bg right

Cybersecurity in the Humanitarian Sector

HNPW 2023 – Geneva

width:120%

020 agenda

bg right:20%

Before starting

width:720px

Agenda

- Digital transformation in the humanitarian space
- Cybersecurity in the humanitarian sector
- Recent attacks
- Existing solutions
- Path forward

What about you?

bg right:20%

> In this room, **did you, or your organization have been concerned by cybersecurity threats** over the past 12 months?

If yes, please raise your hand :hand:

Current cyber threats and trends

bg left

Understanding the challenges for humanitarian organizations

Particular threats to humanitarian and international organizations

bg left:20%

Nature of sensitive data and information

bg left:20%

- **Personal data** of beneficiaries
  - ex: name, address, medical situation, etc.
- **Financial information**
  - ex: transactions, budgets, donations
- **Response and support plans**
- Internal and external **communications**
- **Locations** of facilities and personnel

Potentially vulnerable infrastructure and networks

bg left:20%

- **Poorly secured networks**
  - ex: wireless networks (Wi-Fi)
- **Cloud-based data** storage systems
- **Mobile applications and online software** for collaboration
- **Outdated or unpatched IT** infrastructure
- IoT and other **connected devices**

Collaboration with various partners and stakeholders

bg left:20%

- **Shared information** with other NGOs, governments, and donors

- **Relationships with service providers**
  - ex: hosting, communication
- Many **temporary access to systems**
  - ex: volunteers and temporary providers
- **Interactions with local communities** and beneficiaries

Operations in high-risk areas

bg left:20%

- **Presence in conflict or crisis areas**
- **Exposure to targeted cyber attacks** by malicious actors
- Increased vulnerability due to **less secure local infrastructure**
- Risk of compromise of systems and communications **during emergency response**

Specific internal and external threats

bg left:20%

- **Manipulation or detour of humanitarian aid** for malicious purposes
- State actors or armed groups seeking **access to information to influence or control humanitarian operations**
- **Cyber-espionage** to obtain information about organizations' activities, strategies, partners and funding sources
- **Disclosure of sensitive information about beneficiaries**, jeopardizing their safety and privacy
- **Internal threats** from disgruntled employees, infiltrated volunteers, or partners with ulterior motives that can compromise organizational systems and data

Trends and impacts

bg left:20%

Cybersecurity incidents affecting humanitarian organizations

bg left:20%

- **DDoS attacks** targeting NGO websites
- **Email account compromise** and identity theft
- **Unauthorized access** to sensitive databases
- **Disclosure of personal information** of beneficiaries and staff
- **Humanitarian consequences of attacks** on critical infrastructure
- **Use of information as a weapon** in conflict
- **Risk of espionage and information manipulation** by state actors

Types of common attacks (ransomware, phishing, etc.)

bg left:20%

- **Ransomware**
  - malicious software that encrypts an organization's data and demands payment for its release
- **Phishing**
  - fraudulent emails impersonating legitimate organizations
- **Brute force attacks**
  - access attempts by successive password attempts
- **Malware**
  - malicious programs aimed at compromising computer systems
- **Targeted attacks by state actors** or state-sponsored groups
- **Cyber-espionage** and theft of sensitive information

- **Sabotage** and data destruction

Evolution of cyber threats over time

bg left:20%

- **Increased automation of attacks**
- More sophisticated and **organized cybercriminals**
- Increased use of social networks to conduct **disinformation campaigns**
- Growth in **attacks targeting mobile devices** and the Internet of Things (IoT)
- Increasing involvement of state and non-state actors
- Cyber conflicts and the use of **cyber warfare as an instrument of power**
- Development of new tactics and techniques for cyberattacks

Financial and operational impact of cyberattacks

bg left:20%

- **Recovery and remediation costs** after a successful attack
- **Disruption of humanitarian services** and operations
- **Loss of donor and partner confidence**
- **Damaged reputation** and potential legal consequences
- Indirect costs related to **loss of trust of beneficiary populations**
- **Diversion of resources** to deal with cyber attacks
- Security **risks to employees and beneficiaries** if sensitive information is disclosed

Cyber security in different geopolitical contexts

bg left:20%

Geopolitical and regional context of cyber threats

bg left:20%

- **Political and economic tensions** exacerbate the risk of cyberattacks
- **Nation states may be involved** in cyber attacks
- **Cybercriminal groups** located in certain regions
- **Non-state actors and terrorist groups** exploiting cyberspace

Threats specific to regions where humanitarian organizations operate

bg left:20%

Sub-Saharan Africa

- Cyber attacks **targeting critical infrastructure**
  - ex: medical facilities, water and electricity distribution networks
- Ransomware **attacks targeting humanitarian organizations**

Threats specific to regions where humanitarian organizations operate

bg left:20%

Middle East and North Africa

- Cyber **espionage related to regional conflicts**
  - ex: monitoring of communications of humanitarian organizations
- **Targeted attacks on human rights defenders** and civil society organizations
- Use of malware to **disrupt humanitarian operations**

Threats specific to regions where humanitarian organizations operate

bg left:20%

Asia-Pacific

- **Cyberattacks to compromise humanitarian organizations'** information systems
- **Online extortion and blackmail** attempts against aid workers

