Cybersecurity in the Humanitarian Sector

HNPW 2023 – Geneva

DATA FRIENDLY SPACE

bold code_

Before starting

DATA FRIENDLY SPACE

bold code_

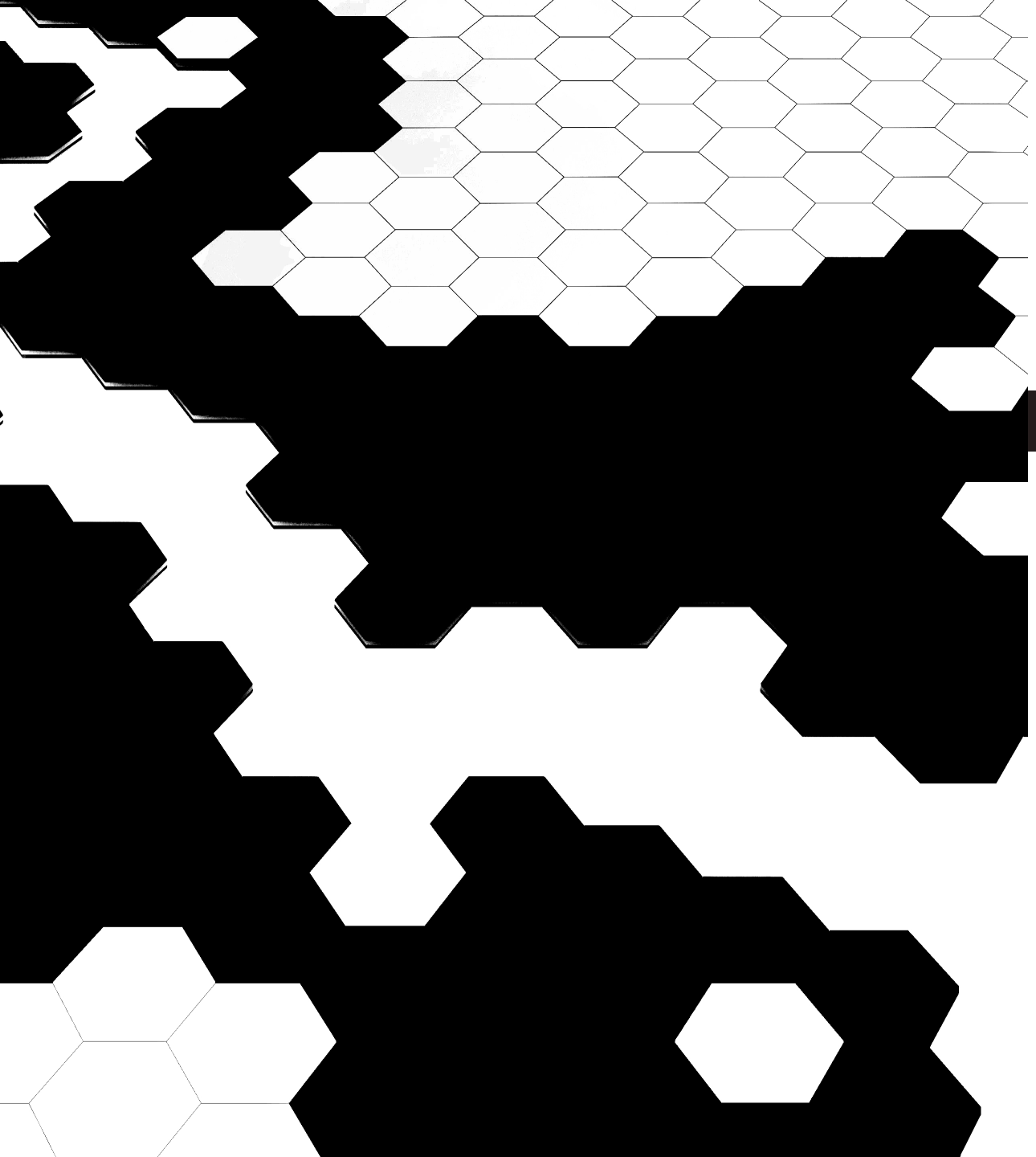
Agenda

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

What about you?

> 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 ✋



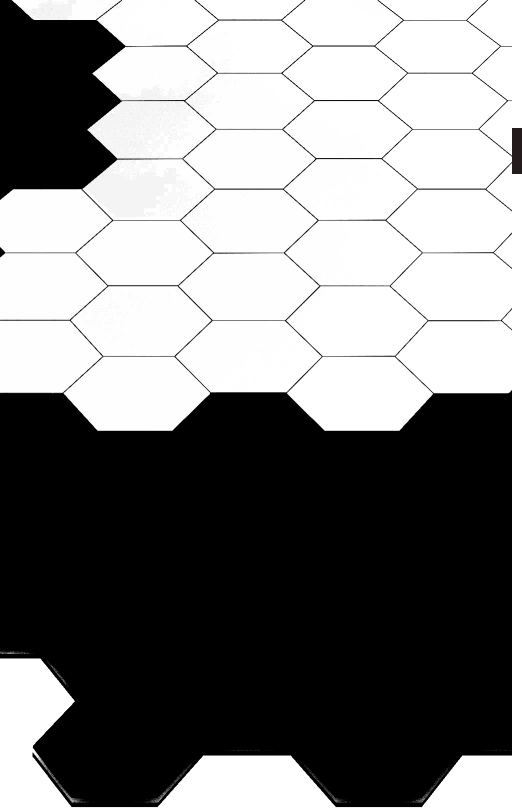
Current cyber threats and trends

Understanding the challenges for humanitarian organizations

Particular threats to humanitarian and international organizations

Nature of sensitive data and information

- **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

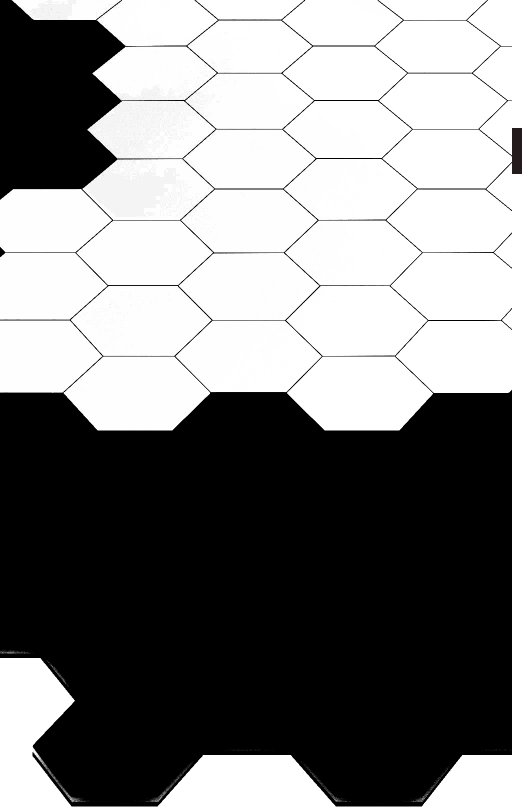


Potentially vulnerable infrastructure and networks

- **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- **Outdated or unpatched IT** infrastructure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**

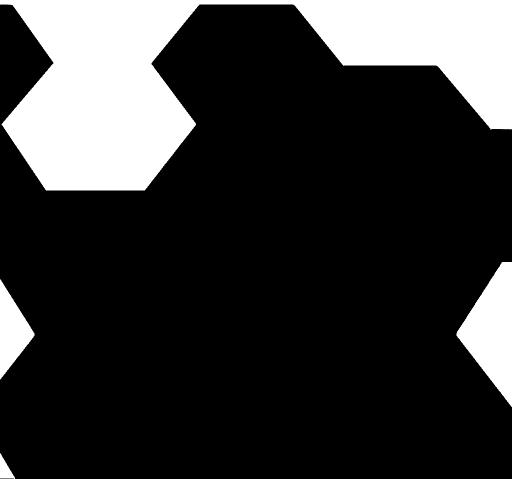
Collaboration with various partners and stakeholders

- **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

- **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

- **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

Cybersecurity incidents affecting humanitarian organizations

- **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.)

- **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

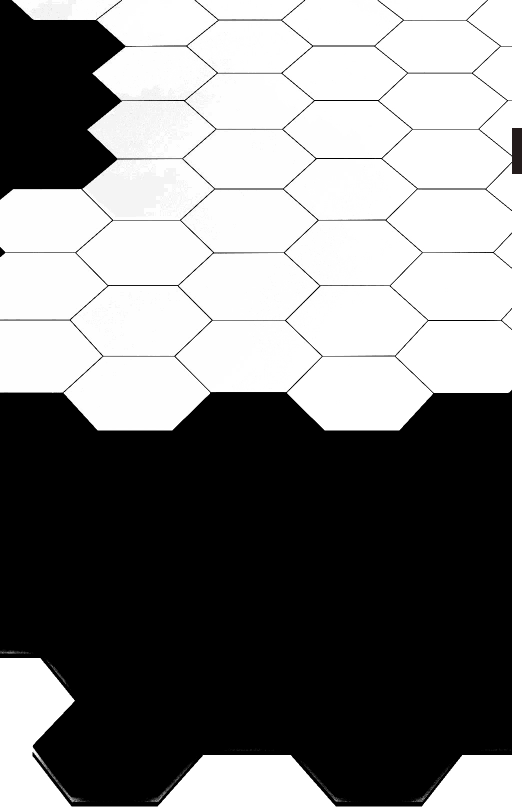
Evolution of cyber threats over time

- **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

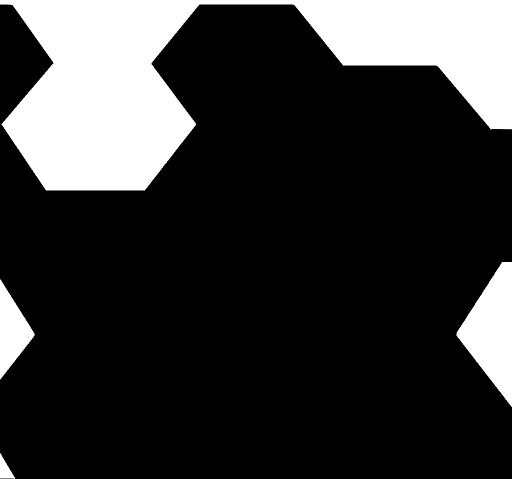
- **Recovery and remediation costs** after a successful attack
- **Disruption of humanitarian services** and operations
- **Loss of donor and partner confidence**
- **Damaged reputation** and potential legal consequences
- Indirect costs related to **loss of trust of beneficiary populations**
- **Diversion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

