Aviation Cybersecurity Culture

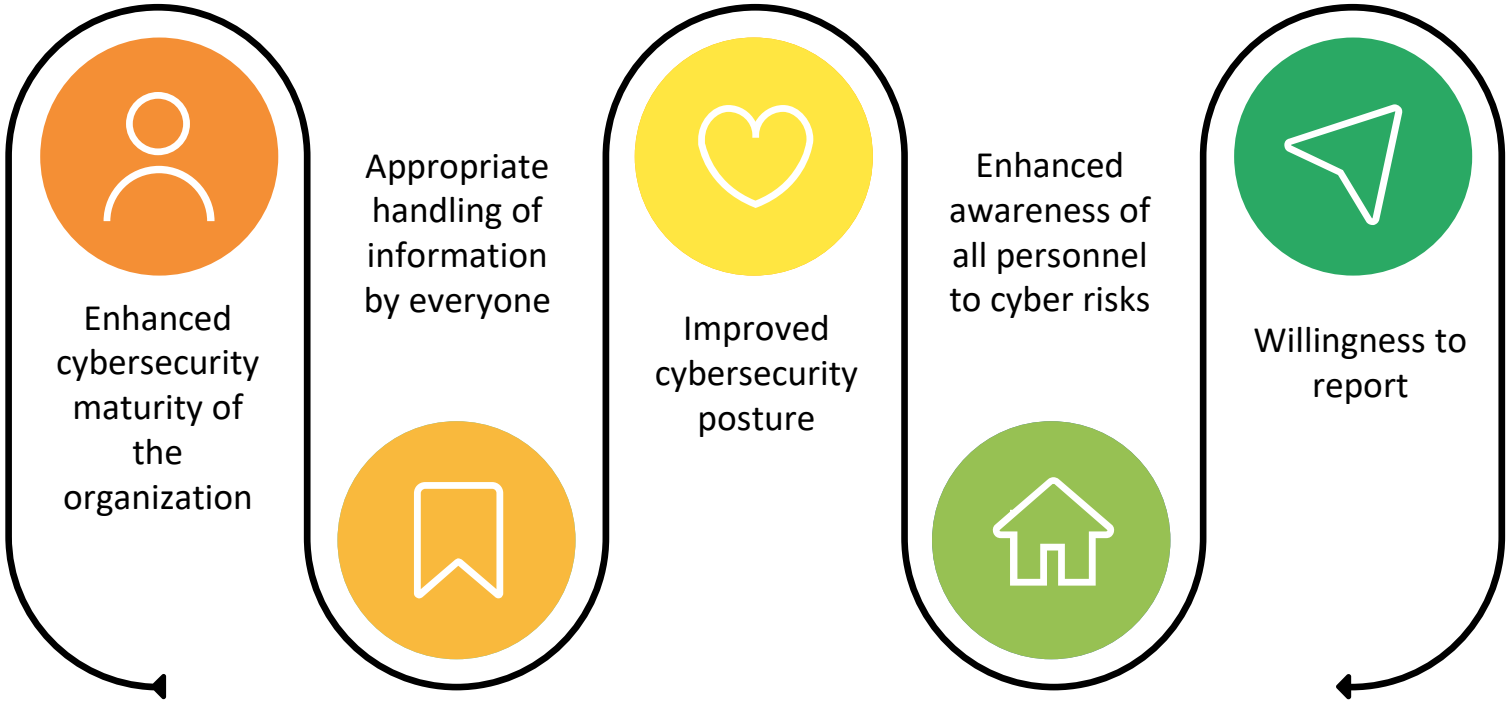
Sonia HIFDI, Chief Aviation Security Policy Section, ICAO

Cybersecurity Culture in Civil Aviation

A set of assumptions, attitudes, beliefs, behaviours, norms, perceptions, and values that are inherent in the **daily operation of an organization** and arereflected by the actions and behaviours of all entities and personnel in their interaction with digital assets