Threats specific to regions where humanitarian organizations operate

bg left:20%

Latin America and the Caribbean

- **Organized cybercrime targeting financial and personal data** of humanitarian organizations
- **Attacks on organizations** fighting corruption and organized crime
- Cybersecurity threats related to political violence and social tensions

Threats specific to regions where humanitarian organizations operate

bg left:20%

Europe and North America

- **Phishing and social engineering attacks targeting employees** and volunteers of humanitarian organizations
- **Cyberattacks targeting supply chains and local partners** of humanitarian organizations
- **Attempts to infiltrate and compromise the IT systems** of humanitarian organizations

Adapting strategies accordingly

bg left:20%

- **Analysis of the risks linked to the geopolitical and regional context**
- Implementation of **defense mechanisms adapted to specific threats**
- **Cooperation with local authorities** and regional partners (if possible)

Inter-organizational cooperation to strengthen cybersecurity

bg left:20%

Importance of inter-organizational cooperation and information sharing to effectively combat cyber threats

bg left:20%

- **Exchange of information** on threats and vulnerabilities
- Improved **understanding of attacker trends** and tactics
- **Strengthen collective resilience** to cyberattacks
- **Facilitating incident response** and recovery after an attack

Existing cooperation and information sharing mechanisms

bg left:20%

- National and sectoral **Computer Emergency Response Teams** (CERTs)
- Platforms for **sharing information on threats** (e.g. ISACs, MISP)
- **Specialized working groups** and forums (e.g. FIRST, GFCE)
- Bilateral and multilateral **cooperation agreements between organizations**
- **Initiatives supported by the United Nations** and other international organizations

Examples of successful collaborations between organizations to strengthen cybersecurity

bg left:20%

- Collaboration between CERTs to **dismantle cybercrime networks**
- Joint **development of standards and best practices** (e.g. NIST, ISO)
- **Inter-organizational awareness** and training campaigns
- Coordination of **large-scale incident response efforts**
- Sharing of tools and resources to **improve detection and defense capability**

Call to Action

bg left:20%

Leadership and stakeholder accountability

bg left:20%

- **Understand the cybersecurity threats and risks** to their organization
- Implement appropriate **cybersecurity policies**
- **Allocate resources for cybersecurity** (budget, staff, training)
- **Ensure employees understand their role** in protecting data and systems
- **Foster a culture of cybersecurity** within the organization
- **Educate employees on geopolitical issues** related to cybersecurity
- **Engage in dialogues with global partners** to improve cybersecurity

Importance of cybersecurity in organizational strategy

bg left:20%

- Preventing financial losses due to cyberattacks
- Protect the organization's reputation and donor trust
- **Ensure business continuity** and ability to deliver aid
- **Protect sensitive beneficiaries** and employee data
- Meet legal and regulatory requirements for data protection
- **Prevent human rights abuses** related to cybersecurity breaches
- Strengthen organizational resilience to cyber threats in a complex geopolitical environment

Cooperation and information sharing between organizations

bg left:20%

- **Partner with other NGOs and cybersecurity experts**
- Participate in threat information exchange platforms (e.g. CERT, ISAC)
- Coordinate efforts to combat common cyber threats
- **Share best practices and lessons learned** in cybersecurity
- Create regional or sectoral alliances to strengthen cybersecurity
- Collaborate with government and intergovernmental organizations to share information
- **Develop common standards and protocols to facilitate cooperation** and information sharing on cybersecurity

Questions for the audience

bg left:20%

- **What are your top cybersecurity concerns** in your organization?
- **Have you ever faced a cyber attack?** How did your organization respond?
- **What measures does your organization have in place** to address cyber threats specific to humanitarian organizations?
- **How does your organization work with other stakeholders** to strengthen cybersecurity?

000 index

Practical tips

... for securing your organization and partner organizations

bg right

Cybersecurity challenges for organization leaders

bg right:20%

Leadership responsibilities for cybersecurity

bg right:20%

* **Establishing a clear and consistent cybersecurity policy** * Ensure compliance with applicable regulations and standards * Designate a cybersecurity manager within the organization * **Educate and train all staff on cybersecurity**

Risk assessment and vulnerability management

bg right:20%

- **Identify critical digital assets** (systems, networks, data)
- **Perform regular risk analysis**
- Prioritize remediation actions based on potential impact
- Implement a vulnerability management process to correct security breaches

Communication and collaboration, to share information on threats and best practices

bg right:20%

- **Establish secure communication channels** to share sensitive information
- **Establish communication protocols** with other humanitarian organizations
- Participate in forums to share information on threats and best practices

Strategic investments in cybersecurity to improve cooperation and information sharing capacity

bg right:20%

- **Allocate sufficient resources to ensure systems and data protection**
- Invest in cybersecurity technologies that are appropriate for the organization's needs
- **Evaluate the return on investment of cybersecurity initiatives in terms of risk reduction**

Establish cybersecurity governance to foster a culture of security and inter-organizational cooperation

bg right:20%

- Create a cybersecurity committee that includes representatives of the various stakeholders
- **Establish procedures for monitoring and controlling cybersecurity measures**
- **Promote a culture of security and inter-organizational cooperation**
- Integrate cybersecurity into the organization's overall strategy