Cyber security in different geopolitical contexts



Geopolitical and regional context of cyber threats

- **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

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

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

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

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

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

- **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

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

- **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

- 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

- 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

Leadership and stakeholder accountability

- **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

- 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

- **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

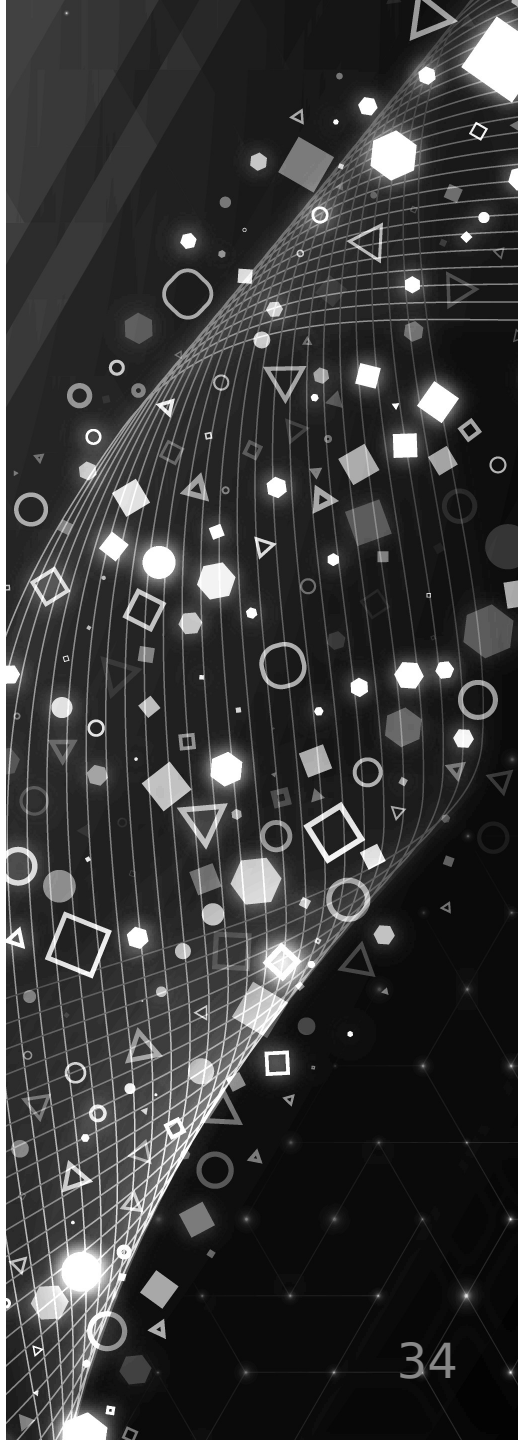
Questions for the audience

- **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?

Practical tips

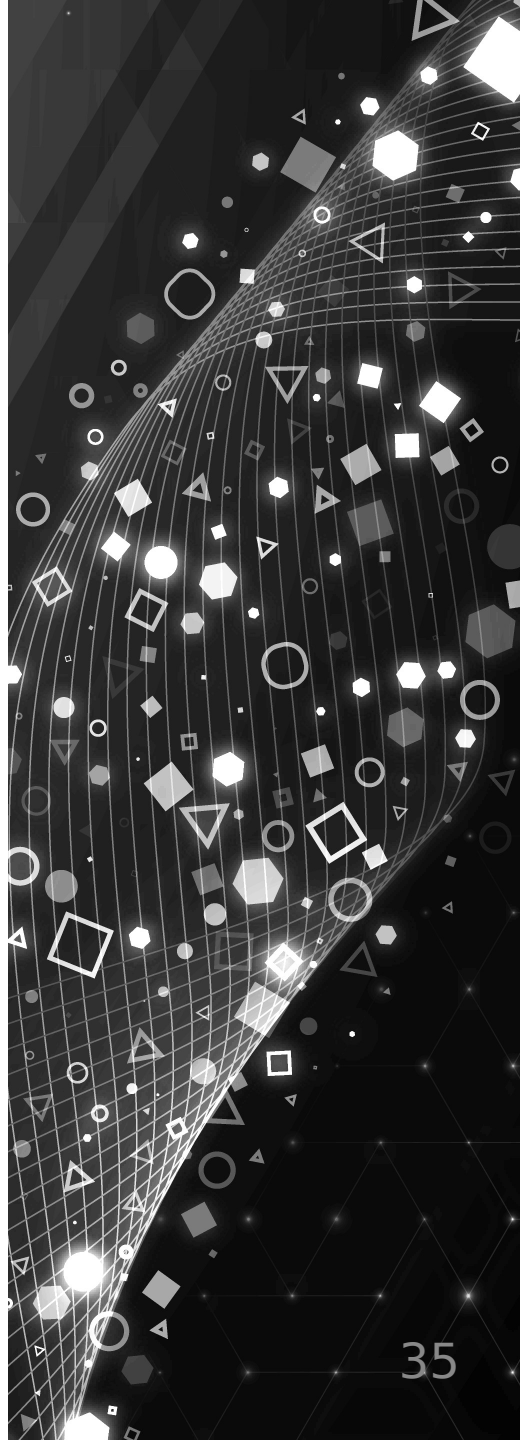
... for securing your organization and partner organizations

Cybersecurity challenges for organization leaders



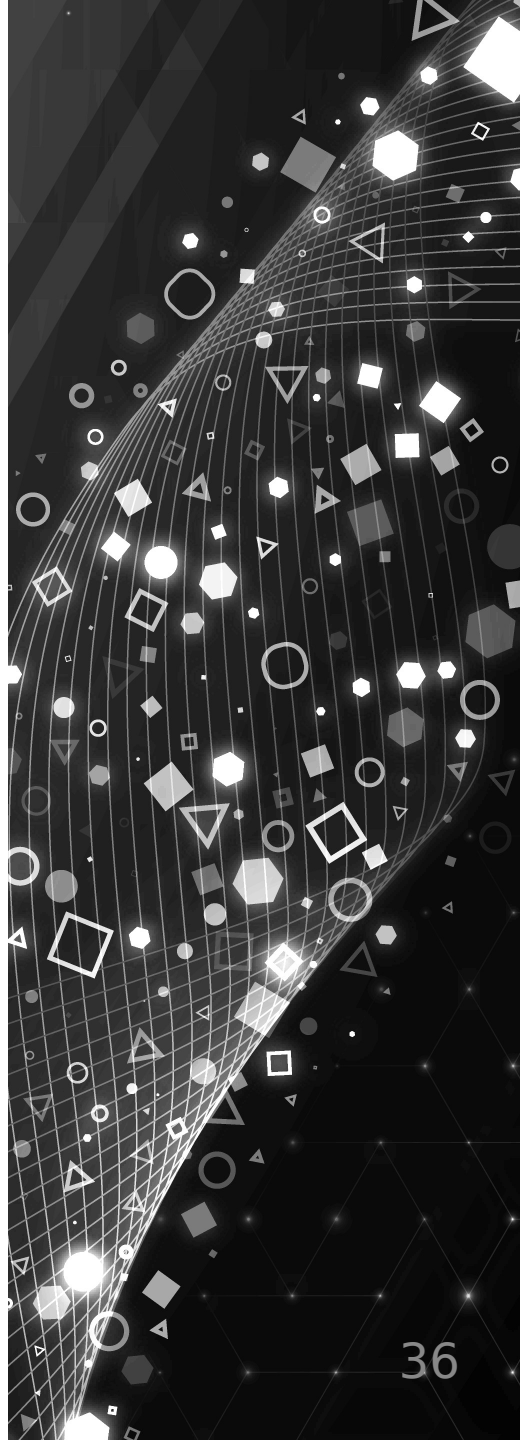
Leadership responsibilities for cybersecurity

- **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**



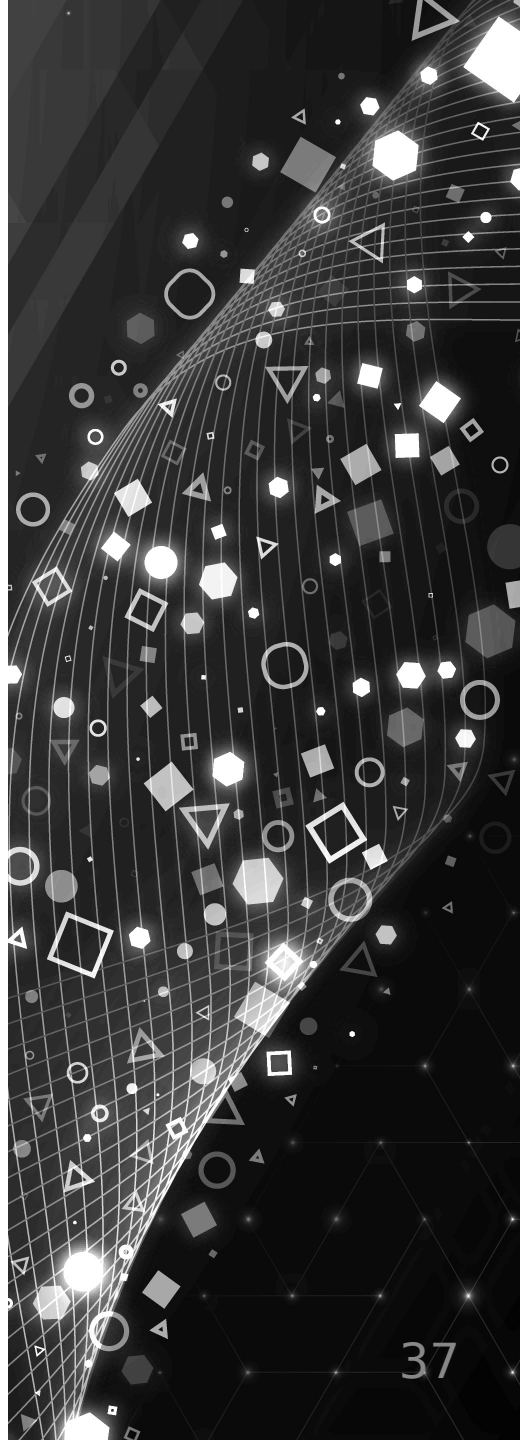
Risk assessment and vulnerability management

- **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



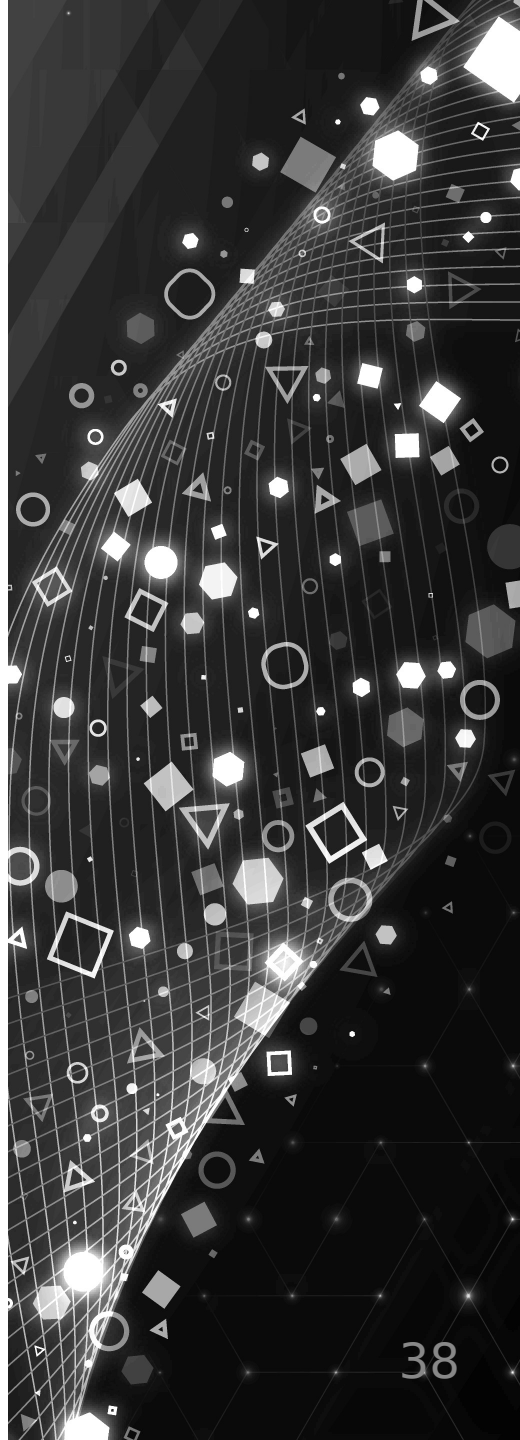
Communication and collaboration, to share information on threats and best practices

