HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

Mini MBA Security and Risk Management: protecting teams and maintaining access

Course handout · Week 9 : Digital security and information protection

A programme of exactly 3 months (12 weeks, 144 hours) to manage the security and risks of a humanitarian organisation: duty of care, context analysis, risk assessment, plans and procedures, acceptance and access negotiation, incidents, crisis management and kidnapping, staff health and wellbeing, digital security and data protection, organisational risks and compliance, risk sharing with partners, governance and business continuity. Corrected numerical exercises, three monthly exams with case studies, and a verifiable diploma from the Humanitarian Academy.

https://humanitairejobs.org/en/academy/mini-mba-securite-risques/semaine-9/

Free document from the Humanitarian Academy. It may be printed and shared freely for training purposes, without modification.

Week 9 : Digital security and information protection

Objectives

- Identify the digital threats specific to humanitarian organisations: phishing, payment fraud, surveillance, data leaks.
- Put in place proportionate basic measures: authentication, backups, encryption, access management, devices.
- Protect the data of the people assisted and of staff, and respond to a digital incident.

Why digital is a security risk

Humanitarian organisations hold highly sensitive information: beneficiary lists (sometimes with biometrics and location), testimonies of violations, medical data, staff information, security analyses, movements. A leak or a hack can put **lives** in danger, not just data.

Several well-known cyberattacks have targeted humanitarian organisations, including the theft of data on hundreds of thousands of vulnerable people. Organisations are also targeted by online financial fraud and by **surveillance** of communications by state or non-state actors.

Main threats:

- **Phishing**: fake emails or messages that steal credentials or install malware.
- **Payment fraud**: a fake supplier, a fake director requesting an urgent payment, a fraudulent change of bank details.
- **Ransomware**: data encrypted in exchange for a ransom.
- **Theft or seizure of devices** (laptops, phones) at checkpoints or during robberies.
- **Surveillance** of communications and social media.
- **Internal errors**: sharing by mistake, a file sent to the wrong recipient, a password left on display.

Basic measures

A few simple measures block the vast majority of common attacks:

- **Multi-factor authentication** (MFA) on email, online storage, banking and accounting software.
- A **password manager** and long, unique passwords.
- Automatic **updates** of systems and applications.
- Regular **backups**, including one offline or isolated copy, and restore tests (3-2-1 rule: three copies, two different media, one copy off-site).
- **Encryption** of laptop and phone storage.

- **Access management**: everyone accesses only what they need; access removed on the day a staff member leaves.
- Regular **training**, with simulated phishing exercises.

Example of an exercise. A fake phishing email is sent to 120 staff: 38 click on the link (31.7%), 14 enter their credentials (11.7%), 9 report the email to the IT department (7.5%). After targeted training, a second exercise gives 12 clicks (10%), 3 credential entries (2.5%) and 41 reports (34.2%). The rise in reports is as important as the fall in clicks: it turns staff into an early warning system.

Payment fraud and financial procedures

CEO fraud and bank-detail fraud cost organisations, including humanitarian ones, considerable sums every year. Financial procedures are the best defence:

- Any **change of bank details** of a supplier or staff member is verified by calling a number already known, never the one given in the request.
- No urgent payment outside procedure, even at the apparent request of a director: dual approval remains mandatory.
- Online banking access uses dedicated devices and accounts, with dual electronic signature.
- Staff know they will be **backed** if they refuse a suspicious payment, even one requested by a superior.

> Urgency and confidentiality are fraudsters' two favourite levers: "I'm in a meeting, make this transfer right away and don't tell anyone."

Devices, checkpoints and surveillance

In the field, digital risks are also **physical**:

- At checkpoints, phones may be searched. A phone containing photos of military positions, messages critical of a party or beneficiary lists can lead to detention. Rule: carry only what is necessary, delete sensitive data from field devices, use dedicated work devices.
- Staff **social media** reveal exploitable information: real-time location, political opinions, photos of colleagues, signs of wealth. A social media policy that is explained and not punitive reduces these risks.
- End-to-end encrypted **messaging apps** protect content, but not the fact that people are communicating, nor the phone itself if it is seized unlocked.
- The use of certain tools (satellite equipment, VPNs, drones) may be prohibited or viewed with suspicion: check the legislation and acceptance.