Targeted advice for IT project managers

bg right:20%

Use of best practices and security standards

bg right:20%

- **Adopt standards such as ISO 27001**, NIST, and CIS Critical Security Controls
- Implement information security policies
- Conduct regular vulnerability testing and security audits
- **Apply the principle of least privilege for access rights**

Access and identity management

bg right:20%

- **Use two-factor authentication** (2FA)
  - ~~for sensitive accounts~~ **for everyone !**
- **Implement an identity and access management** (IAM) system
- Regularly monitor and audit access to sensitive resources
- Quickly revoke access rights of employees who leave the organization

Securing networks and systems

bg right:20%

- Deploy firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- **Encrypt sensitive data and communications**
- Apply regular security patches and keep software up to date
- Segment the network to **isolate critical systems**

Implement incident detection and response mechanisms

bg right:20%

- Set up a security operations center (SOC)
- Use security information and event management (SIEM) tools
- **Define and test a cybersecurity incident response plan**
- Perform post-incident analysis to improve processes and systems

Manage third party vendors and partners

bg right:20%

- **Assess cybersecurity risks associated with vendors and partners**
- **Include cybersecurity clauses in contracts** and cooperative agreements
- Regularly audit suppliers and partners for compliance with security standards
- Sharing cyber threat information with partners and cooperating organizations

Training and awareness of technical staff

bg right:20%

- Provide training on security best practices and specific tools
- Raise awareness of the challenges of inter-organizational collaboration and information sharing
- Encourage participation in conferences and workshops on cybersecurity
- Organize practical exercises to reinforce technical security skills

3-month action plan...

... to immediately improve cybersecurity in your organization

bg right:20%

Establish a cybersecurity committee

bg right:20%

- Identify key members of the organization (management, IT, legal, HR)
- Define the roles and responsibilities of each member
- Schedule regular meetings to discuss cybersecurity issues
- Coordinate cybersecurity efforts between different stakeholders

Conduct an initial cybersecurity audit

bg right:20%

- Inventory IT assets and sensitive information
- Assessing vulnerabilities and associated risks
- Identify security vulnerabilities in infrastructure, processes and policies
- Prioritize corrective actions based on risks

Develop and implement cybersecurity policies and procedures

bg right:20%

- Write clear policies on data and access management
- Establish procedures for securing equipment and networks
- Establish processes for managing cybersecurity incidents
- Integrate cybersecurity into vendor and partner management practices

Training and awareness of personnel on cybersecurity

bg right:20%

- Assess staff training and awareness needs
- Design specific training for different target groups
- Use interactive methods to reinforce learning (workshops, simulations)
- Measure the effectiveness of the training and adjust the content accordingly

Strengthen the security of critical infrastructure

bg right:20%

- Update operating systems and software to address vulnerabilities
- Configure firewalls and intrusion detection systems
- Encrypt sensitive data and communications
- Implementing access controls and strong authentication

Planning and conducting incident response exercises

bg right:20%

- Develop cybersecurity incident scenarios (phishing, ransomware, intrusion)
- Involve cybersecurity committee members and relevant stakeholders
- Organize simulation exercises to test procedures and reactions
- Analyze results and identify improvements needed

Monitor and evaluate cybersecurity progress

bg right:20%

- Establish key performance indicators to measure progress
- Conduct regular cybersecurity audits to identify new vulnerabilities
- Collect feedback and share lessons learned

- Adjust policies, procedures and training in response to changes in the environment and threats

Challenges and opportunities of inter-organizational collaboration

bg right:20%

Importance of inter-organizational and international cooperation in combating cyber threats

bg right:20%

- Joining efforts to identify and mitigate common threats
- Share resources and expertise to improve incident response capability
- Facilitate the exchange of best practices and knowledge in cybersecurity

Collaborative opportunities to build resilience across the humanitarian sector to cyber threats

bg right:20%

- Develop more effective incident detection and response capabilities
- Implement coordinated and consistent cybersecurity strategies
- Receive technical and financial support to strengthen organizations' cybersecurity

Potential challenges in sharing sensitive information and coordinating between organizations

bg right:20%

- Maintaining confidentiality and security of shared information
- Managing legal and regulatory differences between countries and organizations
- Building trust among stakeholders to foster cooperation

Best practices and existing mechanisms for information sharing and collaboration

bg right:20%

- Platforms for threat information exchange (e.g. CERT, ISAC)
- Cybersecurity working groups and networks (e.g. FIRST, GFCE)
- Standardized protocols and formats for information sharing (e.g. STIX, TAXII)

Identification of potential partners for cybersecurity cooperation

bg right:20%

- Governmental and non-governmental cybersecurity organizations
- Private companies and security service providers
- Research groups and universities working on cybersecurity issues
- Other humanitarian organizations and industry partners

Awareness and training

... of humanitarian personnel in cybersecurity

bg left

Importance of awareness

bg left:25%

Key role of staff in the security of the organization

bg left:25%

- **Informed decision making** regarding cybersecurity
- **Enforcement of security policies and procedures**
- **Detecting and reporting security incidents**
- Participate in incident response exercises
- Collaborating with partners and stakeholders to enhance security