- **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



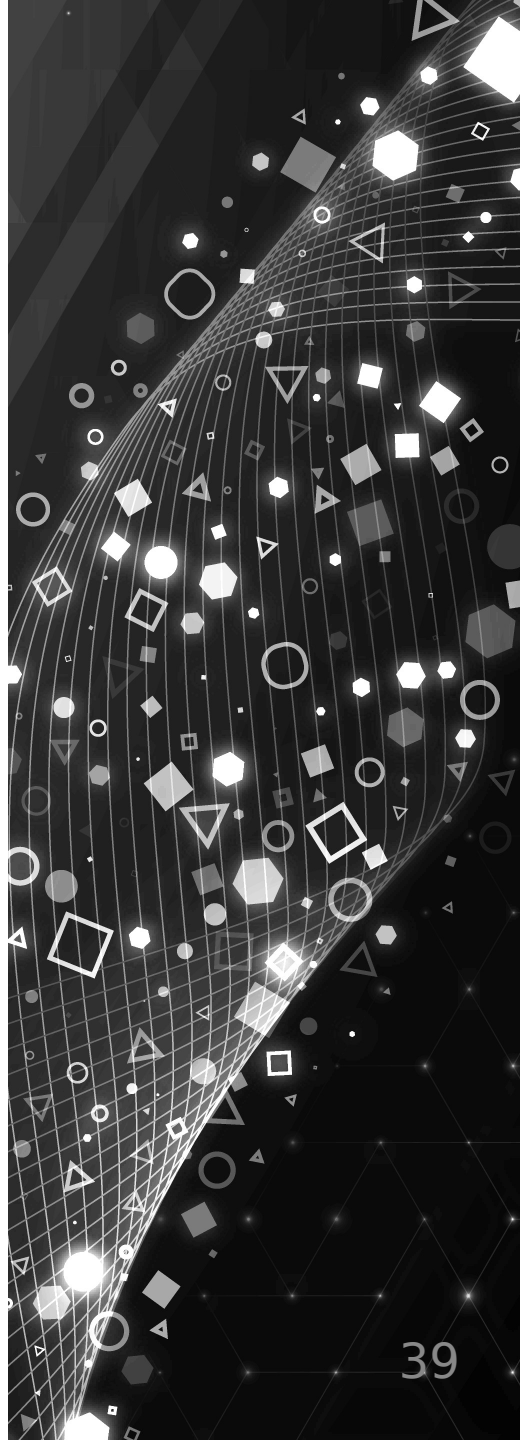
Strategic investments in cybersecurity to improve cooperation and information sharing capacity

- **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**

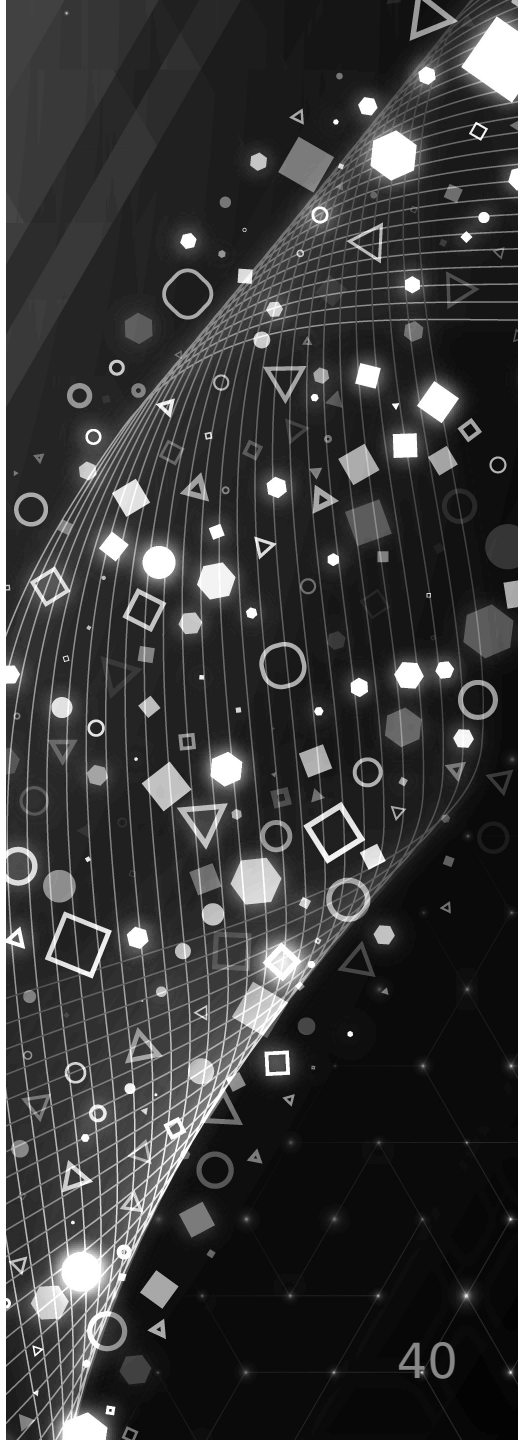


Establish cybersecurity governance to foster a culture of security and inter-organizational cooperation

- 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

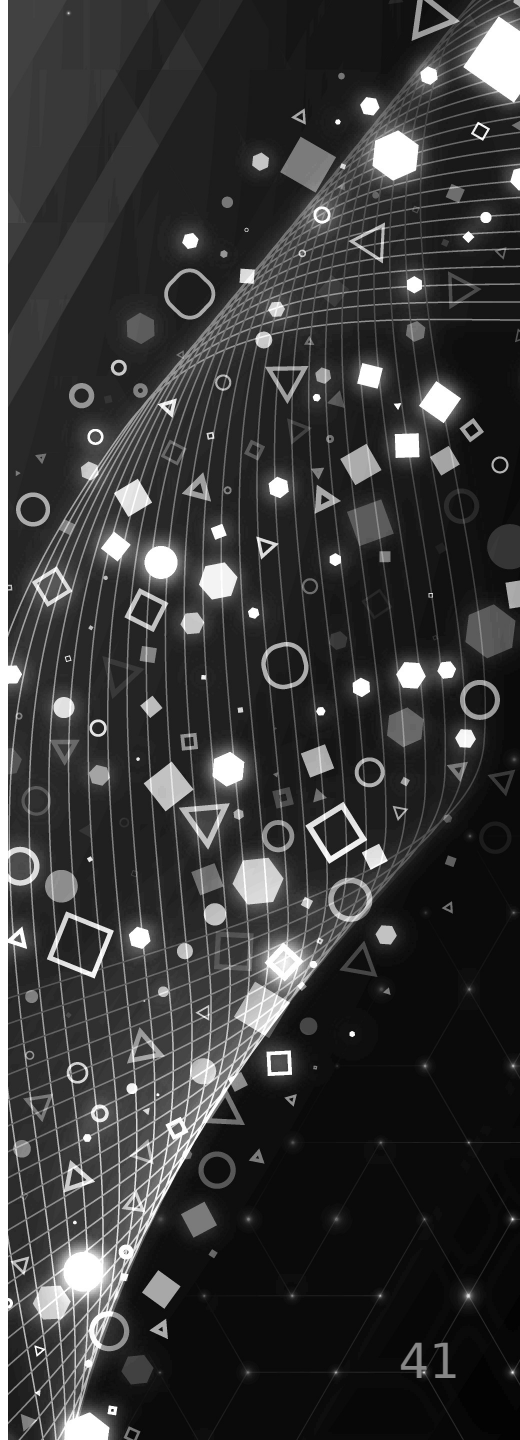


Targeted advice for IT project managers



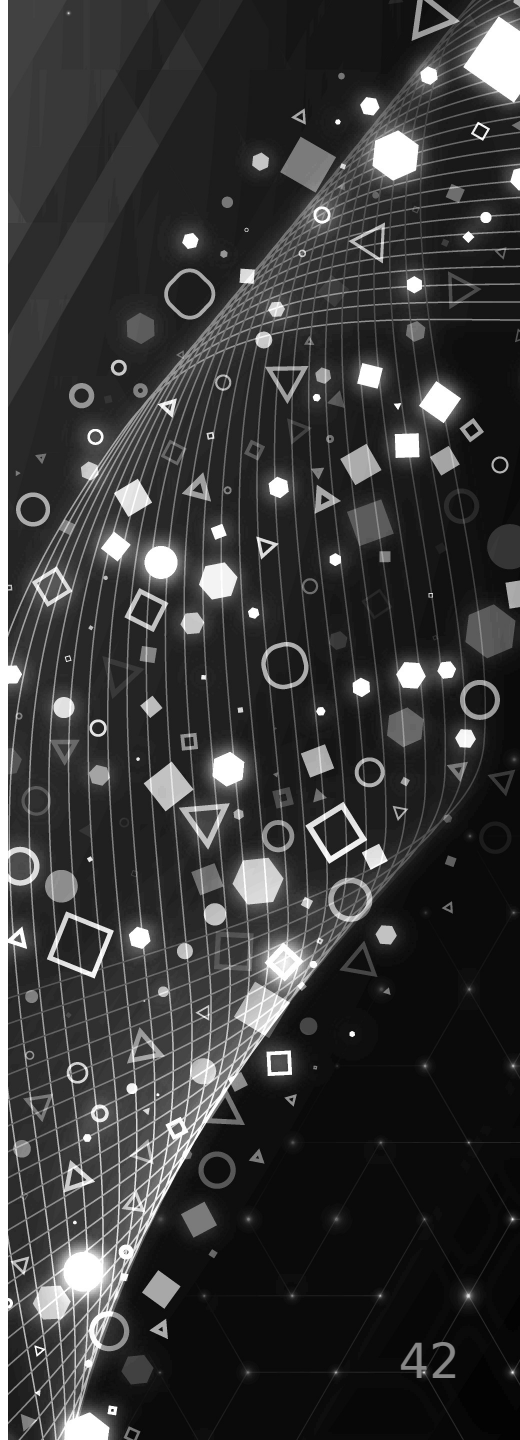
Use of best practices and security standards