AVIATION CYBERSECURITY

Benefits of a Robust Cybersecurity Culture:

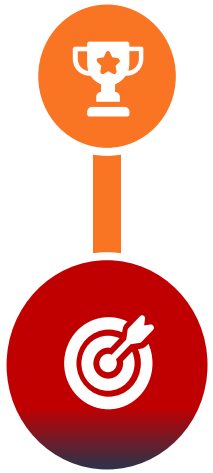


Building a cybersecurity culture

SAFETY

SECURITY

Core Elements:
Leadership



Senior Management:

- ✓ Commit to Cybersecurity Culture
- ✓ Ensure appropriate resources are allocated
- ✓ Lead by Example and abide by rules and processes
- ✓ Make cybersecurity an organizational priority
- ✓ Support implementation, awareness, training, and capacity building
- ✓ Follow up on report processing and resolution
- ✓ Intervene when needed
- ✓ Monitor the cyber posture of the organization

Core Elements:
Cross-Domain Links

Multidisciplinary Task Force:

- ✓ Assess maturity of culture
- ✓ Identify risks and opportunities in culture implementation
- ✓ Bridge requirements of internal stakeholders
- ✓ Support cross-domain activities to foster organizational culture

Core Elements:
Communication

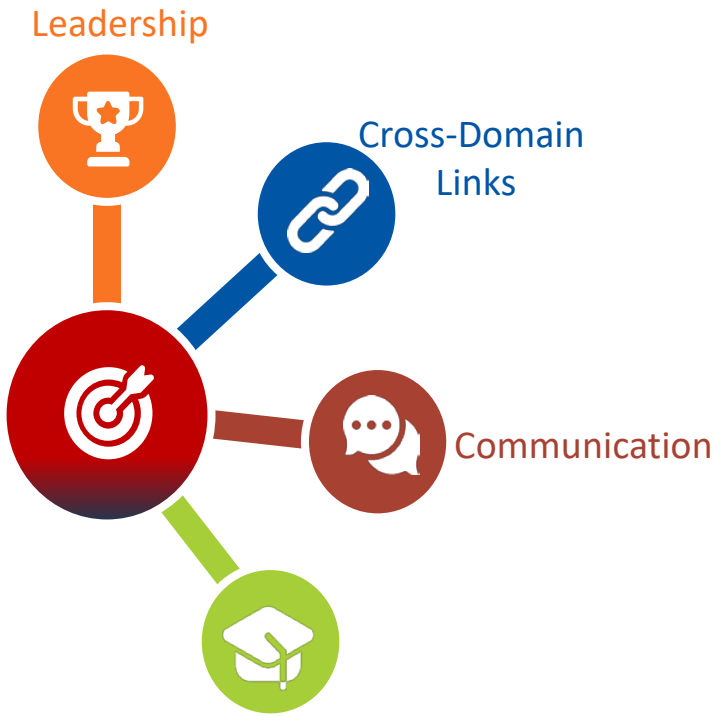
Elements:

- ✓ Communication Skills (style, clarity, listening)
- ✓ Downstream explanation of policies and guidelines

Supports:

- ✓ Awareness
- ✓ Compliance

Core Elements:
Awareness, Training, Education



Core Elements:
Reporting Systems

Contains elements aimed to:

- ✓ ensure confidentiality of personal information
- ✓ define clear policy on confidentiality of handling collected information
- ✓ provide adequate training to all personnel on using the reporting system
- ✓ provide awareness on and implement “just culture” in cybersecurity reporting
- ✓ Implement incentive programme to encouraging personnel to report their own errors as well as any suspicious cyber behaviours they observe