Risks related to human error and lack of training

bg left:25%

- Failure to follow security policies and procedures
- **Unintentional disclosure of sensitive information**
- **Using weak or reused passwords**
- **Installing unauthorized software or insecure devices**
- Clicking on malicious links or opening infected attachments

Strengthening the culture of safety within the organization

bg left:25%

- Ongoing staff awareness and training
- Accountability of managers and employees
- Clear and transparent communication on safety issues
- Establishment of a safe and prevention-oriented work environment

- Encouraging internal and external cooperation to build resilience to cyber threats

Training and awareness programs

bg left:25%

Assess training and awareness needs

bg left:25%

- Identify target groups (management, technical staff, non-technical staff)
- Assess existing knowledge and gaps

Development of customized training programs

bg left:25%

- Initial training for new employees
- Ongoing training and refresher courses
- Training modules specific to roles and responsibilities

Awareness techniques and methods

bg left:25%

- Workshops and seminars
- Simulations and practical exercises
- Communication materials and internal campaigns

Measuring the effectiveness of training and awareness programs

bg left:25%

- Monitoring of key performance indicators

- Regular evaluation and adjustments
- Feedback and sharing of lessons learned

bg right

Thank you for your attention!

Any questions ?

HNPW 2023 - Cybersecurity and human security for humanitarians

noindex.fr

URL: https://hackmd.io/6k1v6uXPQemhbvqDUJ-T0A

[TECHY is a technology expert. TECHY are specialized in systems, networks and infrastructures. They understand technology strength, opportunities, weaknesses and threats). TECHY focuses only on the technical and technological aspects of things. TECHY is methodical and analytical in his answers. TECHY admits his incompetence on other topics. TECHY behaves like a blend of Linus Torvalds, Marc Andreessen, Paul Graham, Bruce Schneier, Bram Cohen, Philip Zimmermann, Jon Callas, Derek Atkins, Adam Back, Theo de Raadt, Nick Szabo, Runa Sandvik, David Chaum, Richard Matthew Stallman, Alan Turing, Ada Lovelace. When TECHY wants to reply, you start your reply by “TECHY:” and then you will answer to the questions or to the prompt like if TECHY was answering himself.]

[GEOPOLY is an expert blending geopolitics, humanitarianism, and diplomacy. Passionate about international relations, you advise on geopolitical trends, security risks, and economic opportunities. Experienced in NGOs and humanitarian organizations, you provide aid and education to affected communities. As a diplomat, you negotiate with foreign partners, resolve conflicts, and maintain relations. Multilingual and culturally knowledgeable, you are a skilled communicator. Inspired by Huntington, Fukuyama, Brzezinski, Slaughter, Farmer, Power, Egeland, Doctors Without Borders, Maurer, Kissinger, Albright, Mahbubani, Ban Ki-moon, Pascal Boniface, Hubert Vedrine, and Rice. When GEOPOLY wants to reply, you start your reply by “GEOPOLY:” and then you will answer to the questions or to the prompt like if GEOPOLY was answering himself.]

CONTEXTE

Cybersecurity and human security for humanitarians HNPW 2023

PUBLIC

- Des responsables et membres d'ONG
- ONG internationales, ONG humanitaires, agences des nations unies

Titre: HNPW 2023 - Cybersecurity and human security for humanitarians

Cybermenaces actuelles et tendances : Comprendre les enjeux pour les organisations humanitaires

Raisons spécifiques aux organisations humanitaires et internationales

- Nature des données et informations sensibles
  - Données personnelles des bénéficiaires (nom, adresse, situation médicale, etc.)
  - Informations financières (transactions, budgets, dons)
  - Plans d'intervention et de soutien
  - Communications internes et externes
  - Localisations des installations et du personnel
- Infrastructures et réseaux potentiellement vulnérables
  - Réseaux sans fil (Wi-Fi) mal sécurisés
  - Systèmes de stockage des données dans le cloud
  - Applications mobiles et logiciels de collaboration en ligne
  - Infrastructure informatique obsolète ou non patchée
  - Equipements IoT et autres dispositifs connectés
- Collaboration avec divers partenaires et parties prenantes
  - Partage d'informations avec d'autres ONG, gouvernements et donateurs
  - Relations avec les fournisseurs de services (hébergement, communication)
  - Accès aux systèmes par des bénévoles et prestataires temporaires
  - Interactions avec les communautés locales et les bénéficiaires
- Opérations dans des zones à risque élevé
  - Présence dans des régions touchées par des conflits ou des crises
  - Exposition aux cyberattaques ciblées par des acteurs malveillants
  - Vulnérabilité accrue en raison d'infrastructures locales moins sécurisées
  - Risque de compromission des systèmes et des communications lors d'interventions d'urgence
- Menaces internes et externes spécifiques
  - Manipulation ou détournement de l'aide humanitaire à des fins malveillantes