- **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**



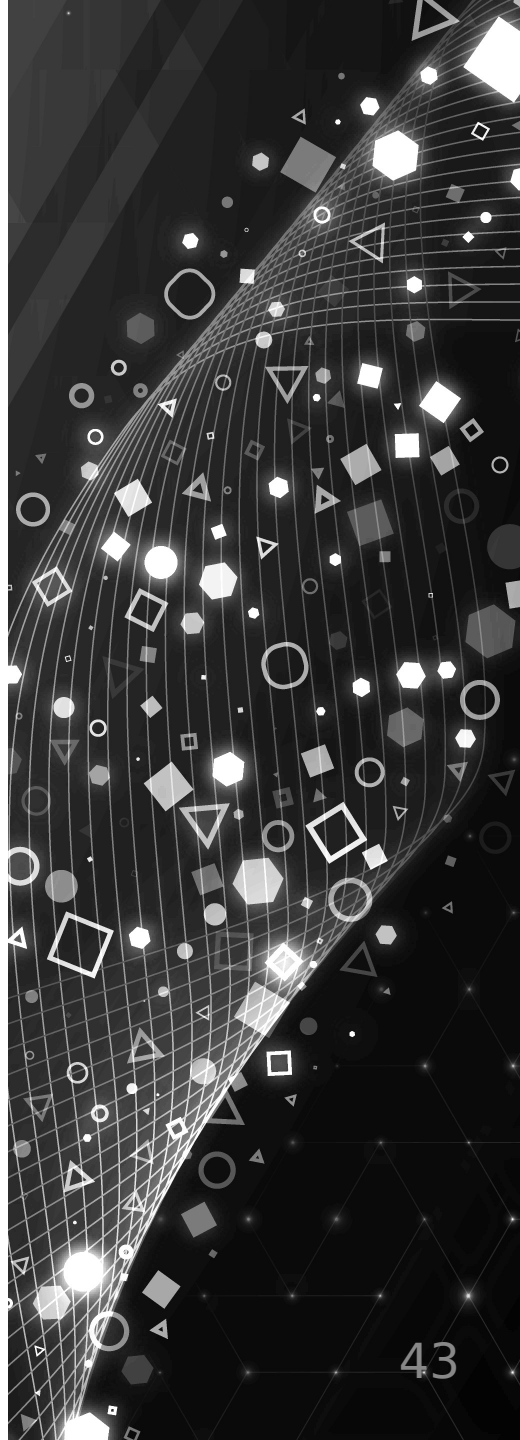
Access and identity management

- **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



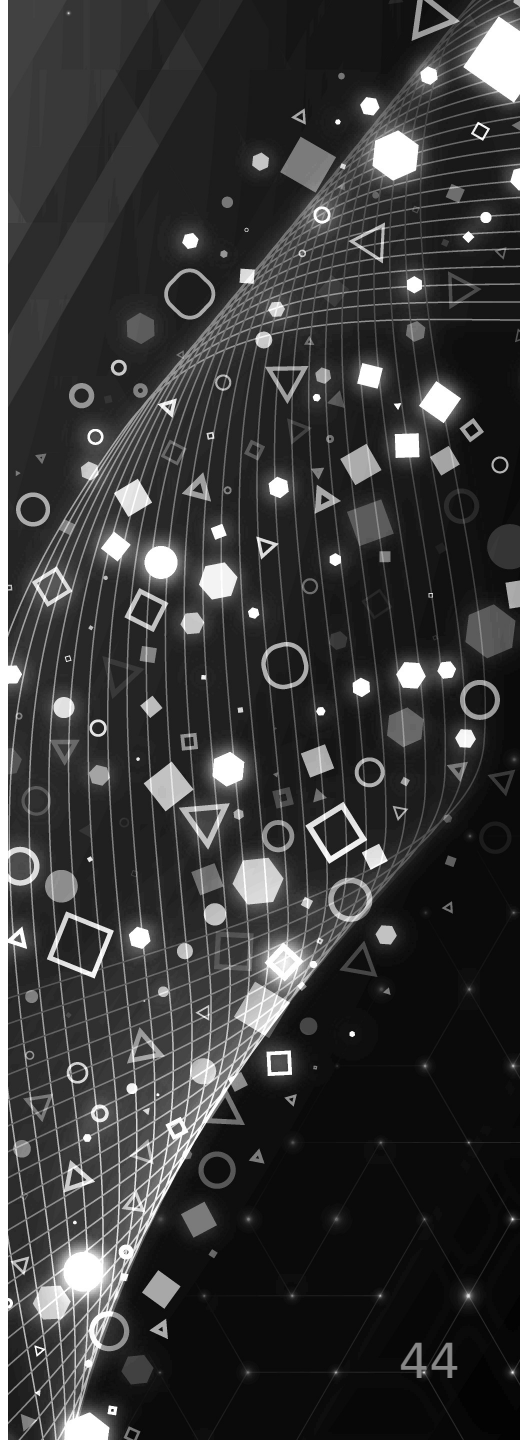
Securing networks and systems

- 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**



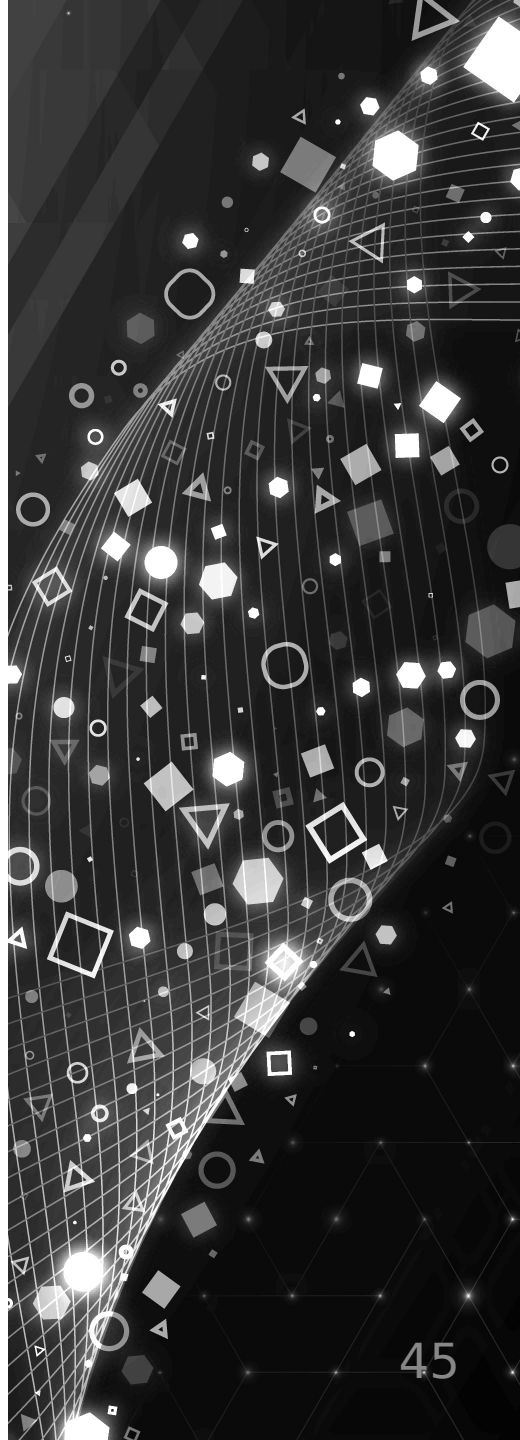
Implement incident detection and response mechanisms

- 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



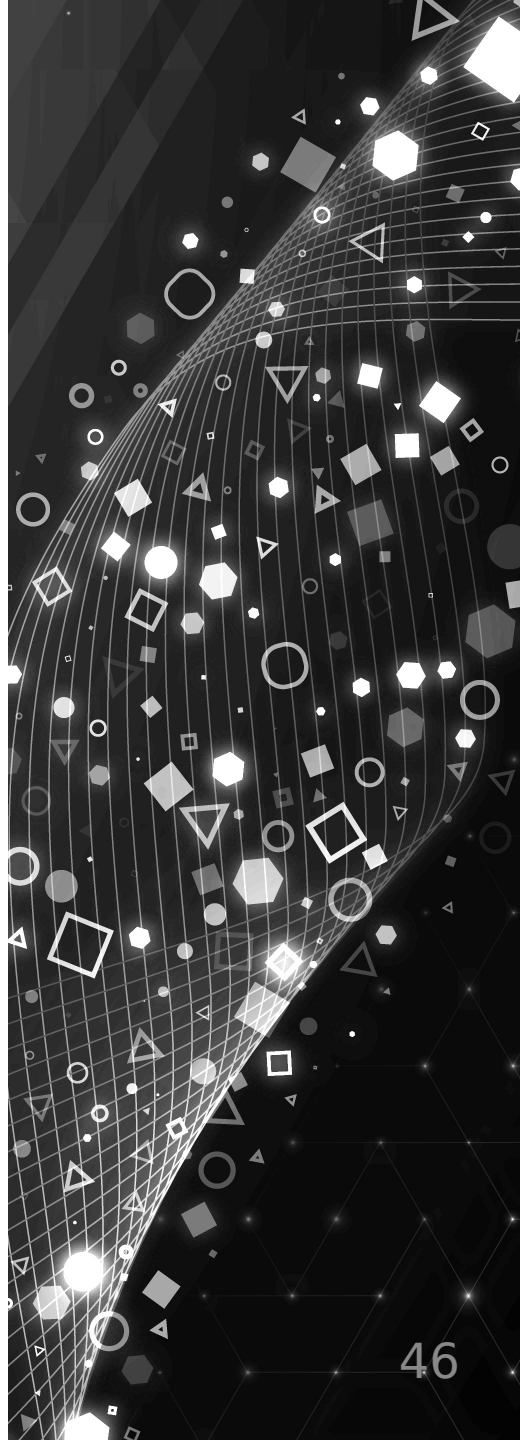
Manage third party vendors and partners

- **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



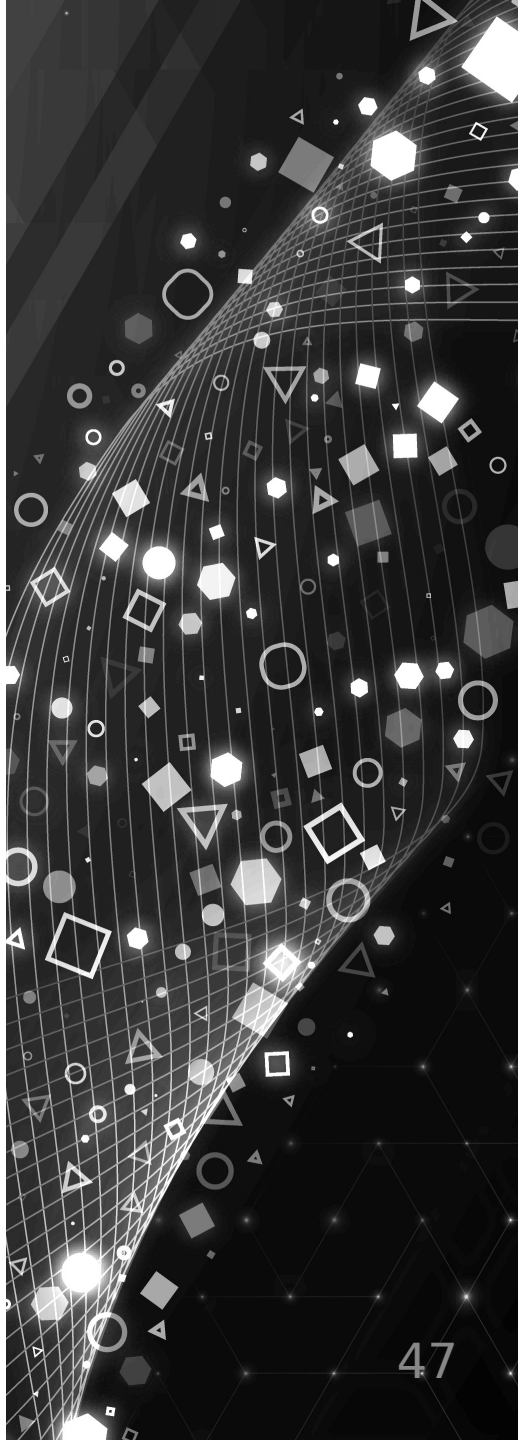
Training and awareness of technical staff