Protecting people's data

The **data protection** of beneficiaries and staff rests on recognised principles (notably the ICRC and Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action):

- **Lawfulness and purpose**: a legitimate basis and a specific purpose for each collection.
- **Minimisation**: collect only what is necessary.
- **Informed consent** where it is the chosen basis, taking power relations into account (a household that needs aid is not free to refuse).
- **Security**: encryption, limited access, logging.
- **Limited retention** and deletion once the purpose has been fulfilled.
- **Controlled sharing** governed by data-sharing agreements, with a risk analysis (including requests from authorities or parties to the conflict).
- **Impact assessment** before any new system (biometrics, mobile payments, shared platform).

Example of minimisation. For a kit distribution, you need to identify the household and check that it has not already received the kit. Ethnic or religious affiliation is not necessary and must not be collected; a photo and fingerprint are generally not necessary either.

Responding to a digital incident

A digital incident (hacked account, stolen computer, ransomware, file sent by mistake) is handled like a security incident:

- **Contain**: change passwords, revoke sessions, isolate the infected device, remotely wipe a stolen device.
- **Assess**: what data, which people, what risk to them?
- **Inform**: senior management, the data protection officer, the people concerned if they are exposed to a risk, supervisory authorities according to the applicable law, donors according to the contracts.
- **Restore** from backups; do not pay a ransom without a decision by senior management and a legal analysis.
- **Learn**: analysis, corrections, training.

Example. An unencrypted laptop containing the list of 3,200 households with their phone numbers and locations is stolen during a robbery. The risk to the people depends on the context: if some households belong to a targeted group, it is high. Actions: immediate assessment, informing the communities concerned through safe channels if they are exposed, changing the means of contact, mandatory encryption of all laptops.

Exercise: an urgent email from the director

Situation. On a Friday at 17:00, the accountant receives an email apparently from the country director, who is travelling: "Confidential. We must pay the USD 48,000 deposit to the new fuel supplier today, otherwise we lose the contract. Bank details attached. I can't be reached, meeting with the minister." The sender's address differs by one letter from the usual address. On the same day, a regular supplier asked by email to change its bank details. The organisation's email system has no two-factor authentication.

Task. 1) Warning signs. 2) Immediate course of action. 3) Lasting measures.

Answer. 1) Urgency, confidentiality, the requester being unreachable, a new supplier with no procurement file, a slightly different sender address, a parallel request to change bank details. 2) Do not pay; call the director on their known number (or their deputy); do not change the regular supplier's details without a verification call to a number already known; report to the IT manager and to finance; keep the emails as evidence. 3) Two-factor authentication across the whole email system; a written rule: no payment outside procedure, dual approval, telephone verification of any change of bank details; training and phishing exercises; filtering of look-alike domains; a clear message from senior management: refusing a suspicious payment will always be backed.

Key takeaways

- Humanitarian data are sensitive: a leak can put lives in danger.
- MFA, unique passwords, updates, 3-2-1 backups, encryption, minimal access, training.
- Payment fraud: verification through a known number, dual approval, backing for whoever refuses.
- Field: stripped-down devices at checkpoints, a social media policy.
- Data protection: purpose, minimisation, security, limited retention, impact assessment.

Quiz

1. 150 staff receive a fake email; 24 click. Click rate:
   A. 24%
   B. 16%
   C. 6.25%
   D. 15%

2. The 3-2-1 backup rule means:
   A. 3 copies, 2 different media, 1 copy off-site
   B. 3 passwords, 2 factors, 1 account
   C. 3 days, 2 weeks, 1 month
   D. 3 servers, 2 countries, 1 cloud

3. A supplier asks by email to change its bank details. You:
   A. Change them immediately
   B. Pay in cash
   C. Reply to the email
   D. Verify by calling the number already known

4. For a kit distribution, collecting households' ethnic affiliation is:
   A. Mandatory
   B. Recommended
   C. Contrary to the minimisation principle if it is not necessary
   D. Risk-free

5. An unencrypted laptop containing beneficiary lists is stolen. First step:
   A. Buy a new laptop
   B. Assess the data exposed and the risk to the people, then inform
   C. Say nothing
   D. Publish a press release

Quiz answers : 1. B · 2. A · 3. D · 4. C · 5. B