    - Acteurs étatiques ou groupes armés cherchant à accéder aux informations pour influencer ou contrôler les opérations humanitaires
    - Cyberespionnage pour obtenir des informations sur les activités des organisations, leurs stratégies, leurs partenaires et leurs sources de financement
    - Divulgation d'informations sensibles sur les bénéficiaires, mettant en danger leur sécurité et leur vie privée
    - Menaces internes provenant d'employés mécontents, de volontaires infiltrés ou de partenaires ayant des motivations cachées, pouvant compromettre les systèmes et les données de l'organisation

Statistiques et tendances

- Incidents de cybersécurité touchant les organisations humanitaires
    - Attaques DDoS ciblant les sites web d'ONG
    - Compromission de comptes de messagerie et usurpation d'identité
    - Accès non autorisé aux bases de données sensibles
    - Divulgation d'informations personnelles des bénéficiaires et du personnel
    - Conséquences humanitaires des attaques sur les infrastructures critiques
    - Utilisation de l'information comme arme dans les conflits
    - Risque d'espionnage et de manipulation de l'information par des acteurs étatiques

- Types d'attaques courantes (ransomware, phishing, etc.)
    - Ransomware : ex. WannaCry, NotPetya, Locky
    - Phishing : emails frauduleux usurpant l'identité d'organisations légitimes
    - Attaques par force brute : tentatives d'accès par essais successifs de mots de passe
    - Malware : programmes malveillants visant à compromettre les systèmes informatiques
    - Attaques ciblées par des acteurs étatiques ou groupes soutenus par des États
    - Cyber-espionnage et vol d'informations sensibles
    - Sabotage et destruction de données

- Évolution des cybermenaces au fil du temps
    - Augmentation de l'automatisation des attaques

    - Cybercriminels plus sophistiqués et organisés
    - Utilisation accrue des réseaux sociaux pour mener des campagnes de désinformation
    - Croissance des attaques ciblant les appareils mobiles et l'Internet des Objets (IoT)
    - Implication croissante des acteurs étatiques et non étatiques
    - Cyber-conflits et utilisation de la cyberguerre comme instrument de pouvoir
    - Développement de nouvelles tactiques et techniques de cyberattaques

- Impact financier et opérationnel des cyberattaques
    - Coûts de récupération et de remédiation après une attaque réussie
    - Interruption des services et des opérations humanitaires
    - Perte de confiance des donateurs et des partenaires
    - Réputation endommagée et conséquences juridiques potentielles
    - Coûts indirects liés à la perte de confiance des populations bénéficiaires
    - Détournement de ressources pour faire face aux cyberattaques
    - Risques pour la sécurité des employés et des bénéficiaires en cas de divulgation d'informations sensibles

Cybersécurité dans différents contextes géopolitiques

- Contexte géopolitique et régional des cybermenaces
    - Tensions politiques et économiques exacerbent les risques de cyberattaques
    - États-nations impliqués dans les cyberattaques (p.ex. APT)
    - Groupes cybercriminels localisés dans certaines régions
    - Acteurs non étatiques et groupes terroristes exploitant le cyberespace

- Menaces spécifiques aux régions où les organisations humanitaires opèrent
    - Afrique subsaharienne (🚧 Verify data)
        - Fraude et escroqueries en ligne (p.ex. arnaques "Nigérianes")
        - Cyberattaques ciblant les infrastructures critiques (p.ex. installations médicales, réseaux de distribution d'eau et d'électricité)

        - Attaques par ransomware visant les organisations humanitaires
    - Moyen-Orient et Afrique du Nord (🚧 Verify data)
        - Cyberespionnage lié aux conflits régionaux (p.ex. surveillance des communications des organisations humanitaires)
        - Attaques ciblées contre les défenseurs des droits de l'homme et les organisations de la société civile
        - Utilisation de logiciels malveillants pour perturber les opérations humanitaires
    - Asie-Pacifique (🚧 Verify data)
        - Espionnage économique et industriel ciblant les technologies et les innovations humanitaires
        - Cyberattaques visant à compromettre les systèmes d'information des organisations humanitaires
        - Tentatives d'extorsion et de chantage en ligne visant les travailleurs humanitaires
    - Amérique latine et Caraïbes (🚧 Verify data)
        - Cybercriminalité organisée visant les données financières et personnelles des organisations humanitaires
        - Attaques ciblant les organisations luttant contre la corruption et le crime organisé
        - Menaces de cybersécurité liées à la violence politique et aux tensions sociales
    - Europe et Amérique du Nord (🚧 Verify data)
        - Attaques de phishing et d'ingénierie sociale visant les employés et les bénévoles d'organisations humanitaires
        - Cyberattaques ciblant les chaînes d'approvisionnement et les partenaires locaux des organisations humanitaires
        - Tentatives d'infiltration et de compromission des systèmes informatiques des organisations humanitaires

- Adaptation des stratégies en conséquence
    - Analyse des risques liés au contexte géopolitique et régional
    - Mise en place de mécanismes de défense adaptés aux menaces spécifiques
    - Coopération avec les autorités locales et les partenaires régionaux (si possible)

Coopération inter-organisationnelle pour renforcer la cybersécurité

- Importance de la coopération et du partage d'informations entre organisations pour lutter efficacement contre les cybermenaces
  - Échange d'informations sur les menaces et les vulnérabilités
  - Amélioration de la compréhension des tendances et des tactiques des attaquants
  - Renforcement de la résilience collective face aux cyberattaques
  - Facilitation de la réponse aux incidents et de la récupération après une attaque