- 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



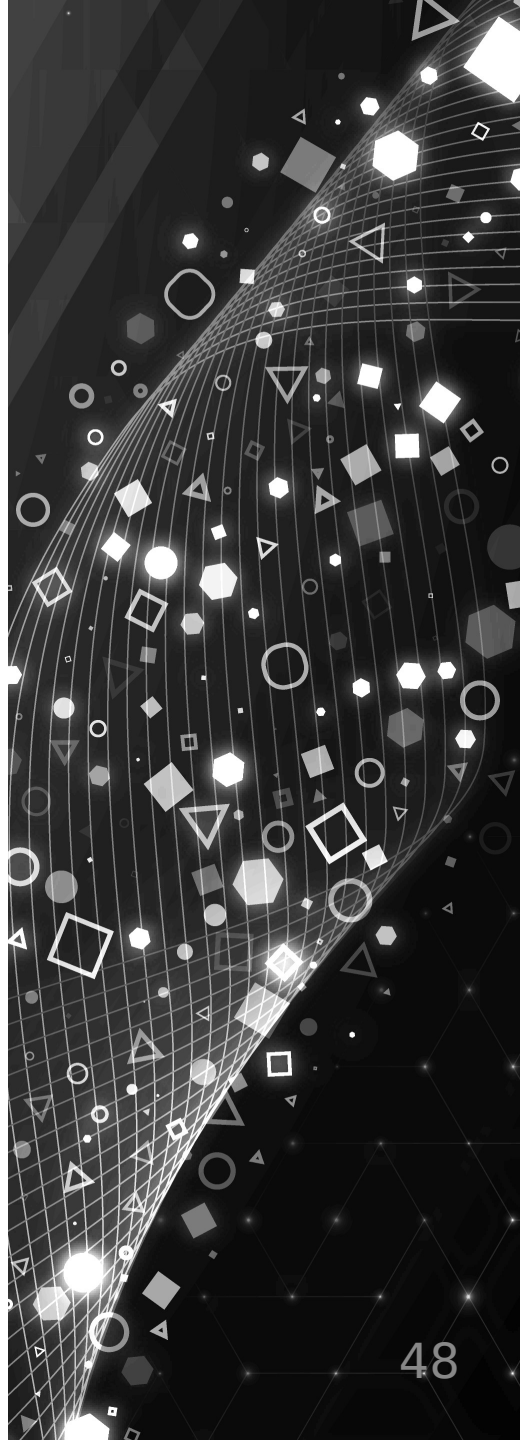
3-month action plan...

... to immediately improve cybersecurity in your organization



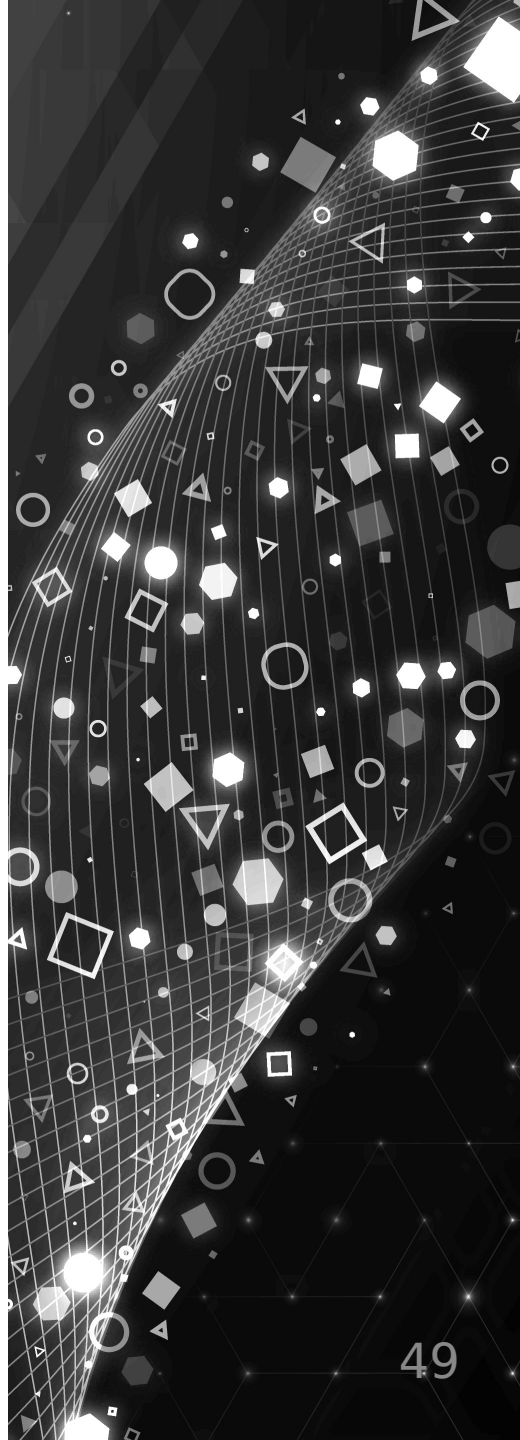
Establish a cybersecurity committee

- 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



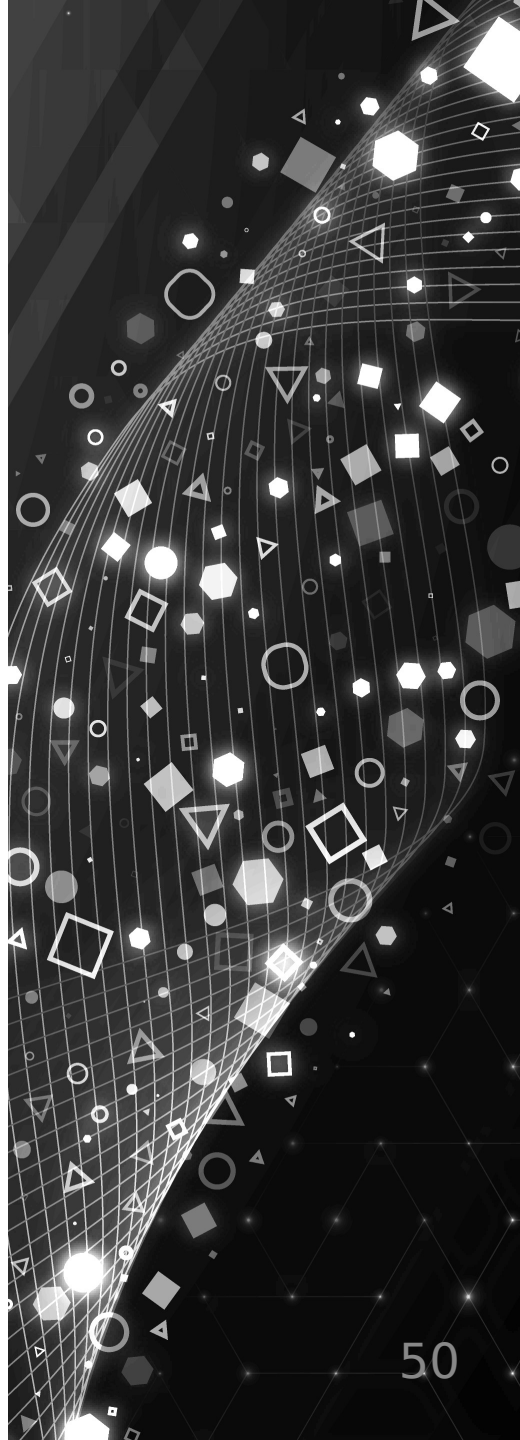
Conduct an initial cybersecurity audit

- 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



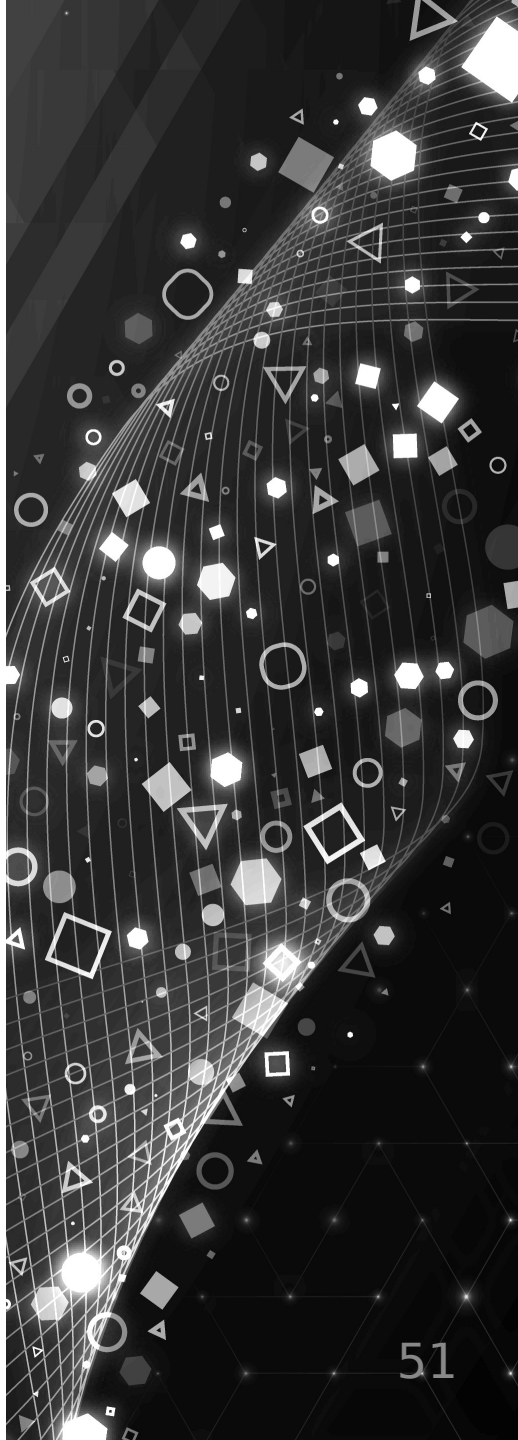
Develop and implement cybersecurity policies and procedures

- 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



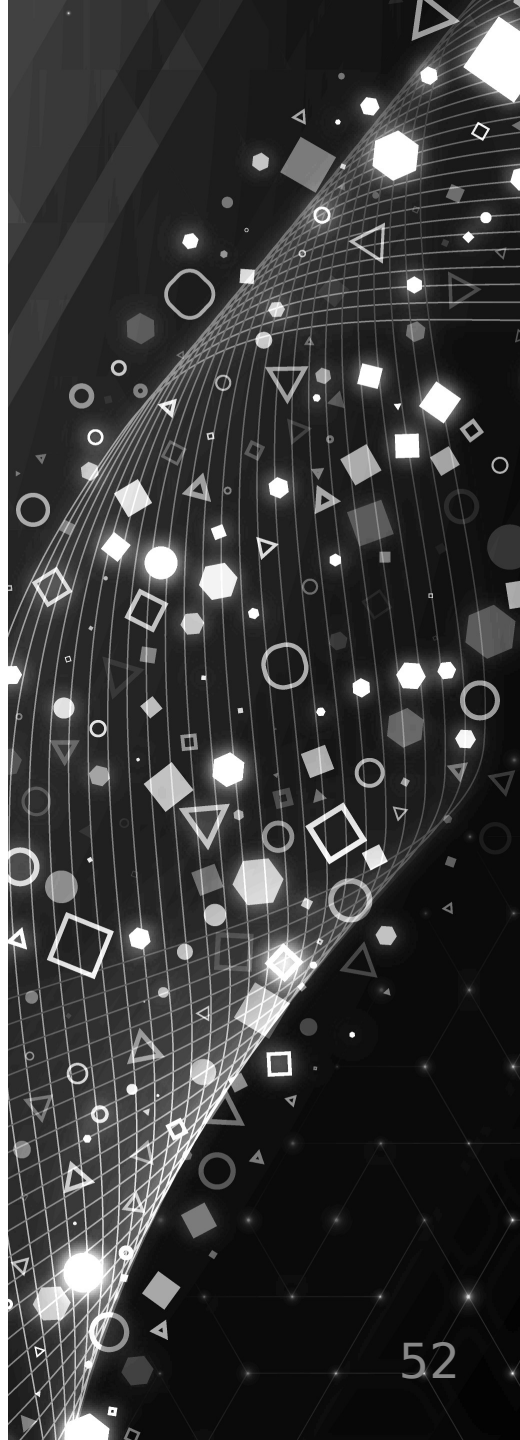
Training and awareness of personnel on cybersecurity

