



INTERPORTPOLICE · Programme Paper

Cyber Security Incident Management

Planning considerations for transportation security authorities

In one line: a cyber incident at an airport or port is an operational security event, not just an IT problem.

The challenge

Ransomware has halted Japan's busiest container port, disrupted terminals across Australia, and taken down flight displays and baggage systems at a major airport for weeks. None of these incidents began as a physical security event; all of them ended as one, grounding flights, stopping cargo and consuming security command attention for days.

Regulators are responding with new obligations for ports, airports and their supply chains. Authorities need police, security and technical teams to plan and command together before the incident, not discover each other during it.

What it is

Built by the INTERPORTPOLICE Joint Cyber Security Task Force, this programme helps airport, seaport and transportation security authorities prepare for and lead through cyber incidents. Its practice guide, Planning Considerations for Cyber Incidents, adapts the Federal Emergency Management Agency 2022 planning considerations for the transportation environment. Cyber incident command is built into P²SeMS.

A central question it answers: when does police and security leadership lead a cyber incident, and when does it support the technical response? An incident contained within IT and operational technology systems is usually led technically; once there are physical consequences, such as a stopped crane, a failed access gate or a grounded aircraft, police and security typically lead on consequences.

What it covers

Element	What it covers
Threat picture	Cyber assets, incident types, current tactics and the incidents that define the current era
Critical services	Working with service owners to identify critical services, dependencies and the consequences of losing them
Resilient systems	Patching, IT/OT network segmentation, manual fallbacks and supply-chain vetting
Command and coordination	A unified coordination structure and clear lead and support roles
People and exercises	The human layer, REDI cyber exercises and the optional Cyber Security Assurance programme
Communications	Integrated communications, public messaging and secure collaboration through the Task Force
Building-block path	Build the foundation, keep it in place, and stay ahead through continuous improvement

What it gives your authority

- A shared understanding between technical leaders and police and security commanders.
- A step-by-step checklist that works as both a technical to-do list and an executive accountability tool.
- Exercises that test the plan before an adversary does.
- A trusted network of peers sharing cyber threats across the sector.

Who it is for

Chief information security officers, IT and operational technology leads, and the police and security commanders who must lead or support the response to a cyber incident.

How to take part

1. Contact INTERPORTPOLICE for the Planning Considerations for Cyber Incidents guide.
2. Join the Joint Cyber Security Task Force and its secure collaboration channel.
3. Exercise your plan with a REDI cyber scenario, and consider the optional Cyber Security Assurance awareness programme for all staff.

Listen on Security Mindset: [Part One: Cyber Considerations for Maritime Incident Management](#) · [Part Two: The Nexus of Police and Security in Relation to Cybersecurity](#)

Contact INTERPORTPOLICE: membership@interportpolice.org · www.interportpolice.org