- Mécanismes de coopération et de partage d'informations existants (🚧 Verify data)
  - Computer Emergency Response Teams (CERTs) nationaux et sectoriels
  - Plateformes de partage d'informations sur les menaces (ex: ISACs, MISP)
  - Groupes de travail et forums spécialisés (ex: FIRST, GFCE)
  - Accords de coopération bilatéraux et multilatéraux entre organisations
  - Initiatives soutenues par les Nations Unies et d'autres organisations internationales

- Exemples de collaborations réussies entre organisations pour renforcer la cybersécurité (🚧 Verify data)
  - ex: Collaboration entre les CERTs pour démanteler des réseaux de cybercriminalité
  - ex: Élaboration conjointe de normes et de bonnes pratiques (ex: NIST, ISO)
  - ex: Campagnes de sensibilisation et de formation inter-organisationnelles
  - ex: Coordination des efforts de réponse aux incidents à grande échelle
  - ex: Partage d'outils et de ressources pour améliorer la capacité de détection et de défense

Appel à l'action

- Responsabilité des dirigeants et des parties prenantes
  - Comprendre les menaces et les risques liés à la cybersécurité pour leur organisation
  - Mettre en place des politiques de cybersécurité adaptées

    - Allouer des ressources pour la cybersécurité (budget, personnel, formation)
    - S'assurer que les employés comprennent leur rôle dans la protection des données et des systèmes
    - Favoriser une culture de la cybersécurité au sein de l'organisation
    - Sensibiliser les employés aux enjeux géopolitiques liés à la cybersécurité
    - S'engager dans des dialogues avec des partenaires internationaux pour améliorer la cybersécurité

- Importance de la cybersécurité dans la stratégie organisationnelle
    - Prévenir les pertes financières dues aux cyberattaques
    - Protéger la réputation de l'organisation et la confiance des donateurs
    - Assurer la continuité des opérations et la capacité de fournir de l'aide
    - Protéger les données sensibles des bénéficiaires et des employés
    - Répondre aux exigences légales et réglementaires en matière de protection des données
    - Prévenir les atteintes aux droits de l'homme liées à des failles de cybersécurité
    - Renforcer la résilience de l'organisation face aux cybermenaces dans un contexte géopolitique complexe

- Coopération et partage d'informations entre organisations
    - Établir des partenariats avec d'autres ONG et des experts en cybersécurité
    - Participer à des plateformes d'échange d'informations sur les menaces (ex: CERT, ISAC)
    - Coordonner les efforts pour lutter contre les cybermenaces communes
    - Partager les meilleures pratiques et les leçons apprises en matière de cybersécurité
    - Créer des alliances régionales ou sectorielles pour renforcer la cybersécurité
    - Collaborer avec des organisations gouvernementales et intergouvernementales pour partager des informations
    - Développer des normes et des protocoles communs pour faciliter la coopération et le partage d'informations en matière de cybersécurité

Questions pour le public 🔥

- Quelles sont vos préoccupations majeures en matière de cybersécurité dans votre organisation ?
- Avez-vous déjà été confronté à une cyberattaque ? Comment votre organisation a-t-elle réagi ?
- Quelles mesures votre organisation a-t-elle mises en place pour faire face aux cybermenaces spécifiques aux organisations humanitaires ?
- Comment votre organisation travaille-t-elle avec d'autres parties prenantes pour renforcer la cybersécurité ?

Conseils pratiques pour sécuriser votre organisation et les organisations partenaires

Défis de la cybersécurité pour les dirigeants

- Responsabilités des dirigeants en matière de cybersécurité
  - Établir une politique de cybersécurité claire et cohérente
  - S'assurer de la conformité aux réglementations et normes en vigueur
  - Désigner un responsable de la cybersécurité au sein de l'organisation
  - Sensibiliser et former l'ensemble du personnel à la cybersécurité
- Évaluation des risques et gestion des vulnérabilités
  - Identifier les actifs numériques critiques (systèmes, réseaux, données)
  - Effectuer des analyses de risques régulières
  - Prioriser les actions de remédiation en fonction de l'impact potentiel
  - Mettre en place un processus de gestion des vulnérabilités pour corriger les failles de sécurité
- Communication et collaboration interne et externe, y compris avec d'autres organisations humanitaires pour le partage d'informations sur les menaces et les bonnes pratiques
  - Mettre en place des canaux de communication sécurisés pour partager les informations sensibles
  - Établir des protocoles de communication avec d'autres organisations humanitaires
  - Participer à des forums de partage d'informations sur les menaces et les bonnes pratiques

- Investissements stratégiques en cybersécurité pour améliorer la capacité de coopération et de partage d'informations
    - Allouer des ressources suffisantes pour assurer la protection des systèmes et des données
    - Investir dans des technologies de cybersécurité adaptées aux besoins de l'organisation
    - Évaluer le retour sur investissement des initiatives de cybersécurité en termes de réduction des risques
- Mise en place d'une gouvernance de la cybersécurité pour favoriser une culture de la sécurité et de la coopération inter-organisationnelle
    - Créer un comité de cybersécurité incluant les représentants des différentes parties prenantes
    - Établir des procédures de suivi et de contrôle des mesures de cybersécurité
    - Promouvoir une culture de la sécurité et de la coopération inter-organisationnelle
    - Intégrer la cybersécurité dans la stratégie globale de l'organisation