- 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



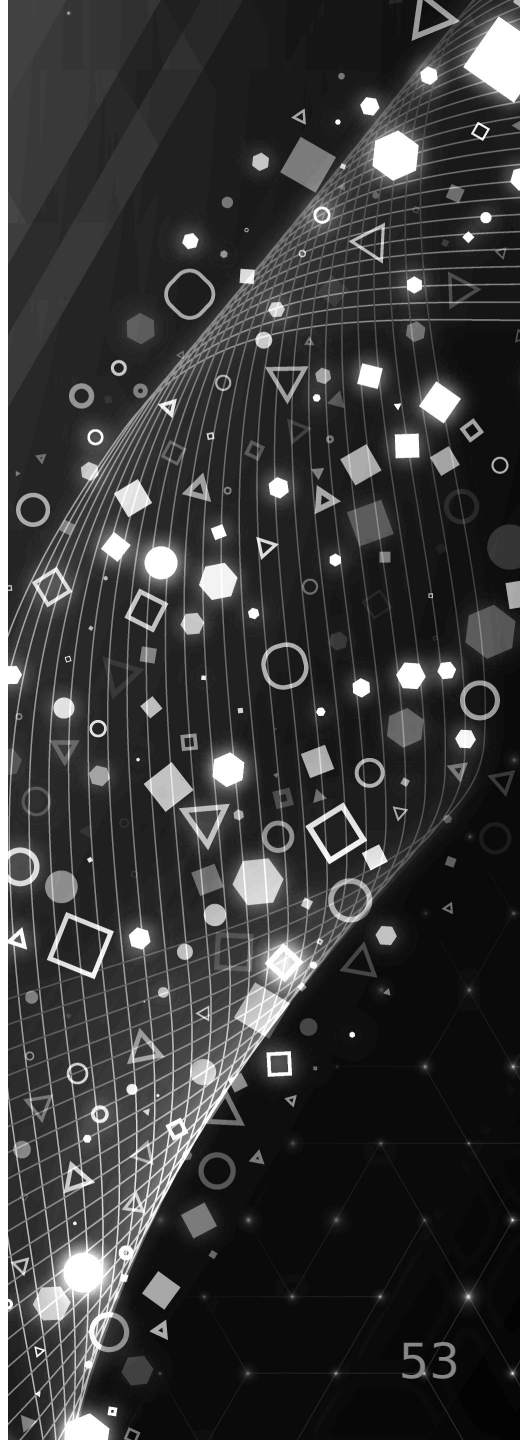
Strengthen the security of critical infrastructure

- 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



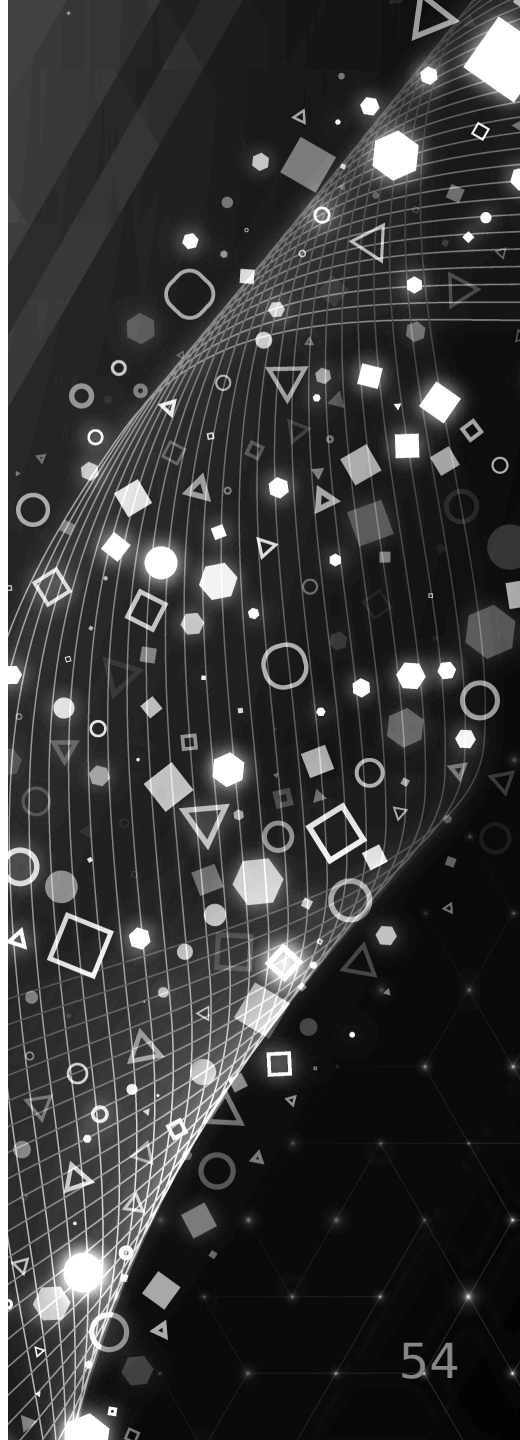
Planning and conducting incident response exercises

- 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



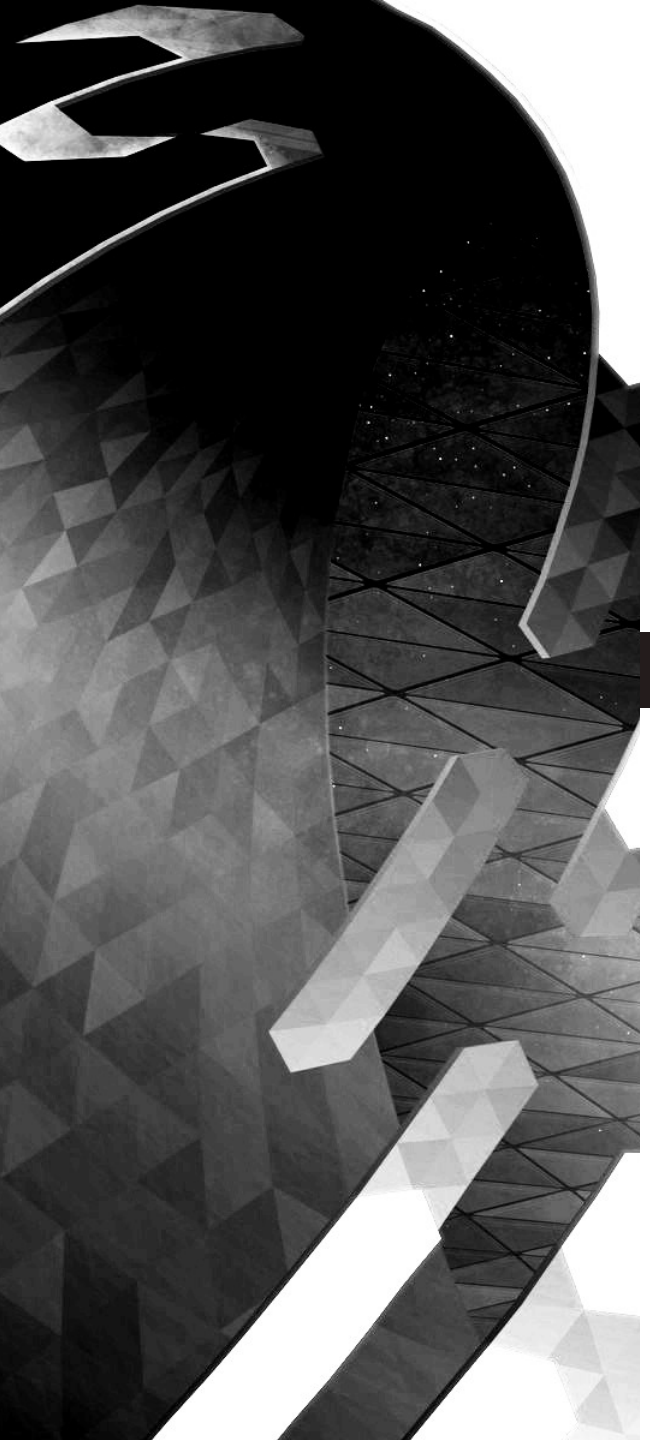
Monitor and evaluate cybersecurity progress

