equitably prioritised by the organisation, and that digital security measures and strategies are inclusive.

Conclusion

It is hard to overstate how much the 'digital revolution' is now affecting the global aid sector and how that influence will only continue to grow. More and more functions that used to be done by staff are now being replaced by software applications or other digital system. COVID-19 has only driven this shift to digital ways of working, and as organisations see possible savings in cost and carbon footprint this is likely to stay. File sharing systems, videoconferencing, social media campaigns or fundraising, marketing meta-analysis tools and many other systems have only increased our digital footprint.

Even at the programme delivery level technology is increasingly changing the way we reach communities and provide support. All at a time when agenda media, social division, misinformation, disinformation, cybercrime and our data as a valuable commodity, increases threats to the sector.

The first step in addressing these challenges is awareness that they exist. Dismissing digital security as solely an IT department issue is a clear duty of care and do no harm failure. It is an issue for all staff from senior management to project staff. It is highly probably that digital risk will replace physical risk in the next decade as the principal threat to the aid sector.

Start with an honest and broad digital risk assessment for your organisation and programmes, do your research and develop good digital risk mitigation strategies.

Useful sources

ACT Digital Security Guidelines

Further information

GISF *Security to Go Digital Security module*

HNPW x GISF *Managing Security Risks in a Digital World*

GISF *Digital Security Resources*