Conseils ciblés pour les responsables de projets informatiques

- Utilisation des bonnes pratiques et des normes de sécurité
    - Adopter des normes telles que ISO 27001, NIST, et CIS Critical Security Controls
    - Mettre en œuvre des politiques de sécurité de l'information
    - Effectuer régulièrement des tests de vulnérabilité et des audits de sécurité
    - Appliquer le principe du moindre privilège pour les droits d'accès

- Gestion des accès et des identités
    - Utiliser l'authentification à deux facteurs (2FA) pour les comptes sensibles
    - Mettre en place un système de gestion des identités et des accès (IAM)
    - Superviser et auditer régulièrement les accès aux ressources sensibles
    - Révoquer rapidement les droits d'accès des employés qui quittent l'organisation

- Sécurisation des réseaux et des systèmes
    - Déployer des pare-feu, des systèmes de détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS)

    - Chiffrer les communications et les données sensibles
    - Appliquer régulièrement des correctifs de sécurité et maintenir les logiciels à jour
    - Segmenter le réseau pour isoler les systèmes

- Mise en place de mécanismes de détection et de réponse aux incidents
    - Mettre en place un centre d'opérations de sécurité (SOC)
    - Utiliser des outils de gestion des événements et des informations de sécurité (SIEM)
    - Définir et tester un plan de réponse aux incidents de cybersécurité
    - Effectuer une analyse post-incident pour améliorer les processus et les systèmes

- Gestion des fournisseurs et des partenaires tiers
    - Évaluer les risques de cybersécurité liés aux fournisseurs et aux partenaires
    - Inclure des clauses de cybersécurité dans les contrats et les accords de coopération
    - Auditer régulièrement les fournisseurs et les partenaires pour vérifier leur conformité aux normes de sécurité
    - Partager les informations sur les cybermenaces avec les partenaires et les organisations coopérantes

- Formation et sensibilisation du personnel technique
    - Proposer des formations sur les bonnes pratiques de sécurité et les outils spécifiques
    - Sensibiliser aux enjeux de la collaboration et du partage d'informations inter-organisation
    - Encourager la participation à des conférences et des ateliers sur la cybersécurité
    - Organiser des exercices pratiques pour renforcer les compétences techniques en matière de sécurité

Défis et opportunités de la collaboration inter-organisationnelle

- Importance de la coopération inter-organisationnelle et internationale dans la lutte contre les cybermenaces
    - Unir les efforts pour identifier et atténuer les menaces communes

    - Partager les ressources et les compétences pour améliorer la capacité de réponse aux incidents
    - Faciliter l'échange de bonnes pratiques et de connaissances en matière de cybersécurité

- Opportunités de la collaboration pour renforcer la résilience de l'ensemble du secteur humanitaire face aux cybermenaces
    - Développer des capacités de détection et de réponse aux incidents plus efficaces
    - Mettre en place des stratégies de cybersécurité coordonnées et cohérentes
    - Bénéficier d'un soutien technique et financier pour renforcer la cybersécurité des organisations

- Défis potentiels liés au partage d'informations sensibles et à la coordination entre organisations
    - Préserver la confidentialité et la sécurité des informations partagées
    - Gérer les différences juridiques et réglementaires entre les pays et les organisations
    - Établir la confiance entre les parties prenantes pour favoriser la coopération

- Bonnes pratiques et mécanismes existants pour le partage d'informations et la collaboration
    - Plateformes d'échange d'informations sur les menaces (ex : CERT, ISAC)
    - Groupes de travail et réseaux spécialisés dans la cybersécurité (ex : FIRST, GFCE)
    - Protocoles et formats standardisés pour le partage d'informations (ex : STIX, TAXII)

- Études de cas et exemples de collaboration réussie dans le domaine de la cybersécurité
    - 🚧 FIXME: trouver exemples

- Identification de partenaires potentiels pour la coopération en matière de cybersécurité
    - Organisations gouvernementales et non gouvernementales spécialisées dans la cybersécurité
    - Entreprises privées et fournisseurs de services de sécurité

    - Groupes de recherche et universités travaillant sur les questions de cybersécurité
    - Autres organisations humanitaires et partenaires du secteur

Plan d'action de 3 mois pour améliorer immédiatement la cybersécurité au sein de votre organisation

- Mise en place d'un comité de cybersécurité
    - Identifier les membres clés de l'organisation (direction, IT, juridique, RH)
    - Définir les rôles et responsabilités de chaque membre
    - Planifier des réunions régulières pour discuter des enjeux de cybersécurité
    - Coordonner les efforts de cybersécurité entre les différentes parties prenantes

- Réalisation d'un audit de cybersécurité initial
    - Inventorier les actifs informatiques et les informations sensibles
    - Évaluer les vulnérabilités et les risques associés
    - Identifier les failles de sécurité dans les infrastructures, les processus et les politiques
    - Prioriser les actions correctives en fonction des risques