- 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

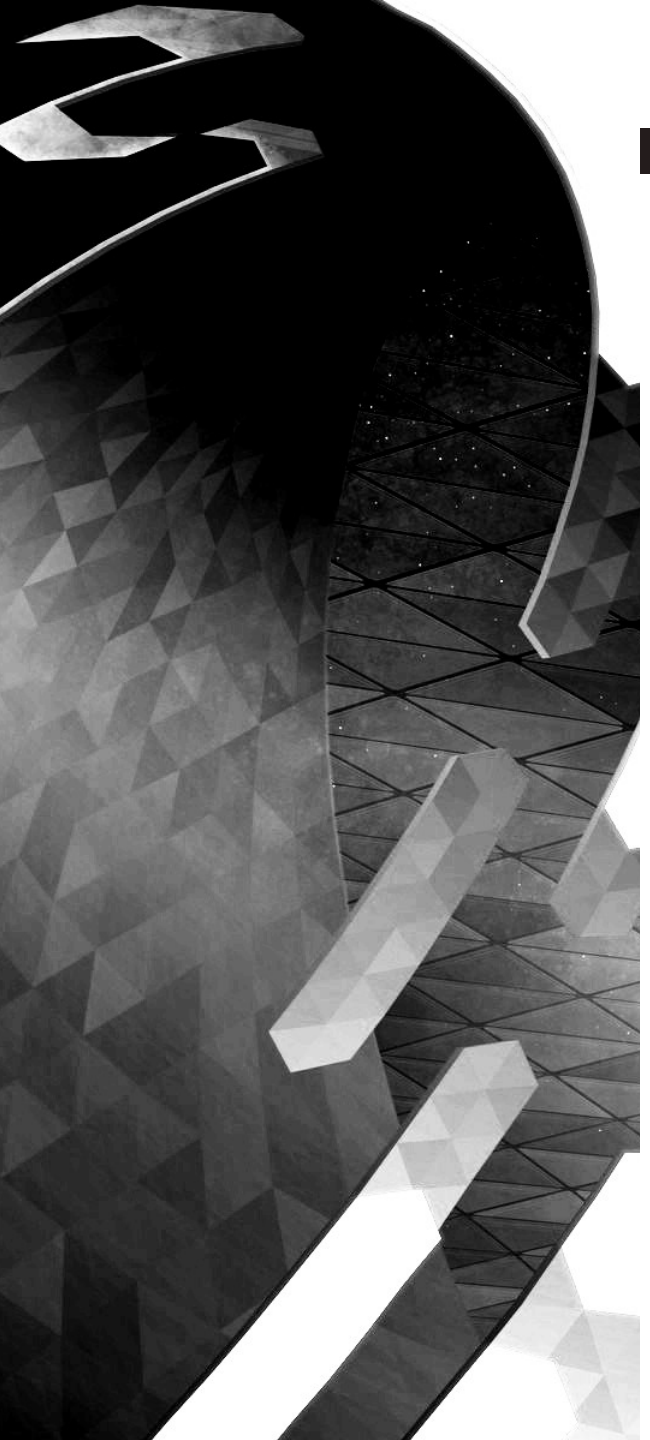


Awareness and training

... of humanitarian personnel in cybersecurity

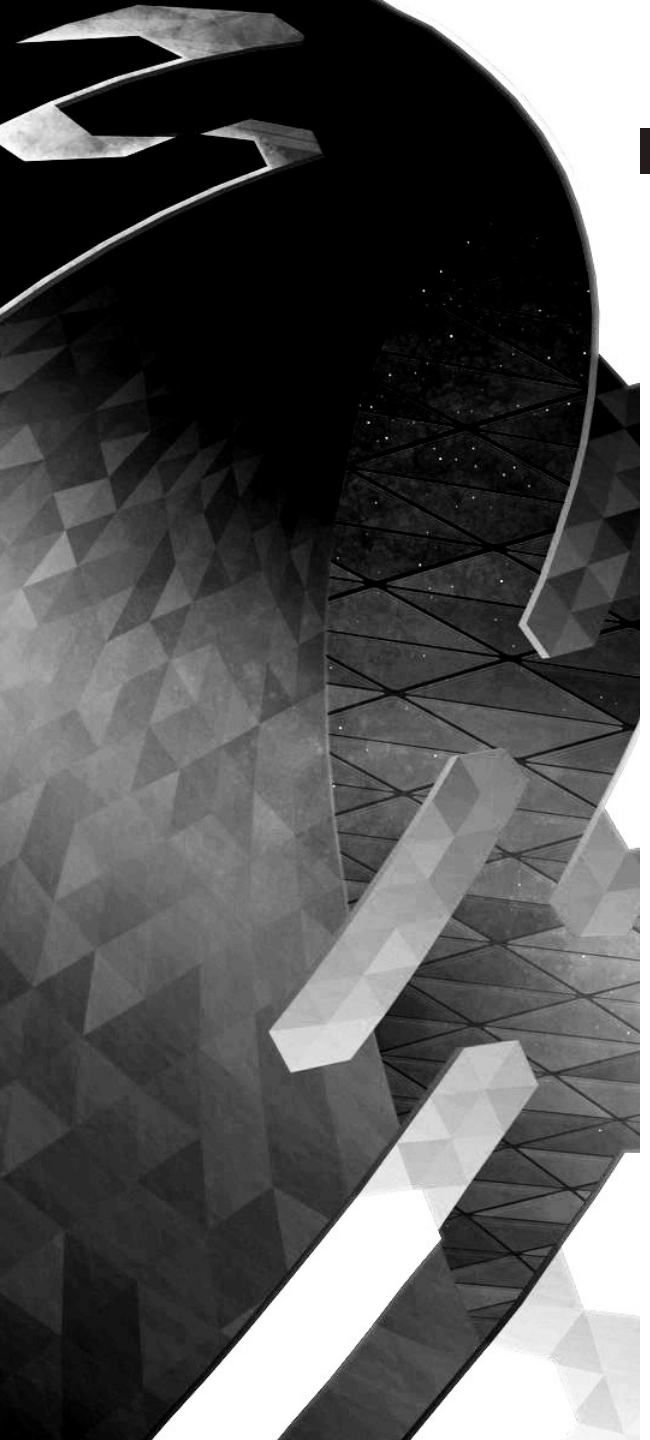


Importance of awareness



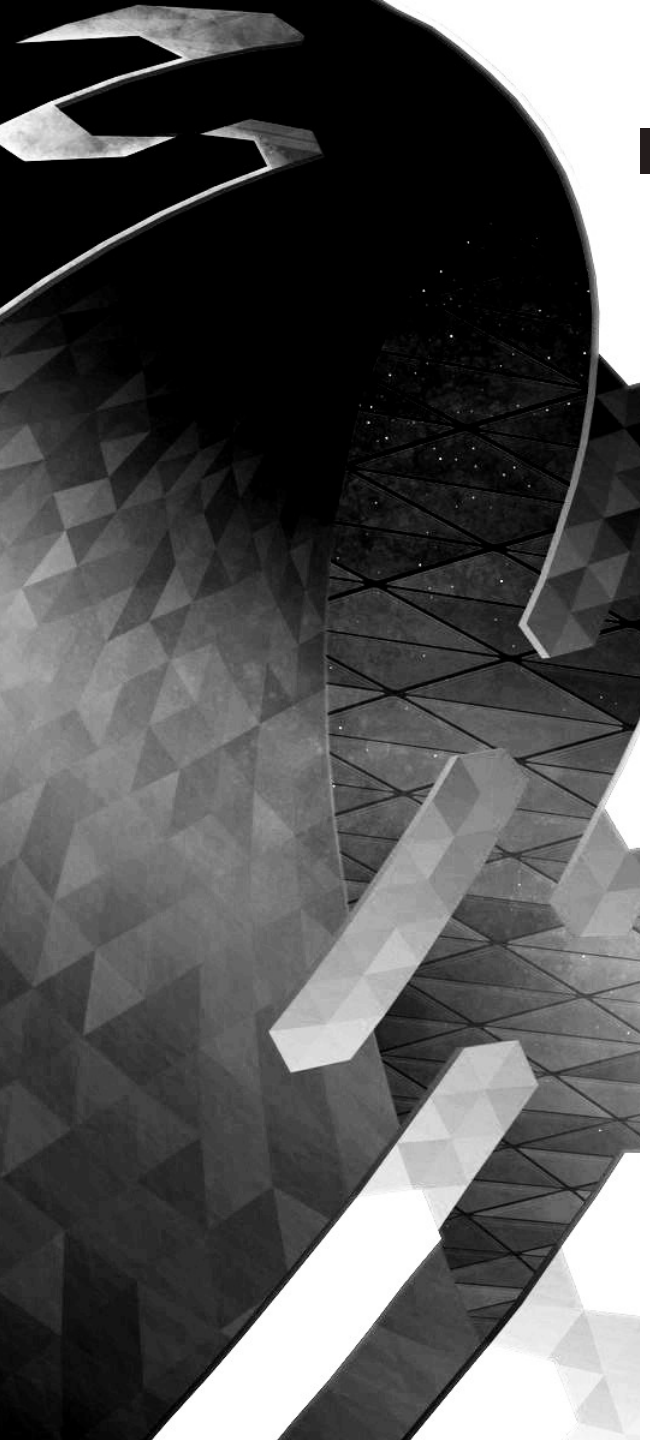
Key role of staff in the security of the organization

- **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



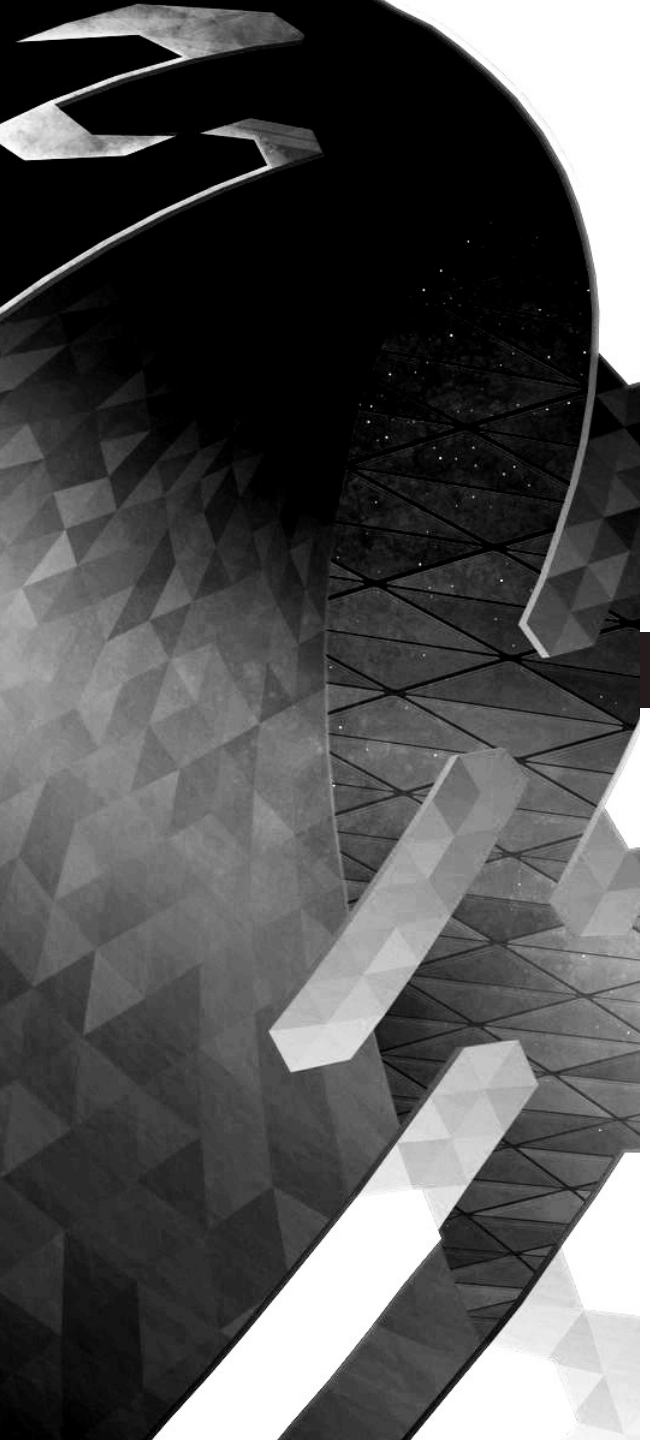
Risks related to human error and lack of training

