

Role title:	Cybersecurity Consultant
Remuneration:	Daily rate in region of £200 - £250, subject to experience and location. ECC applies the ICSC salary post adjustment scales to ensure equity among staff in different locations.
Role purpose:	To assist ECC and members of the international Casualty Recorders Network to develop and implement essential cybersecurity policies and practices.
Working hours:	Flexible. Must be able to work across UK and East Africa time zones.
Contract:	Initially 45 days to be delivered within 8 months. Contract may be extended/renewed subject to agreement.
Reports to:	Executive Director
Location:	Fully remote / home based

Application deadline: 20 February 2026

About us

ECC is a UK registered charity which exists to support, raise awareness of, and promote the careful recording of casualties of armed conflict worldwide. We convene an international network of casualty recording organisations, and support its members with technical advice, capacity building support, training, advocacy, and networking opportunities. We also research aspects of casualty recording, including its procedures, development, legal basis, and impacts. The ultimate aim of our work is to save lives, relieve suffering, and support sustainable conflict resolution.

ECC supports and coordinates the Casualty Recorders Network (CRN), a group of organisations that document deaths and injuries resulting from armed violence in diverse and often high-risk environments.

Role purpose

The purpose of this role is to improve the cybersecurity knowledge, practice and capabilities of ECC and selected members of the Casualty Recorders Network. These organisations work with highly sensitive personal information, as well as material which is legally or politically sensitive. Strengthening data security and cybersecurity practices is essential to protect witnesses, victims, staff and other partners.

The Consultant will work with ECC and ten (10) selected organisations within the CRN to conduct a professional security assessment of each, identify the most appropriate

solutions for their needs, and advise on implementing these. For each organisation the process will include:

- Reviewing existing IT infrastructure, data management systems, security policies, security incident reports, network diagrams, asset inventories, etc.
- Interviewing designated key person(s) at each organisation to identify security priorities, infrastructure needs, ongoing budget potential, technical controls, staff training programmes, etc
- Review policies and draft updates as needed
- Conduct technical testing including vulnerability scanning, configuration reviews
- Compile findings, present recommendations
- Present results, discuss recommendations, answer questions
- If needed, assist with implementation of required changes

The consultant's risk analysis, recommendations and policy proposals must be suitable for the specific security context and infrastructure reality of CRN members. They must be appropriate for complex security environments and not simply theoretical best practice.

Estimated time requirement is 32 hours (four working days) per organisation, plus initial briefing and familiarisation time with ECC.

Key Responsibilities

1. Assessment and Risk Analysis

- Conduct assessments of existing data security and cybersecurity practices within ECC and selected CRN member organisations.
- Identify risks related to data collection, storage, processing, transmission, and sharing, including risks specific to conflict affected or repressive environments.
- Map threat models relevant to casualty recording (e.g. state and nonstate surveillance, data breaches, insider risks, device loss, and cyberattacks).

2. Policy and Framework Development

- Develop or update data security, cybersecurity, and information governance policies aligned with humanitarian principles and human rights standards.

- Support the development of data classification, access control, retention, and secure deletion frameworks.
- Ensure alignment with relevant data protection regulations where applicable (e.g. GDPR or equivalent standards), while remaining sensitive to local contexts.

3. Technical and Operational Guidance

- Provide practical recommendations on secure data storage, encryption, authentication, backups, and incident response.
- Advise on secure use of hardware, software, cloud services, and communication tools used by casualty recorders.
- Support the selection and configuration of secure, low risk tools suitable for resource constrained and high risk environments.

4. Capacity Building and Training

- Design and deliver tailored training sessions and guidance materials for ECC staff and CRN members on data security and cybersecurity.
- Build awareness of digital hygiene, secure workflows, and risk aware decision making.
- Develop user-friendly resources (e.g. checklists, SOPs, quick reference guides) for non-specialist audiences.

5. Incident Preparedness and Response

- Support the development of incident response plans and escalation procedures.
- Advise on breach response, harm mitigation, and communication strategies in the event of a data or security incident.
- Promote a culture of continuous improvement and learning around digital security.

6. Coordination and Advisory Support

- Work closely with ECC coordination staff and CRN members to ensure recommendations are realistic and context appropriate.
- Provide ongoing advisory support during the consultancy period.
- Contribute to strategic discussions on ethical data management and protection of affected populations.

Deliverables (both for ECC and selected CRN members)

- Data security and cybersecurity assessment report(s).
- Practical, prioritised recommendations and risk mitigation plans.
- Updated or newly developed policies, SOPs, and guidance documents.
- Training sessions and accompanying materials.
- Incident response and data protection guidance tailored to casualty recording.

Required Qualifications and Experience

- Demonstrated expertise in data security, cybersecurity, and information risk management.
- Experience working with sensitive data, preferably in humanitarian, human rights, journalism, or civil society contexts.
- Strong understanding of digital security challenges in conflict affected, fragile, or high risk environments.
- Experience conducting risk assessments and developing practical, nontechnical guidance.
- Proven ability to communicate complex technical concepts to nontechnical audiences.
- Fluency in English.

Desirable Qualifications

- Fluency in Arabic and/or Somali and/or French.
- Familiarity with casualty recording, human rights documentation, or protection focused data collection.
- Knowledge of relevant data protection and privacy standards and regulations.
- Experience working with international networks or decentralized partner organisations.
- Background in capacity building and adult learning.

Competencies

- Strong analytical and problem solving skills.
- Cultural sensitivity and ethical awareness.
- Ability to work independently and collaboratively across time zones.
- Commitment to humanitarian principles, human rights, and data responsibility.

Reporting and Coordination

The consultant will report to the ECC Executive Director and Network Director, and work closely with designated focal points within CRN member organisations.

How to apply

To apply for this role, please send your CV/Resume and a covering letter highlighting how you meet the requirements for this role to: director@everycasualty.org.

DEADLINE: Friday 20 February 2026

If you have questions about the role which you would like to discuss before applying, please contact info@everycasualty.org.