Core Elements:
Continuous review and improvement

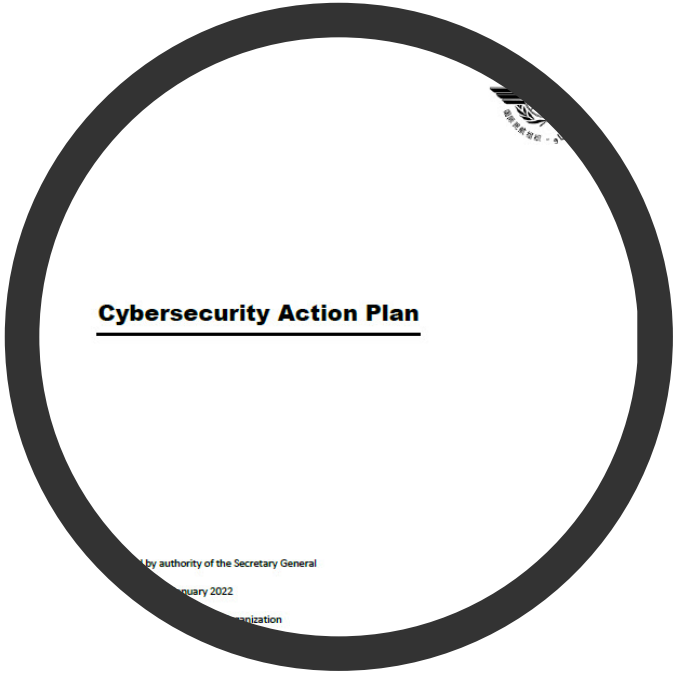
Developing Performance Indicators including:

- ✓ Statistics on reports/compare with organization's logs
- ✓ Results of recurrent training
- ✓ Results of tests/simulations of cyber incidents
- ✓ Questionnaires/interviews/etc.

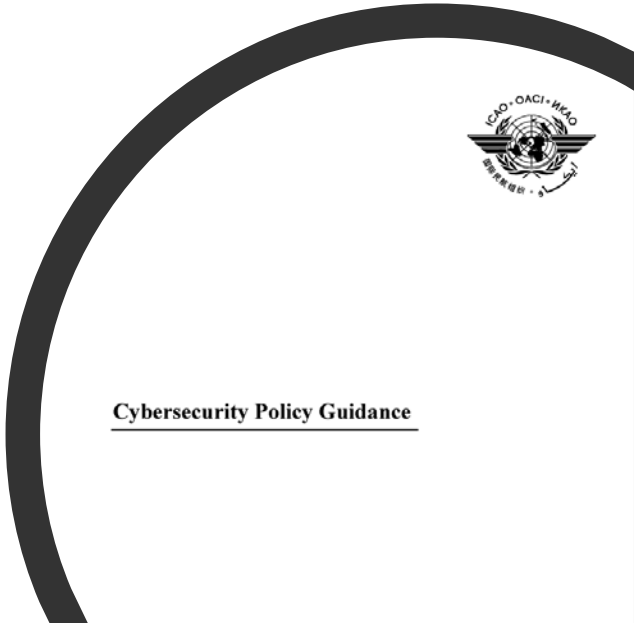
Core Elements:
Positive Work Environment

Elements:

- ✓ Setting targets on cyber incidents to and periodic briefings on achievements
- ✓ Provision of adequate procedures, training, and tools to personnel
- ✓ Involvement of personnel in decision-making/feedback
- ✓ Allocate time for training
- ✓ Recognize good performance
- ✓ Timely response to feedback and reports
- ✓ Providing personnel with appropriate levels of responsibility



ICAO Aviation Cybersecurity Resources



https://www.icao.int/aviationcybersecurity/Pages/default.aspx

ICAO Aviation Security Resources – Guidance In the Pipeline

- ✓ Generic high-level Cyber Threat and Risk Assessment Methodology
- ✓ Aviation Cybersecurity Glossary of Terms
- ✓ Principles to integrate aviation cybersecurity into State Safety Programmes (SSP) and National Civil Aviation Security Programmes (NCASP)
- ✓ Cyber Incident Reporting
- ✓ Cyber Information Sharing
- ✓ Cyber Incident Response & Recovery and Coordination with Organizational crisis management/emergency response plans

Thank You

ICAO