- 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

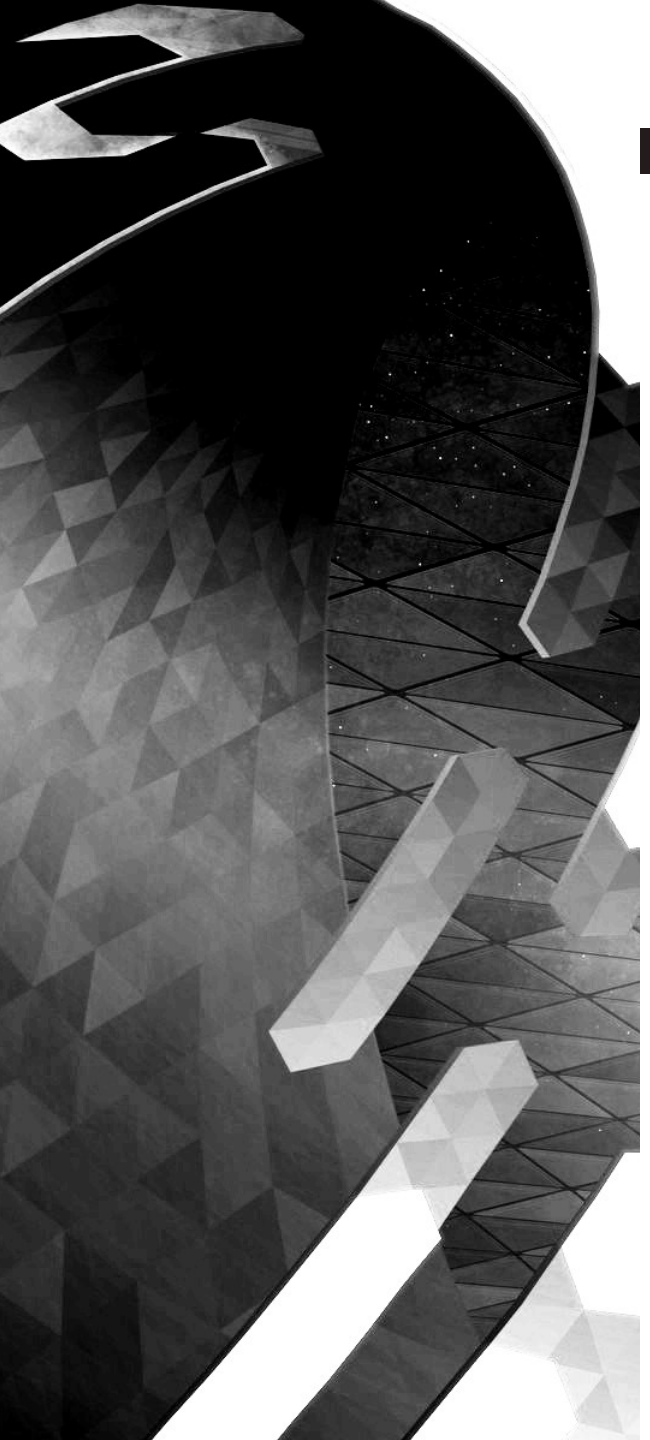


Strengthening the culture of safety within the organization

- 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

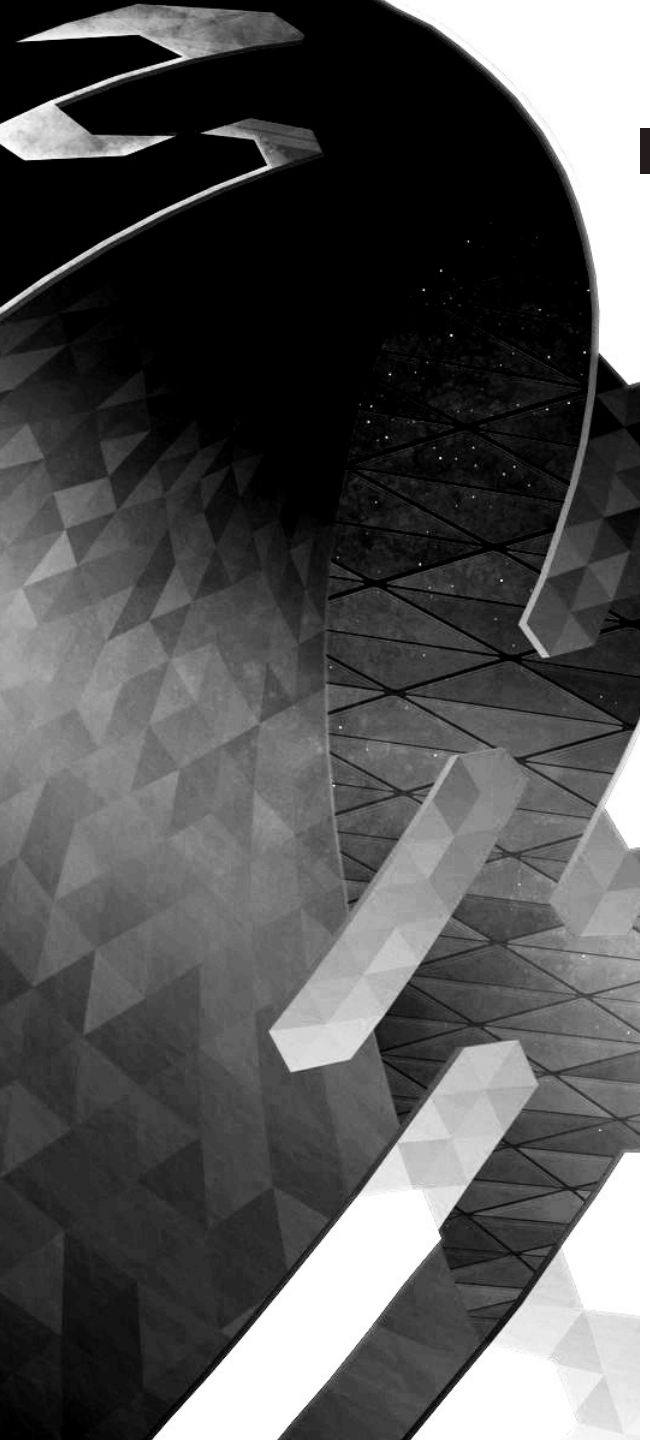


Training and awareness programs



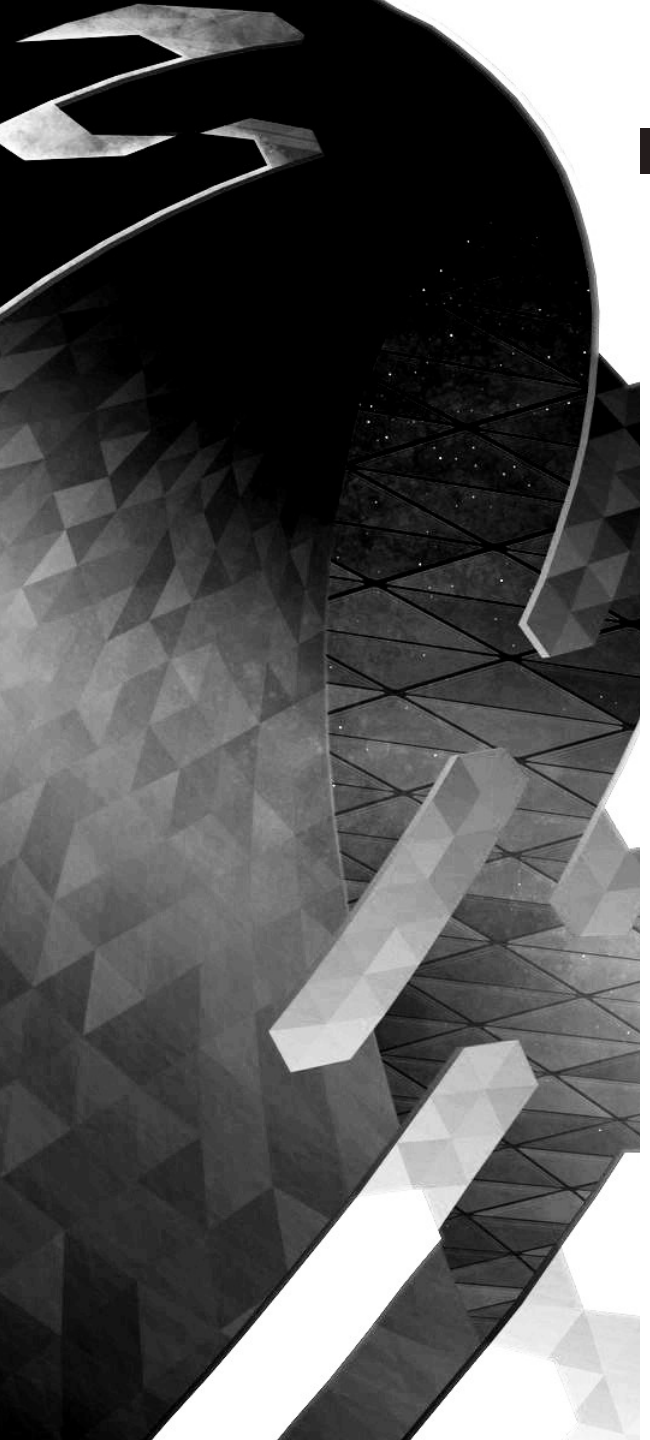
Assess training and awareness needs

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



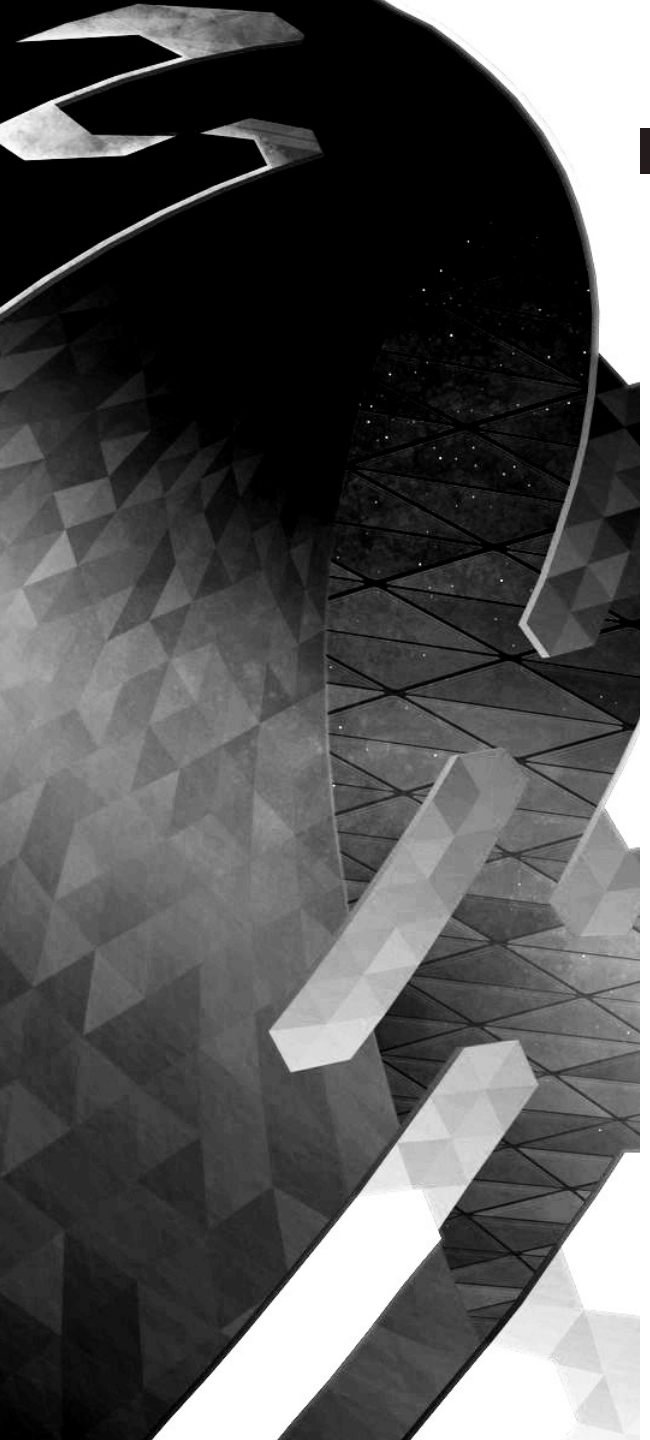
Development of customized training programs

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



Awareness techniques and methods

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



Measuring the effectiveness of training and awareness programs

- Monitoring of key performance indicators
- Regular evaluation and adjustments
- Feedback and sharing of lessons learned

Thank you for your attention!

Any questions ?