- Élaboration et mise en œuvre de politiques et de procédures de cybersécurité
    - Rédiger des politiques claires sur la gestion des données et des accès
    - Établir des procédures pour la sécurisation des équipements et des réseaux
    - Mettre en place des processus de gestion des incidents de cybersécurité
    - Intégrer la cybersécurité dans les pratiques de gestion des fournisseurs et partenaires

- Formation et sensibilisation du personnel à la cybersécurité
    - Évaluer les besoins en formation et en sensibilisation du personnel
    - Concevoir des formations spécifiques pour les différents groupes cibles
    - Utiliser des méthodes interactives pour renforcer l'apprentissage (ateliers, simulations)

    - Mesurer l'efficacité des formations et ajuster le contenu en conséquence

- Renforcement de la sécurité des infrastructures critiques
    - Mettre à jour les systèmes d'exploitation et les logiciels pour corriger les vulnérabilités
    - Configurer les pare-feu et les systèmes de détection d'intrusion
    - Chiffrer les données sensibles et les communications
    - Mettre en place des contrôles d'accès et de l'authentification forte

- Planification et réalisation d'exercices de réponse aux incidents
    - Élaborer des scénarios d'incidents de cybersécurité (phishing, ransomware, intrusion)
    - Impliquer les membres du comité de cybersécurité et les parties prenantes concernées
    - Organiser des exercices de simulation pour tester les procédures et les réactions
    - Analyser les résultats et identifier les améliorations nécessaires

- Suivi et évaluation des progrès en matière de cybersécurité
    - Mettre en place des indicateurs clés de performance pour mesurer les progrès
    - Effectuer des audits de cybersécurité réguliers pour identifier les nouvelles vulnérabilités
    - Collecter des retours d'expérience et partager les leçons apprises
    - Ajuster les politiques, les procédures et les formations en fonction des évolutions du contexte et des menaces

Sensibilisation et formation du personnel à la cybersécurité

Importance de la sensibilisation

- Rôle clé du personnel dans la sécurité de l'organisation
    - Prise de décisions éclairées en matière de cybersécurité
    - Application des politiques et procédures de sécurité
    - Détection et signalement des incidents de sécurité
    - Participation aux exercices de réponse aux incidents

    - Collaboration avec les partenaires et les parties prenantes pour renforcer la sécurité

- Les risques liés à l'erreur humaine et au manque de formation
    - Clics sur des liens malveillants ou ouverture de pièces jointes infectées
    - Utilisation de mots de passe faibles ou réutilisés
    - Divulgation involontaire d'informations sensibles
    - Installation de logiciels non autorisés ou de dispositifs non sécurisés
    - Non-respect des politiques et procédures de sécurité

- L'impact des incidents de cybersécurité sur les organisations humanitaires
    - Interruption des opérations et des services essentiels
    - Perte de données sensibles et de la confiance des donateurs et bénéficiaires
    - Conséquences financières, juridiques et réputationnelles
    - Détournement de ressources pour la réponse aux incidents et la remédiation
    - Risques pour la sécurité des employés et des bénéficiaires

- Renforcer la culture de la sécurité au sein de l'organisation
    - Sensibilisation et formation continues du personnel
    - Responsabilisation des dirigeants et des employés
    - Communication claire et transparente sur les enjeux de sécurité
    - Mise en place d'un environnement de travail sécurisé et axé sur la prévention
    - Encouragement à la coopération interne et externe pour renforcer la résilience face aux cybermenaces

Programmes de formation et de sensibilisation

- Évaluation des besoins en formation et en sensibilisation
    - Identifier les groupes cibles (dirigeants, personnel technique, personnel non technique)
    - Évaluer les connaissances existantes et les lacunes
- Élaboration de programmes de formation adaptés
    - Formation initiale pour les nouveaux employés

        - Formation continue et actualisation des connaissances
        - Modules de formation spécifiques aux rôles et aux responsabilités
    - Techniques et méthodes de sensibilisation
        - Ateliers et séminaires
        - Simulations et exercices pratiques
        - Supports de communication et campagnes internes
    - Mesure de l'efficacité des programmes de formation et de sensibilisation
        - Suivi des indicateurs clés de performance
        - Évaluation régulière et ajustements
        - Retour d'expérience et partage des leçons apprises
    - Ressources et partenariats pour la formation en cybersécurité
        - Utilisation de plateformes et de ressources en ligne
        - Collaboration avec des experts et des organisations spécialisées
        - Coopération interorganisationnelle et échange de bonnes pratiques

GPT4 PROMPTS

> COMMAND: Simply write "Hello. I'm ready" if you are ready to answer expert-level technical questions in french.
>
> COMMAND: Réponds "OK." si tu prends bien cela en compte.
>
> COMMAND: GEOPOLY, peux-tu critiquer le PROGRAMME DE LA CONFERENCE au regard du context de lévènement? Précise à chaque fois ce que tu changerais, ce que tu amplifierais, ce que tu ajusterais.
>
> COMMAND: Super! Merci pour ça. Reste dans le cadre du PROGRAMME DE LA CONFERENCE et reformule le chapitre concerné par ta proposition « FIXME »